Symmetric graphs of diameter two

Maria Carmen Amarra
B.S., M.S. University of the Philippines – Diliman

This thesis is presented for
the degree of
Doctor of Philosophy
of
The University of Western Australia

School of Mathematics and Statistics
November 2012

Abstract

A graph Γ is *G-symmetric* if it admits an arc-transitive subgroup G of automorphisms, and has *diameter* 2 if it is not a complete graph (that is, it has at least one pair of nonadjacent vertices) and if any two nonadjacent vertices have a common neighbour. Using normal quotient analysis, the study of G-symmetric diameter 2 graphs can be reduced to the following cases:

(i) All nontrivial G-normal quotient graphs of Γ are complete graphs.

(ii) All nontrivial normal subgroups of G act transitively on the vertex set of Γ.

We consider in detail the pairs (Γ, G) that satisfy (i) where Γ may have diameter greater than two, as well as those that satisfy (ii) where Γ has diameter 2 and G is maximal in the symmetric group of the vertex set of Γ subject to being non-2-transitive.

For the first case, we show that if Γ has at least three nontrivial normal quotients, then G corresponds to a finite transitive linear group H and Γ can be constructed from the natural vector space of H. We classify all connected graphs arising from groups H which are not subgroups of a one-dimensional affine group, and identify those which have diameter greater than two. For the second case, the group G is given by C. E. Praeger's classification of quasiprimitive permutation groups, and we focus on the subcase where G is of affine type. Such groups G correspond to irreducible subgroups of the general linear group which, in turn, have been classified by M. Aschbacher. Moreover, a uniform construction for Γ is known, so it only remains to determine which graphs have diameter 2. Using a case-by-case analysis, we are able to classify all diameter 2 graphs for some of the Aschbacher classes; in the others we determine bounds on certain parameters in order to have diameter 2, which reduce the number of unresolved cases.

Dedicated to the memory of

Arturo Amarra, Mario Valencia,

and

Carmen Ponce-Villaroman

This research was undertaken with the support of an Endeavour International Postgraduate Research Scholarship (March 2008 to March 2012), a Samaha Top-Up Scholarship (March 2008 to September 2011), a Scholarship for International Research Fees (April to June 2012), and a University Postgraduate Award (International Students) from The University of Western Australia.

Acknowledgements

My deepest gratitude goes, naturally, to my supervisors, Professors Cheryl Praeger and Michael Giudici. I can give them no praise or compliment that has not already been given by others, except perhaps to say: I am a better mathematician (and writer) for having worked with them. (Which is not to say, of course, that one has not much farther to go.) I hope, throughout my professional life, to be able to do justice to the training I received from them.

I thank The University of Western Australia for providing the financial support that made this whole undertaking possible, and the School of Mathematics and Statistics — especially the Centre for the Mathematics of Symmetry and Computation — for providing a supportive intellectual environment. Special thanks to Dr. John Bamberg and Dr. Pablo Spiga for pointing out connections with other areas; that their ideas were not developed in this thesis is entirely my shortcoming.

And also to:

My family, without whom I would not be here — or anywhere; especially my mother for saying *Mangangarap ka na nga lang, taasan mo na* (Aim high), and my father for his incredible patience and understanding;

Gino and Manjo, for the friendship that has managed to survive the years and the geographical distance;

Beth, for being there, and for all the other things that can never be repaid;

Chevs — the other Cheryl, for taking over the cleaning and the cooking, for practically feeding her (useless) flatmate those last six months, and above all for the companionship of the past four years;

And all my other friends in Perth, then and now, from whom I learned a lot — including the meaning of *bittersweet*.

Maraming salamat.

Contents

Introduction

A *graph* is an abstraction of a network, and consists of a set of vertices linked by edges. Perhaps the best-known application of symmetric graphs is in the design of networks for parallel computing, where graph properties such as symmetry, valency, and diameter (among others) correlate with network properties such as efficiency, connectivity, and resilience (see [**2, 11, 26**]). In this context, symmetric graphs with small diameters, with their regular structure and high connectivity, are particularly desirable (see [**12, 16**]).

This thesis investigates the general structure of symmetric graphs with diameter 2 — that is, those graphs whose automorphism group acts transitively on their arc set, and in which any pair of vertices are connected or are connected to a common vertex. The symmetric diameter 2 case is interesting since this includes all symmetric strongly regular graphs, and in particular all of the rank 3 graphs (see Sections 1.4 and 6.3).

All symmetric graphs are vertex-transitive, and we set up our analysis by identifying the *basic* vertex-transitive graphs. These are graphs whose structure provides insight on the structure of any given vertex-transitive graph, and which can thus be considered as the building blocks of vertex-transitive graphs. We achieve the above using normal quotient reduction, which is described in Section 2.4, and obtain the following result:

Theorem 1. *Let Γ be a connected graph with a vertex-transitive group G of automorphisms. Then there exists a proper normal subgroup N of G (possibly the trivial subgroup) such that, relative to G/N, the corresponding normal quotient Γ_N is either*

(1) quotient-complete, or
(2) vertex-quasiprimitive and not complete.

The terms *quotient-complete* and *vertex-quasiprimitive* are defined in Section 2.4. We note that the property of being quotient-complete or vertex-quasiprimitive (or, for that matter, arc-transitive) is dependent on the subgroup of automorphisms being considered, and gives extra useful information that we can exploit. Hence the characterisation of the graphs that arise in Theorem 1 involves identifying the pairs (Γ, G), where Γ is a graph and $G \leq \mathrm{Aut}(\Gamma)$ with the desired property. Our broad aim is to classify all symmetric, diameter 2 graphs that are either quotient-complete or vertex-quasiprimitive.

In the quotient-complete case we consider graphs which are symmetric *with diameter possibly greater than two.* For symmetric quotient-complete graphs, a significant parameter is the number k of nontrivial complete normal quotients. Infinite families of examples exist for the cases $k = 1$ and $k = 2$, for which we give constructions in Section 4.2. A complete classification, however, is difficult to achieve. For $k \geq 3$ it turns out that the graph structure is more restricted, and the corresponding automorphism groups arise from finite transitive linear groups H acting on a vector space over a finite field. The main result for this case is Theorem 2.

Theorem 2. *Let Γ be a graph with a symmetric group G of automorphisms, such that Γ is G-quotient-complete with k distinct nontrivial, complete G-normal quotients. If $k \geq 3$ then Γ has order c^2 for some prime power c, and all nontrivial complete normal quotients have order c. Furthermore, either $k = c$ and $\Gamma \cong c.K_c$, or $k \leq \sqrt{c}+1$. All pairs (Γ, G) are known, up to possible additional examples associated with one-dimensional affine groups.*

In addition to the above, we also determine which of the graphs in Theorem 2 have diameter 2.

The vertex-quasiprimitive case further divides according to Praeger's classification of finite quasiprimitive permutation groups (Theorem 1.3.8). Under this system the quasiprimitive groups are characterised by their *socle*, which is the direct product of all minimal normal subgroups. We restrict our attention to the groups and graphs that satisfy Hypothesis 3 below. (A permutation group is 2-*transitive* on a set if it is transitive on the set of ordered pairs of distinct elements of that set.)

Hypothesis 3. For a nonempty set Ω, the group $G \leq \mathrm{Sym}(\Omega)$ is quasiprimitive on Ω, and is maximal in $\mathrm{Sym}(\Omega)$ such that G is not 2-transitive.

By Theorem 1.3.8, a group G satisfying Hypothesis 3 must be one of the following:

(i) a group of affine type;
(ii) a group of diagonal type;
(iii) a wreath product of symmetric groups in product action; or
(iv) an almost simple group.

We say that the quasiprimitive group G is *maximal* of *affine type* (respectively, of *diagonal type*, *product type*, or *almost simple type*) in case (i) (respectively, (ii), (iii), or (iv)). The socle of G is abelian if and only if G is of affine type.

Much of our work deals with the case where G is maximal of affine type. In this case G is a subgroup of an affine group $\mathrm{AGL}(d,p)$ for some prime p, with the natural action of $\mathrm{AGL}(d,p)$ on the underlying vector space V. The point stabiliser G_0 of the zero vector is an irreducible subgroup of $\mathrm{GL}(d,p)$ which is maximal with respect to being intransitive on the set $V^{\#}$ of nonzero vectors. The possibilities for G_0 are given by Aschbacher's Theorem (see Theorem 3.6.1), which classifies the irreducible subgroups of the finite classical groups. This result organises the irreducible subgroups into eight classes $\mathcal{C}_i$, $2 \leq i \leq 9$, and our preliminary analysis shows that we only need to consider the subgroups of $\Gamma\mathrm{L}(n,q)$ and

$\Gamma\mathrm{Sp}(n,q)$, where $q^n = p^d$, which are maximal in the classes $\mathcal{C}_i$ for $2 \le i \le 9$, $i \ne 3$. Most of the groups in classes $\mathcal{C}_2$ to $\mathcal{C}_8$ can be described as stabilising a particular geometric configuration in V; those in the class $\mathcal{C}_9$ do not have a uniform geometric description, and so we do not consider this class in detail. Results in [**21, 22**] on the existence of regular orbits imply order restrictions on G_0; however, these are not strong enough to rule out examples or to resolve this case.

Our main result for the affine case is Theorem 4.

Theorem 4. *Let Γ be a connected graph with a symmetric group G of automorphisms, where G is vertex-quasiprimitive and is maximal of affine type. Then Γ is isomorphic to a Cayley graph $\mathrm{Cay}(V,S)$, where $V = \mathbb{F}_p^d$ for some prime p and S is an orbit of the point stabiliser G_0 of the zero vector, with $\langle S\rangle = V$ and $S = -S$. The group G_0 is a subgroup of $\Gamma\mathrm{L}(n,q)$ or $\Gamma\mathrm{Sp}(n,q)$, where $q^n = p^d$. If $\mathrm{diam}(\Gamma) = 2$ then one of the following holds:*

(1) (G_0,S) are as in Tables 1 and 2;

(2) G_0 satisfies the conditions in Table 3; or

(3) G_0 belongs to the class $\mathcal{C}_9$.

Furthermore, all pairs (G_0,S) in Tables 1 and 2 yield G-symmetric diameter 2 graphs $\mathrm{Cay}(V,S)$.

In Tables 1 and 2, the sets X_s and Y_s are as in (5.3.3) and (5.4.3), respectively, $c(v)$ is as in (5.5.4), W_β is as in (5.3.7), S_0 is as in (3.3.1), and $S_\#$, $S_\square$, and $S_\boxtimes$ are as in (5.2.1). Cayley graphs are defined in Section 2.2.

	$G_0 \cap \mathrm{GL}(n,q)$	S	Conditions
1	$\mathrm{GL}(m,p) \wr \mathrm{Sym}\,(t)$, $mt = d$	X_s	$q^m > 2$ and $s \ge t/2$
2	$\mathrm{GL}(k,q) \otimes \mathrm{GL}(m,q)$, $km = d$	Y_s	$s \ge \frac{1}{2}\min\{m,n\}$
3	$\mathrm{GL}(n,q^{1/r}) \circ Z_{q-1}$, $r > 2$ and $n > 2$	v^{G_0}	$c(v) = r-1$ or $c(v) = r$
4	$\mathrm{GL}(n,q^{1/r}) \circ Z_{q-1}$, $r = 2$ or $n = 2$	v^{G_0}	$c(v) = 1$
5	$(Z_{q-1} \circ (Z_4 \circ Q_8)).\mathrm{Sp}(2,2)$, $d = 2$, q odd	v^{G_0}	$v \in V^\#$
6	$\mathrm{GL}(m,q) \wr_\otimes \mathrm{Sym}\,(2)$, $m^2 = d$	Y_s	$s \ge m/2$
7	$\mathrm{GU}(n,q)$, $n \ge 2$	S_0, $S_\#$	
8	$\mathrm{GO}(n,q)$, $n = 3$ and $q = 3$	S_0	
9	$\mathrm{GO}(n,q)$, qn odd, $n > 3$ or $q > 3$	S_0, $S_\square$, or $S_\boxtimes$	
10	$\mathrm{GO}^+(n,q)$, n even, q odd, $n > 2$ or $q > 2$	S_0 or $S_\#$	
11	$\mathrm{GO}^-(n,q)$, n even, q odd, $n > 2$	S_0 or $S_\#$	

TABLE 1. Symmetric diameter 2 graphs from maximal subgroups of $\Gamma\mathrm{L}(n,q)$

If G is maximal of diagonal type then the corresponding graphs Γ can also be constructed as Cayley graphs $\mathrm{Cay}(T^{d-1},S)$, where T is a nonabelian simple group, $d \ge 2$, and S is a union of conjugacy classes of T^{d-1}. We are not able to classify all diameter 2 graphs that arise, although we do know that diameter 2 graphs exist for $d = 2$ due to the progress made on Thompson's Conjecture and other related results (see Section 6.1).

	$G_0 \cap \mathrm{GL}(n,q)$	S	Conditions
1	$\mathrm{Sp}(m,q)^t.[q-1].\mathrm{Sym}\,(t)$, $mt = d$	X_s	$q^m > 2$ and $s \geq t/2$
2	$\mathrm{GL}(m,q).[2]$, $2m = d$	W_β	$\beta \in \mathbb{F}_q$
3	$(Z_{q-1} \circ Q_8).\mathrm{O}^-(2,2)$, $d = 2$, q odd	v^{G_0}	$v \in V^\#$
4	$\mathrm{GO}^+(n,q)$, $n = 2$ and $q = 2$	S_0	
5	$\mathrm{GO}^+(n,q)$, qn even, $n > 2$ or $q > 2$	S_0 or $S_\#$	
6	$\mathrm{GO}^-(n,q)$, qn even, $n > 2$	S_0 or $S_\#$	

Table 2. Symmetric diameter 2 graphs from maximal subgroups of $\Gamma\mathrm{Sp}(n,q)$

	$G_0 \cap \mathrm{GL}(n,q)$	Conditions	Restrictions
1	$\mathrm{GSp}(k,q) \otimes \mathrm{GO}^\epsilon(m,q)$, m odd, $q > 3$		Proposition 5.4.4
2	$\mathrm{GL}(n,q^{1/r}) \circ Z_{q-1}$	$c(v) \neq r-1, r$	Proposition 5.5.3 (2), (3), (4)
3	$(Z_{q-1} \circ R).\mathrm{Sp}(2t,r)$, $d = r^t$	R of type 1, $t \geq 2$	Proposition 5.6.1 (1)
4	$(Z_{q-1} \circ R).\mathrm{Sp}(2t,2)$, $d = r^t$	R of type 2, $t \geq 2$	Proposition 5.6.1 (2)
5	$(Z_{q-1} \circ R).\mathrm{O}^-(2t,2)$, $d = r^t$	R of type 4, $t \geq 2$	Proposition 5.6.1 (3)
6	$\mathrm{GL}(m,q) \wr_\otimes \mathrm{Sym}\,(t)$, $m^t = d$	$t \geq 3$	Proposition 5.7.3
7	$\mathrm{GSp}(m,q) \wr_\otimes \mathrm{Sym}\,(t)$, $m^t = d$, q odd	$t \geq 3$	Proposition 5.7.4

Table 3. Other conditions for diameter 2 (affine case)

For $d \geq 3$ we obtain necessary conditions for diameter 2. Our main result for this case is Theorem 5.

Theorem 5. *Let Γ be a connected graph with a symmetric group G of automorphisms, where G is vertex-quasiprimitive and is maximal of diagonal type. Then $\Gamma \cong \mathrm{Cay}(T^{d-1}, S)$, where T is a nonabelian simple group and S is an orbit of $\mathrm{Aut}\,(T) \times \mathrm{Sym}\,(d)$. If $\mathrm{diam}(\Gamma) = 2$ then one of the following holds:*

(1) $d = 2$ and $S \cup S^2 = T$;

(2) $d = 3$ and S does not contain $(t, 1_T)$ for any $t \in T$; or

(3) $d \geq 4$, $|T|$ is bounded above by a function of d, and S satisfies the restrictions described in Proposition 6.1.6.

If G is maximal of product type then $G \cong \mathrm{Sym}\,(k) \wr \mathrm{Sym}\,(m)$, $k \geq 5$ and $m \geq 2$, with the product action (1.3.1), and the resulting graph is the *distance-ν graph* $H^\nu(m,k)$ of the Hamming graph $H(m,k)$ for some $\nu \in \{0,\ldots,m\}$, which is defined in Section 6.2. We thus have Theorem 6.

Theorem 6. *Let Γ be a connected graph with a symmetric group G of automorphisms, such that G is vertex-quasiprimitive and is maximal of product type. Then $G = \mathrm{Sym}\,(k) \wr \mathrm{Sym}\,(m)$ with $k \geq 5$, and Γ is a distance-ν graph $H^\nu(m,k)$ of the Hamming graph $H(m,k)$, for some $\nu \in \{0,\ldots,m\}$. Furthermore, $\mathrm{diam}(\Gamma) = 2$ if and only if $\nu \geq \frac{1}{2}m$.*

The rest of this thesis is organised as follows.

Chapters 1, 2 and 3 present the basic concepts used throughout the thesis, as well as related results: Chapter 1 on permutation groups and group actions, Chapter 2 on algebraic graph theory, and Chapter 3 on linear algebra. We prove Theorem 1 in Section 2.4. We also present some classification theorems that form the framework of our analysis of various cases — namely, the O'Nan-Scott Theorem for quasiprimitive groups (Theorem 1.3.8), Hering's Theorem (Theorem 3.5.1), and Aschbacher's Theorem (Theorem 3.6.1).

Chapter 4 deals with quotient-complete symmetric graphs. We give examples for the cases where the parameter k has value 1 or 2, and prove Theorem 2 for the case where $k \geq 3$. The connected graphs that arise are presented in Tables 4.1.1 and 4.1.2; those with diameter 2 are determined and are indicated in the table by the symbol "†". We do not treat completely the case corresponding to transitive subgroups of one-dimensional affine groups, but instead consider only subcases corresponding to some infinite families of subgroups.

Chapter 5 deals with vertex-quasiprimitive symmetric graphs with an automorphism group that is maximal of affine type, and is devoted to the proof of Theorem 4.

Finally, in Chapter 6 we look briefly at the remaining vertex-quasiprimitive cases, which are those where the automorphism group has nonabelian socle and is maximal with respect to being non-2-transitive. We prove Theorems 5 and 6 and pose questions for further research.

The publications arising from this thesis are [**3**] and [**4**].

CHAPTER 1

Permutation groups

In this chapter we introduce some terms, notation, and relevant results on permutation groups. Most of the content is standard and can be found in [**17**]. The more specialised material in Sections 1.2 and 1.3 can be found in [**40**].

1.1. Basic concepts and notation

Throughout this section assume that Ω is a finite nonempty set.

A *permutation* of Ω is a bijection from Ω to itself. The set of all permutations of Ω is a group under composition, called the *symmetric group* on Ω and denoted by $\mathrm{Sym}\,(\Omega)$. If $\Omega = \{1, \dots, n\}$, we also write $\mathrm{Sym}\,(\Omega)$ as $\mathrm{Sym}\,(n)$, the *symmetric group on n letters*. A *permutation group* on Ω is a subgroup of $\mathrm{Sym}\,(\Omega)$.

An *action* of a group G on Ω is a map $G \times \Omega \to \Omega$, $(g, \omega) \mapsto \omega^g$, with the following properties: (i) $\omega^{1_G} = \omega$ for all $\omega \in \Omega$; and (ii) $\omega^{gh} = (\omega^g)^h$ for all $\omega \in \Omega$ and $g, h \in G$. We say that "G acts on Ω" if G has an action on Ω.

For the rest of the section assume that the group G acts on Ω.

Every element g of G induces a permutation of the set Ω, given by the map $\overline{g} : \omega \mapsto \omega^g$ for all $\omega \in \Omega$. The map $\rho : G \to \mathrm{Sym}\,(\Omega)$, where $\rho(g) = \overline{g}$ for all $g \in G$, is a homomorphism of groups and is called a *permutation representation* of G. We denote the image of ρ by G^Ω. If $\ker \rho = \{1_G\}$ then $G \cong G^\Omega$ (and so G is isomorphic to a subgroup of $\mathrm{Sym}\,(\Omega)$) and in this case we say that ρ is *faithful*. We shall frequently use the phrase "kernel of the action" of G to refer to the kernel of the corresponding permutation representation, which consists of all elements of G that fix every element of Ω under the action.

An *orbit* of an element $\omega \in \Omega$ under the action of G is the set $\omega^G := \{\omega^g \mid g \in G\}$. Clearly, the set of G-orbits in Ω form a partition of Ω. If G has exactly one orbit in Ω then its action is said to be *transitive*; otherwise, it is *intransitive*. Equivalently, G acts transitively on Ω (or "G is transitive on Ω") if for any two elements $\alpha, \beta \in \Omega$ there is a $g \in G$ such that $\alpha^g = \beta$.

The *stabiliser* in G *of a point* $\omega \in \Omega$ is the set G_ω (alternatively, $\mathrm{Stab}_G(\omega)$) of all elements of G which fix ω under the action. That is, $G_\omega = \{g \in G \mid \omega^g = \omega\}$. The set G_ω is a subgroup of G. The action of G is said to be *semiregular* if G_ω is the trivial subgroup for all $\omega \in \Omega$; if the action is both semiregular and transitive then it is said to be *regular*.

The relationship between the orbit of a point and its stabiliser is captured in the following fundamental result.

Theorem 1.1.1 (Orbit-Stabiliser Theorem)**.** [**17**, Theorem 1.4A (iii)] *Let Ω be a finite nonempty set, and G a group acting on Ω. Then for any $\omega \in \Omega$,*

$$\left|\omega^G\right| = |G : G_\omega|$$

The next theorem collects some basic results on transitive groups.

Theorem 1.1.2. [**17**, Corollary 1.4A, Exercise 1.4.1, Theorem 1.6A (iv)] *Let Ω be a finite nonempty set. If G is a group acting transitively on Ω, then the following hold.*

1. *(1) The point stabilisers in G form a single conjugacy class of subgroups of G. In particular, $G_{\omega^g} = g^{-1}G_\omega g$ for any $\omega \in \Omega$ and $g \in G$.*
2. *(2) $|G : G_\omega| = |\Omega|$ for each $\omega \in \Omega$.*
3. *(3) The action of G is regular if and only if $|G| = |\Omega|$.*
4. *(4) Let $H \leq G$ and $\omega \in \Omega$. Then the following are equivalent: (i) $G = G_\omega H$; (ii) $G = HG_\omega$; and (iii) H is transitive. In particular, the only transitive subgroup of G containing G_ω is G itself.*
5. *(5) If $H \lhd G$ then the number of H-orbits in Ω divides $|G : H|$.*

In this paragraph assume that G acts transitively on Ω. A *suborbit* of G is an orbit of a point stabiliser G_ω for any $\omega \in \Omega$. If $g \in G$ and $\alpha, \beta \in \Omega$ with $\alpha^g = \beta$, then by statement 1 of Theorem 1.1.2 we have $\beta^{G_{\omega^g}} = \left(\alpha^{G_\omega}\right)^g$. So g induces a bijection from the set of G_ω-orbits to the set of G_{ω^g}-orbits, and since G is transitive the number of suborbits is independent of the choice of ω. The number of its suborbits is called the *rank* of G, and the lengths of the suborbits are its *subdegrees*. There is a one-to-one correspondence between the set of suborbits of G and the set of G-orbits in the Cartesian set $\Omega \times \Omega$ under the action

$$(\alpha, \beta)^g := (\alpha^g, \beta^g) \quad \forall\ \alpha, \beta \in \Omega,\ g \in G. \tag{1.1.1}$$

Indeed, it is not difficult to show that for any $\alpha \in \Omega$ and G-orbit Δ in $\Omega \times \Omega$, the set $\Delta(\alpha) := \{\beta \mid (\alpha, \beta) \in \Delta\}$ is an orbit of G_α. The orbits of G on $\Omega \times \Omega$ are called its *orbitals* on Ω. Clearly, the set $\Delta_0 := \{(\omega, \omega) \mid \omega \in \Omega\}$ is a G-orbital; this is called the *trivial* or *diagonal* orbital. For each orbital Δ define $\Delta^* := \{(\beta, \alpha) \mid (\alpha, \beta) \in \Delta\}$; if $\Delta = \Delta^*$ then Δ is said to be *self-paired*.

We now consider some generalisations of the concept of a point stabiliser. Suppose that Δ is a nonempty proper subset of Ω, and for any $g \in G$ denote by Δ^g the set $\{\delta^g \mid \delta \in \Delta\}$. The sets

$$G_{(\Delta)} = \{g \in G \mid \delta^g = \delta \quad \forall\ \delta \in \Delta\}$$

and

$$G_{\{\Delta\}} = \{g \in G \mid \delta^g \in \Delta \quad \forall\ \delta \in \Delta\} = \{g \in G \mid \Delta^g = \Delta\}$$

are called the *pointwise stabiliser* and the *setwise stabiliser*, respectively, of Δ. Both $G_{(\Delta)}$ and $G_{\{\Delta\}}$ are subgroups of G, with $G_{(\Delta)} \trianglelefteq G_{\{\Delta\}}$. It is easy to see that

$$G_{(\Delta)} = \bigcap_{\delta \in \Delta} G_\delta,$$

and that the action of G on Ω induces an action of $G_{\{\Delta\}}$ on Δ. The set Δ is said to be *G-invariant* if $G_{\{\Delta\}} = G$, that is, if $\Delta^g = \Delta$ for all $g \in G$. Clearly, Δ is G-invariant if and only if it is a union of orbits of G. In this case the action of G restricted to Δ is an action of G on Δ with kernel $G_{(\Delta)}$, so that with the notation above we have $G/G_{(\Delta)} \cong G^\Delta$.

Example 1.1.3. Consider the action of G on itself via conjugation, that is,

$$a^g := g^{-1}ag \quad \forall\, a, g \in G.$$

The point stabiliser of $a \in G$ is the subgroup $C_G(a)$ of all group elements that commute with a, and is called the *centraliser* of a in G. If H is a subgroup of G, the pointwise stabiliser of H is the subgroup $C_G(H)$ where

$$C_G(H) = \{x \in G \mid hx = xh \quad \forall\, h \in H\},$$

and is likewise called the *centraliser* of H in G. (If $H = G$ the group $C(G) := C_G(G)$ is calld the *center* of G.) The setwise stabiliser of H is the subgroup $N_G(H)$ given by

$$N_G(H) = \{x \in G \mid x^{-1}hx \in H \quad \forall\, h \in H\}.$$

Observe that $H \trianglelefteq N_G(H)$; indeed, $N_G(H)$ is the largest subgroup of G that contains H as a normal subgroup. We call $N_G(H)$ the *normaliser* of H in G. □

Some properties of the centraliser of a transitive group are given in Theorem 1.1.4.

Theorem 1.1.4. [**17**, Theorem 4.2A] *Let $G \leq \mathrm{Sym}\,(\Omega)$ be transitive, $\omega \in \Omega$, and $C := C_{\mathrm{Sym}(\Omega)}(G)$. Then:*

(1) C is semiregular, and $C \cong N_G(G_\omega)/G_\omega$.
(2) C is transitive if and only if G is regular.
(3) If C is transitive, then it is conjugate to G in $\mathrm{Sym}\,(\Omega)$ and hence C is regular.
(4) $C = 1$ if and only if $N_G(G_\omega) = G_\omega$.
(5) If G is abelian, then $C = G$.

Suppose that G acts transitively on Ω. A *G-invariant partition* of Ω is a partition $\mathcal{P}$ such that $P^g \in \mathcal{P}$ for all parts $P \in \mathcal{P}$ and $g \in G$. Thus G permutes the parts of a G-invariant partition $\mathcal{P}$, and if $g^{\mathcal{P}}$ denotes the permutation of $\mathcal{P}$ induced by the element $g \in G$, then the map $G \to \mathrm{Sym}\,(\mathcal{P})$, given by $g \mapsto g^{\mathcal{P}}$ for all $g \in G$, is a permutation representation of G on $\mathcal{P}$ with image $G^{\mathcal{P}}$. Clearly, the *trivial partitions* $\{\Omega\}$ and $\{\{\omega\} \mid \omega \in \Omega\}$ are G-invariant, with $G^{\mathcal{P}}$ trivial if $\mathcal{P} = \{\Omega\}$, and $G^{\mathcal{P}} \cong G$ if $\mathcal{P} = \{\{\omega\} \mid \omega \in \Omega\}$.

It is sometimes necessary to compare two different actions of a group G. The actions of G on nonempty sets Ω and Δ are said to be *equivalent* if there is a bijection $\lambda : \Omega \to \Delta$ such that

$$\lambda(\omega^g) = (\lambda(\omega))^g \quad \forall\ \omega \in \Omega,\ g \in G.$$

In this case the actions of G "differ only in the labelling of the points of the sets involved" [**17**, Section 1.6]. If both actions are transitive, the lemma below gives a necessary and sufficient condition for determining whether or not they are equivalent.

Lemma 1.1.5. [**17**, Lemma 1.6B] *Let G be a group acting acting transitively on the nonempty sets Ω and Δ, and let H be a point stabiliser in G^Ω. Then the actions are equivalent if and only if H is also a point stabiliser in G^Δ.*

Example 1.1.6. [**17**, p. 22] Let G be a group, and let H be a subgroup of G. Consider the action of G on the set Γ_H of right cosets of H in G, given by

$$(Ha)^g := Hag \quad \forall\ Ha \in \Gamma_H,\ g \in G.$$

This action is transitive, and the stabiliser of the point Ha is the subgroup $a^{-1}Ha$. In particular, the subgroup H is the point stabiliser of $H \in \Gamma_H$. We can also define an action of G on the set of left cosets aH of H by

$$(aH)^g := g^{-1}aH \quad \forall\ a, g \in G,$$

and again H is the stabiliser of the point H. It follows from Lemma 1.1.5 that the action of G on the set of right cosets of H and the action of G on the set of left cosets of H are equivalent. □

A consequence of Lemma 1.1.5 and Example 1.1.6 is that every transitive action of G is equivalent to G^{Γ_H} for some $H \leq G$. Moreover, the transitive actions of G are given up to equivalence by the actions G^{Γ_H}, as H varies over the conjugacy classes of subgroups of G.

The notion of equivalent actions of the same group can be generalised to involve actions of two different groups. Suppose that G and H are groups acting on nonempty sets Ω and Δ, respectively. Then G and H are *permutation isomorphic* if there is a bijection $\lambda : \Omega \to \Delta$ and a group isomorphism $\phi : G \to H$ such that

$$\lambda(\omega^g) = \lambda(\omega)^{\phi(g)} \quad \forall\ \omega \in \Omega,\ g \in G.$$

In other words, the actions are "the same" except for the labelling of the points of the sets and of the elements of the groups involved. The next result gives a criterion for two groups, acting faithfully on the same set, to be permutation isomorphic.

Lemma 1.1.7. [**17**, Exercise 1.6.1] *Let G and H be groups acting faithfully on Ω. Then G and H are permutation isomorphic if and only if they are conjugate in* $\mathrm{Sym}(\Omega)$.

If $G \leq \mathrm{Sym}(\Omega)$ is regular, then by Example 1.1.6 its action on Ω is equivalent to its action on itself by right multiplication and also to its action by left multiplication by the inverse, which are given, respectively, by

$$a^g := ag \quad \forall\, a, g \in G$$

and

$$a^g := g^{-1}a \quad \forall\, a, g \in G.$$

The representations of G into $\mathrm{Sym}(G)$ which correspond to each of the actions above are called the *right* and *left regular representations* of G, respectively. The following results on regular groups will be useful later on.

Theorem 1.1.8. *Let G be a regular subgroup of $\mathrm{Sym}(\Omega)$. Then $X := N_{\mathrm{Sym}(\Omega)}(G) \cong G \rtimes \mathrm{Aut}(G)$, with the natural action of $\mathrm{Aut}(G)$ on G. The group X acts on G with the right multiplication action of G on itself and the natural action of $\mathrm{Aut}(G)$ on G, and the point stabiliser in X of 1_G is $\mathrm{Aut}(G)$.*

The group $G \rtimes \mathrm{Aut}(G)$ in Theorem 1.1.8 is called the *holomorph* of G and is denoted by $\mathrm{Hol}(G)$.

1.2. Blocks, primitivity and quasiprimitivity

Throughout this section suppose that the group G acts transitively on the nonempty set Ω.

A *block of imprimitivity* (or simply *block*) for G is a nonempty subset Δ of Ω with the property that for each $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \varnothing$. The entire set Ω, as well as the single-element subsets of Ω, are clearly blocks for G, and are referred to as the *trivial* blocks. Any other block is *nontrivial.* A transitive group G is said to be *primitive* if the only blocks for G are the trivial blocks; otherwise, it is said to be *imprimitive.*

Let Δ be a block for G. It is easy show that the setwise stabiliser $G_{\{\Delta\}}$ is transitive on Δ, and that for any $g \in G$, the set Δ^g is also a block for G. We call $\mathcal{D} := \{\Delta^g \mid g \in G\}$ the *system of blocks* for G containing Δ. Clearly, a system of blocks for G is a G-invariant partition of Ω, and each part of a G-invariant partition is a block for G. It thus follows that G is primitive on Ω if and only if the only G-invariant partitions are the trivial ones.

The following theorem describes the relation between blocks for and subgroups of G, and provides an alternative definition of primitivity. This result can be found in [**17**, Theorem 1.5A]; we state here the version presented in [**45**].

Theorem 1.2.1. *Let G be a group acting transitively on a set Ω, and let $\omega \in \Omega$. Then there is a bijection between the collection of subgroups of G containing G_ω, and the set of blocks of G containing ω, defined by $H \mapsto \omega^H$ for any $H \leq G$ with $G_\omega \leq H$.*

In particular, G is primitive if and only if G_ω is a maximal subgroup of G for any $\omega \in \Omega$.

The partition consisting of the orbits of a normal subgroup of G is G-invariant, and is called a *G-normal partition*. These will be of interest later on (see Section 2.4). The following theorem from [**17**], which we restate here with the assumption that G is finite, gives the basic properties of G-normal partitions.

Theorem 1.2.2. [**17**, Theorem 1.6A] *Let G be a finite group acting transitively on a set Ω, and let $N \lhd G$. Then the following hold:*

1. *The orbits of N form a system of blocks for G.*
2. *If Δ and Φ are two N-orbits then N^Δ and N^Φ are permutation isomorphic.*
3. *If any point in Ω is fixed by all elements of N, then N lies in the kernel of the action of G.*
4. *The group N has at most $|G : N|$ orbits, and the number of orbits of N divides $|G : N|$.*
5. *If G acts primitively on Ω then either N is transitive or N lies in the kernel of the action.*

The action of G is said to be *quasiprimitive* if and only if the only G-normal partitions are the trivial ones. Clearly, all primitive groups are quasiprimitive, but there are quasiprimitive groups which are imprimitive. An example of such a group is given below.

Example 1.2.3. Let G be a nonabelian simple group and let H be a nontrivial and non-maximal subgroup of G. Consider the action of G by right multiplication on the set Γ_H of right cosets of H in G. Since the only normal subgroups of G are the trivial subgroup and G itself, all G-normal partitions are trivial. Hence G^{Γ_H} is quasiprimitive. Since H is a point stabiliser in G^{Γ_H} (see Example 1.1.6) and H is not maximal in G, it follows from Theorem 1.2.1 that G^{Γ_H} is imprimitive. □

1.3. The O'Nan-Scott Theorem for quasiprimitive groups

The structure of a finite quasiprimitive permutation group can be studied by considering the subgroup generated by its minimal normal subgroups. A nontrivial normal subgroup of a group G is *minimal* if it does not properly contain any nontrivial normal subgroup of G. The subgroup of G generated by all of its minimal normal subgroups is called the *socle* of G and is denoted by $\mathrm{soc}(G)$. Theorem 1.3.1 lists some basic results on the structure of the socle of a finite group.

Theorem 1.3.1. [**17**, Theorem 4.3A] *Let G be a nontrivial finite group.*

(1) *If N is a minimal normal subgroup of G and M is any normal subgroup of G, then either $N \leq M$ or $\langle M, N\rangle = M \times N$.*
(2) *There exist minimal normal subgroups $N_1, \ldots, N_k$ of G such that* $\mathrm{soc}(G) = N_1 \times \ldots \times N_k$.
(3) *If N is a minimal normal subgroup of G then there exist simple groups $T_1, \ldots, T_\ell$ which are conjugate under G such that $N = T_1 \times \ldots \times T_\ell$.*
(4) *If the subgroups N_i in (2) are nonabelian, then these are the only minimal normal subgroups of G. Similarly, if the subgroups T_j in (3) are nonabelian, then these are the only minimal normal subgroups of N.*

The next result is an immediate consequence of Theorem 1.3.1.

Corollary 1.3.2. [**17**, Corollary 4.3A] *If N is a minimal normal subgroup of a finite group, then either N is elementary abelian or $Z(N) = 1$.*

In the case where the group G is quasiprimitive, the structure of the socle is more constrained, as can be seen in the next two results. The first one, discovered by Burnside, concerns 2-transitive groups and is considered to be a precursor of the O'Nan-Scott Theorem. A group $G \leq \mathrm{Sym}(\Omega)$ is said to be 2-*transitive* if the G-action on the set of ordered pairs of distinct elements of Ω, with the action defined in (1.1.1), is transitive. It is known that all 2-transitive groups are primitive.

Theorem 1.3.3. [**17**, Theorem 4.1] *A finite 2-transitive group has a unique minimal normal subgroup N. Moreover, N is either a regular elementary abelian p-group for some prime p, or a nonregular nonabelian simple group.*

The next result, which can be found in [**17**, Theorem 4.3B], is originally stated for primitive groups, but also applies to quasiprimitive groups.

Theorem 1.3.4. *Let G be a group acting quasiprimitively on Ω and let N be a minimal normal subgroup of G. Then exactly one of the following holds:*

(1) *N is regular and elementary abelian of order p^d for some prime p and integer d, and $\mathrm{soc}(G) = N = C_G(N)$;*
(2) *N is regular and nonabelian, $C_G(N)$ is a minimal normal subgroup of G which is permutation isomorphic to N, and $\mathrm{soc}(G) = N \times C_G(N)$;*
(3) *N is nonabelian (possibly regular or nonregular), $C_G(N) = 1$, and $\mathrm{soc}(G) = N$.*

Each case in Theorem 1.3.4 determines certain possible quasiprimitive actions, which are described in Theorem 1.3.8. Before we state this, we first describe in some detail certain constructions which arise in some of the cases in Theorem 1.3.8.

1.3.1. Product actions. Let H and K be groups with K acting on a finite nonempty set Θ with $m \geq 2$ elements, say $\Theta = \{1, \ldots, m\}$. The action of K on Θ induces an action of K on H^m, as follows : for any $(h_1, \ldots, h_m) \in H^m$ and $x \in K$,

$$(h_1, \ldots, h_m)^x := (h_{1'}, \ldots, h_{m'}), \quad \text{where } i' := i^{x^{-1}} \quad \forall\, i. \tag{1.3.1}$$

The *wreath product* $H \wr K$ (with respect to the K-action on Θ) is the semidirect product $H^m \rtimes K$, with the K-action (1.3.1) on H^m. The group H^m is called the *base group* of the wreath product, and K is called the *top group*.

In the wreath product $H \wr K$, assume that the group H acts on a finite nonempty set Λ. Set $\Omega := \Lambda^m$. The *product action* of $H \wr K$ on Ω is defined by

$$(\lambda_1, \ldots, \lambda_m)^{(\overline{h}, x)} := \left(\lambda_{1'}{}^{h_{1'}}, \ldots, \lambda_{m'}{}^{h_{m'}}\right), \quad \text{where } i' := i^{x^{-1}} \quad \forall\, i, \tag{1.3.2}$$

for all $(\lambda_1, \ldots, \lambda_m) \in \Omega$, $\overline{h} := (h_1, \ldots, h_m) \in H^m$, and $x \in K$. Hence we may think of the product action as a "composition" of two actions: the natural componentwise action of the base group H^m on Ω, and the action of K by permutation of the components of Ω.

The product action of a wreath product is primitive under the conditions given in Theorem 1.3.5.

Theorem 1.3.5. [**17**, Lemma 2.7A] *Suppose that H and K are nontrivial groups acting on the finite sets Λ and Θ, respectively, with $|\Theta| = m \geq 2$. Then the wreath product $H \wr K = H^m \rtimes K$ (with respect to the K-action on Θ) is primitive on the product action on $\Omega := \Lambda^m$ if and only if the K-action on Θ is transitive and the H-action on Λ is primitive but not regular.*

1.3.2. Diagonal type subgroups. Let T be a group in its right regular action, and let $k \geq 2$. Let $D := \{(c, \ldots, c) \mid c \in T\} \leq T^k$ and let Ω be the set of cosets of D in T^k. Then Ω can be identified with T^{k-1}. The product action of $T \wr \mathrm{Sym}\,(k)$ on T^k, which is imprimitive by Theorem 1.3.5, induces the following faithful action on Ω: for any $(t_1, \ldots, t_{k-1}) \in \Omega$, $\overline{a} := (a_1, \ldots, a_k) \in T^k$, and $\pi \in \mathrm{Sym}\,(k)$,

$$(t_1, \ldots, t_{k-1})^{\overline{a}.\pi} := \left(a_{k'}{}^{-1} t_{k'}{}^{-1} t_{1'} a_{1'}, \ldots, a_{k'}{}^{-1} t_{k'}{}^{-1} t_{(k-1)'} a_{(k-1)'}\right) \tag{1.3.3}$$

where $i' := i^{\pi^{-1}}$ for all i and $t_k := 1_T$. The group $A := \{(\tau, \ldots, \tau) \mid \tau \in \mathrm{Aut}\,(T)\} \leq \mathrm{Aut}\,(T)^k$ acts on Ω by

$$(t_1, \ldots, t_{k-1})^{(\tau, \ldots, \tau)} := (t_1{}^{\tau}, \ldots, t_{k-1}{}^{\tau}) \tag{1.3.4}$$

for all $(t_1, \ldots, t_{k-1}) \in T^k$ and $\tau \in \mathrm{Aut}\,(T)$, and this action commutes with that of $\mathrm{Sym}\,(k)$. Note that the subgroup D induces the subgroup $\{(\tau, \ldots, \tau) \mid \tau \in \mathrm{Inn}(T)\} \leq A$.

If T is a nonabelian simple group and $H := T^k$, then by [**17**, Lemma 4.5B], the group $W := N_{\mathrm{Sym}(\Omega)}(H)$ can be written as

$$W = \left\{(a_1, \ldots, a_k).\pi \mid \pi \in \mathrm{Sym}\,(k),\ a_i \in \mathrm{Aut}\,(T),\ a_i a_j^{-1} \in \mathrm{Inn}(T) \quad \forall i, j\ \right\}. \tag{1.3.5}$$

Hence $W \cong (T \wr \mathrm{Sym}\,(k)).\mathrm{Out}\,(T)$, and the stabiliser in W of $\omega := (1_T, \ldots, 1_T) \in \Omega$ is

$$W_\omega = A \times \mathrm{Sym}\,(k) \cong \mathrm{Aut}\,(T) \times \mathrm{Sym}\,(k)\,.$$

A group G is said to be of *diagonal type* if

$$T^k = H \leq G \leq W = N_{\mathrm{Sym}(\Omega)}(H)$$

for some nonabelian simple group T. In this case $\mathrm{Inn}(T) \lesssim G_\omega \lesssim \mathrm{Aut}\,(T) \times \mathrm{Sym}\,(k)$, and G acts by conjugation on the set $\mathcal{T} := \{T_1, \ldots, T_k\}$ of simple direct factors of H.

A group of diagonal type is primitive under the conditions given in Theorem 1.3.6.

Theorem 1.3.6. [**17**, Theorem 4.5A] *Using the notation above, suppose that* $G \leq \mathrm{Sym}\,(\Omega)$ *is of diagonal type. Then* G *is primitive if and only if* $k = 2$*, or* $k \geq 3$ *and the conjugation action of* G *on* $\mathcal{T}$ *is primitive. In particular,* W *is primitive for all* $k \geq 2$*.*

1.3.3. Twisted wreath product. Let T and P be groups, and $Q \leq P$ such that there exists a homomorphism $\varphi : Q \to \mathrm{Aut}\,(T)$. Denote by $\mathrm{Fun}(P, T)$ the set of all functions $f : P \to T$, which is a group under pointwise multiplication, and define

$$H := \left\{ f \in \mathrm{Fun}(P, T) \;\middle|\; f(xy) = f(x)^{\varphi(y)} \quad \forall\, x \in P, y \in Q \right\}.$$

Then $H \leq \mathrm{Fun}(P, T)$ and $H \cong T^k$, where $k = |P : Q|$. The group P acts on H by

$$f^z(x) := f(zx) \tag{1.3.6}$$

for all $f \in H$ and $x, z \in P$, and it can be shown that this action preserves the group operation on H so $P \lesssim \mathrm{Aut}\,(H)$. The *twisted wreath product* $T\,twr_\varphi\,P$ is defined to be the semidirect product $H \rtimes P$ with the action in (1.3.6).

The group $T\,twr_\varphi\,P$ acts on H as follows: H acts on itself by right multiplication, and P acts on H by (1.3.6). The stabiliser in $T\,twr_\varphi\,P$ of 1_H ($= f$ where $f(x) = 1_T$ for all $x \in P$) is precisely P.

Theorem 1.3.7 gives a special case of the twisted wreath product that is primitive.

Theorem 1.3.7. [**17**, Lemma 4.7A] *Using the notation above, let* $G = T\ twr_\varphi P \leq \mathrm{Sym}\,(H)$ *where* T *is a nonabelian simple group,* $P \leq \mathrm{Sym}\,(k)$ *is primitive with point stabiliser* Q*, and* $\mathrm{Im}\,\varphi \geq \mathrm{Inn}(T)$ *but* $\mathrm{Im}\,\varphi$ *is not a homomorphic image of* P*. Then* G *is a primitive group with regular socle* H *and point stabiliser isomorphic to* P*.*

1.3.4. The O'Nan-Scott quasiprimitive types. The O'Nan-Scott Theorem for quasiprimitive groups, which was established by C.E. Praeger in [**39**], identifies eight quasiprimitive actions and asserts that these are the only possible ones. This is a generalisation of the O'Nan-Scott Theorem for primitive groups [**17**, Theorem 4.1A], and in most cases the quasiprimitive types can be described in a similar way as the corresponding primitive types.

Theorem 1.3.8 (O'Nan-Scott Theorem for quasiprimitive groups)**.** [**39**, Theorem 1] *Each finite quasiprimitive group is permutation isomorphic to a group of exactly one of the quasiprimitive types HA, HS, HC, AS, TW, SD, CD and PA.*

The descriptions of the different O'Nan-Scott quasiprimitive types, which we give below, can be found in [**39**, Section 2] and [**40**, Section 12]. We present them according to the cases in Theorem 1.3.4 to which they correspond.

Assume throughout that $G \leq \mathrm{Sym}(\Omega)$ is a quasiprimitive group with $\mathrm{soc}(G) = H \cong T^d$ for some simple group T and integer $d \geq 1$, and that N is a minimal normal subgroup of G. Then N is transitive and by Theorem 1.1.2 (4) we have $G = N.G_\omega$ for any $\omega \in \Omega$.

As it happens, all quasiprimitive groups belonging to Cases 1 and 2 (that is, of types HA, HS, HC) are primitive.

Case 1: $H = N$ abelian and regular. Then H is elementary abelian, say $H = \mathbb{Z}_p^d$ for some prime p, and we can identify H with a vector space $V(d,p)$ of dimension d over $\mathbb{F}_p$. It follows from Theorem 1.1.8 that $G \leq \mathrm{Hol}(H) = \mathrm{AGL}(V)$ and the point stabiliser of the zero vector is contained in $\mathrm{GL}(V)$. This case corresponds to one quasiprimitive type.

HA (HOLOMORPH OF AN ABELIAN GROUP): The group $\mathrm{soc}(G) = H$ is regular and elementary abelian, say $H = \mathbb{Z}_p^d$ for some prime p; $\Omega = V(d,p)$; and $H \leq G \leq \mathrm{AGL}(V)$ with $G = H.G_0$, where H is identified with the group of translations on V and the point stabiliser G_0 of the zero vector is an irreducible subgroup of $\mathrm{GL}(V)$. The group G acts on Ω via the natural action of $\mathrm{AGL}(V)$ on V.

Case 2: $H = N \times C_G(N)$, N nonabelian and regular. Again by Theorem 1.1.8 we have $G \leq \mathrm{Hol}(N)$. We have two types, corresponding to each of the subcases $N = T$ and $N = T^k$ for some $k \geq 2$.

HS (HOLOMORPH OF A SIMPLE GROUP): The group $N = T$ is regular and nonabelian, and $\mathrm{soc}(G) = H \cong T^2$; $\Omega = T$; and $T^2 \leq G \leq T^2.\mathrm{Out}(T) \leq W$, where W is as in (1.3.5) with $k = 2$. The group G acts on Ω with the action of W defined in (1.3.3) and (1.3.4). Equivalently, $T.\mathrm{Inn}(T) \leq G \leq \mathrm{Hol}(T)$ with the following action: for any $t \in \Omega$, $a \in T$ and $\tau \in \mathrm{Aut}(T)$,

$$t^{a.\tau} := t^\tau a^\tau$$

If $\omega = 1_T \in \Omega$, then $G = T.G_\omega$ where $\mathrm{Inn}(T) \leq G_\omega \leq \mathrm{Aut}(T)$.

HC (HOLOMORPH OF A COMPOUND GROUP): The group $N = T^k$, for some $k \geq 2$, is regular and nonabelian, and $\mathrm{soc}(G) = H \cong T^{2k}$; $\Omega = T^k$; and $T^{2k} \leq G \leq U \wr \mathrm{Sym}(k)$, where $U := T^2.\mathrm{Out}(T) \leq \mathrm{Sym}(T)$ is a quasiprimitive group of type HS. The group G acts on Ω with the product action of $U \wr \mathrm{Sym}(k)$ defined in (1.3.2). Equivalently, $N.\mathrm{Inn}(N) \leq G \leq \mathrm{Hol}(N)$ with the following action: for any $(t_1, \ldots, t_k) \in \Omega$,

$\overline{a} := (a_1, \ldots, a_k) \in T^k$ and $\sigma \in \mathrm{Aut}\,(N) = \mathrm{Aut}\,(T) \wr \mathrm{Sym}\,(k)$,

$$(t_1, \ldots, t_k)^{\overline{a}.\sigma} := (t_1 a_1, \ldots, t_k a_k)^{\sigma}.$$

If $\omega = 1_N = (1_T, \ldots, 1_T) \in \Omega$ then $G = N.G_\omega$, where $\mathrm{Inn}(N) \leq G_\omega \leq \mathrm{Aut}\,(N)$ and G_ω acts transitively by conjugation on the simple direct factors of N.

Case 3: $H = N$ nonabelian, $C_G(N) = 1$. In this case H may be regular or nonregular. Hence the map $\psi : G \to \mathrm{Aut}\,(H)$, where $\psi(g) : h \mapsto g^{-1}hg$ for any $h \in H$ and $g \in G$, is an endomorphism, and $G \lesssim \mathrm{Aut}\,(H) = \mathrm{Aut}\,(T) \wr \mathrm{Sym}\,(d)$. The case where H is simple corresponds to one quasiprimitive type.

AS (ALMOST SIMPLE): The group $\mathrm{soc}(G) = T$ is nonabelian simple, and may be regular or nonregular; $T \leq G \leq \mathrm{Aut}\,(T)$ and $G = TG_\omega$, for some $\omega \in \Omega$.

For the remaining cases $H = T^d$ for some $d \geq 2$. If H is regular then we get another quasiprimitive type.

TW (TWISTED WREATH): The group $\mathrm{soc}(G) = H \cong T^d$ is regular and nonabelian, with $d \geq 2$; $\Omega = H$; and $G = T\,twr_\varphi\,P$, where H, P and φ are as defined in Section 1.3.3. Furthermore,

$$\mathrm{core}_P\left(\varphi^{-1}(\mathrm{Inn}(T))\right) = \bigcap_{x \in P} \varphi^{-1}(\mathrm{Inn}(T))^x = \{1\}.$$

The group G acts on Ω as follows: H acts on itself by right multiplication and P acts on H by the action defined in (1.3.6). If $\omega := 1_H$, then $G_\omega = P$.

The case where H is nonregular corresponds to three quasiprimitive types.

SD (SIMPLE DIAGONAL): The group $\mathrm{soc}(G) = H = T^d$ is nonregular and nonabelian, with $d \geq 2$; $\Omega = T^{d-1}$; and $T^d \leq G \leq W$, where W is as defined in (1.3.5) with $k = d$. The group G acts on Ω with the action of W defined in (1.3.3) and (1.3.4), with G acting transitively (not necessarily primitively) by conjugation on the d simple direct factors of H. If $\omega := 1_H$ then $H_\omega = I \leq G_\omega \leq A \times \mathrm{Sym}\,(d)$, where $I := \{(t, \ldots, t) \mid t \in \mathrm{Inn}(T)\}$ and $A := \{(a, \ldots, a) \mid a \in \mathrm{Aut}\,(T)\}$.

CD (COMPOUND DIAGONAL): The group $\mathrm{soc}(G) = H = T^d$ is nonregular and nonabelian, with $d \geq 4$; $\Omega = \Lambda^m$ for some divisor m of d, $m \geq 2$; and $T^d \leq G \leq U \wr \mathrm{Sym}\,(m)$, where $U \leq \mathrm{Sym}\,(\Lambda)$ is a quasiprimitive group of type SD with $\mathrm{soc}(U) = T^{d/m}$. The group G acts on Ω with the product action defined in (1.3.2), and acts transitively by conjugation on the d simple direct factors of H.

PA (PRODUCT ACTION): The group $\mathrm{soc}(G) = H = T^d$ is nonregular and nonabelian, with $d \geq 2$; $\Omega = \Lambda^d$; and $T^d \leq G \leq U \wr \mathrm{Sym}(k)$, where $U \leq \mathrm{Sym}(\Lambda)$ is a quasiprimitive group of type AS with $\mathrm{soc}(U) = T$ and U nonregular. The group G acts on Λ^d with the product action defined in (1.3.2), and acts transitively by conjugation on the d simple direct factors of H. If $\omega = (\lambda, \ldots, \lambda) \in \Lambda^d$ then $H_\omega \leq G_\omega \leq U_\lambda \wr \mathrm{Sym}(k)$. Also $\mathcal{P} = \Lambda^d$ is a fixed G-invariant partition of Ω, and for a fixed $\lambda \in \Lambda$, there is a (possibly trivial) G-invariant patition $\mathcal{P}'$ of Ω such that $H_\delta = (T_\lambda)^d$ for some $\delta \in \mathcal{P}'$, and for $\alpha \in \delta$ the point stabiliser H_α is a subdirect product of $(T_\lambda)^d$ (i.e., H_α projects surjectively onto each of the direct factors of $(T_\lambda)^d$).

1.4. Rank 3 groups

We discuss here briefly the quasiprimitive rank 3 groups, which give rise to symmetric, vertex-quasiprimitive graphs with diameter 2 (see Section 6.3). Recall from Section 1.1 that the rank of a permutation group $G \leq \mathrm{Sym}(\Omega)$ is the number of G-orbitals on Ω; hence G has rank 3 if it has exactly two orbits on the set of ordered pairs of distinct elements in Ω.

The following result by P. Cameron gives a relationship between the rank of a primitive permutation group G with nonabelian socle, and the number of simple direct factors in $\mathrm{soc}(G)$.

Theorem 1.4.1. [**10**, Proposition 5.1] *Let G be a primitive group with $\mathrm{soc}(G) = T^d$ for some nonabelian simple group T. If G has rank r, then $d \leq r - 1$.*

Together with Theorem 1.3.1, this implies that if G is primitive with rank 3 then one of the following holds:

(i) $\mathrm{soc}(G)$ is regular and elementary abelian (i.e., G is of type HA);
(ii) $\mathrm{soc}(G) = T$ where T is nonabelian simple (i.e., G is of type AS);
(iii) $\mathrm{soc}(G) = T^2$ where T is nonabelian simple.

The primitive rank 3 groups satisfying (i) are classified by M. Liebeck in [**34**]. Those satisfying (ii) are classified in [**7**] for the case where T is an alternating group, [**28**] for T a classical group, and [**35**] for T an exceptional group of Lie type or a sporadic group. The groups satisfying (iii) are subgroups of a wreath product $U \wr \mathrm{Sym}(2)$ where U is 2-transitive with $\mathrm{soc}(U) = T$, and the classification of all 2-transitive groups (see [**10**]) gives all primitive rank 3 permutation groups in this case.

The quasiprimitive rank 3 groups which are imprimitive are determined by A. Devillers, et.al. in [**15**]. They show that if G is a group which is quasiprimitive and imprimitive with rank 3, then the following conditions are satisfied.

(i) The group G has a unique system $\mathcal{D}$ of blocks.
(ii) The action of G on its block system is faithful (and thus $G^{\mathcal{D}} \cong G$).

(iii) The group G is a subgroup of the wreath product $H \wr X$, where $X \cong G^{\mathcal{D}}$ and $H = G^{\Delta}_{\{\Delta\}}$ for some $\Delta \in \mathcal{D}$, and both H and X are 2-transitive.

(iv) The group G is almost simple.

So the classification of imprimitive quasiprimitive rank 3 groups follows from the classification of 2-transitive groups.

Thus we have:

Theorem 1.4.2. [**15**, Corollary 1.4] *All quasiprimitive rank* 3 *permutation groups are known. They are either primitive, or imprimitive and almost simple.*

CHAPTER 2

Algebraic graph theory

In this chapter we introduce some definitions, notation and relevant results on permutation groups. The material in the first section is standard, and can be found in [**9**]. In the last section we discuss briefly the progress made on Thompson's Conjecture, which may yield examples of symmetric diameter 2 graphs for some of the vertex-quasiprimitive cases. The content of this section can also be found in [**29**] (for Section 2.3), [**40**, Section 4] and [**41**, Section 7] (for Section 2.4).

2.1. Basic concepts

A *graph* Γ consists of a nonempty set $V(\Gamma)$ of nodes or *vertices*, and a set $E(\Gamma)$ of *edges* that connect some (possibly none or all) pairs of distinct vertices. The graph Γ is *finite* if $V(\Gamma)$ is a finite set. Two vertices α and β which are connected by an edge are said to be *adjacent*, and α is called a *neighbour* of β and vice versa. An edge is usually denoted as an unordered pair of adjacent vertices, that is, the edge connecting adjacent vertices α and β is $\{\alpha, \beta\}$. An *arc* is a directed edge and is represented by an ordered pair of adjacent vertices; thus each edge $\{\alpha, \beta\}$ determines two arcs, namely, (α, β) and (β, α). We will sometimes write $\alpha \sim_\Gamma \beta$ to indicate that $\{\alpha, \beta\} \in E(\Gamma)$.

A graph Δ is said to be a *subgraph* of Γ if $V(\Delta) \subseteq V(\Gamma)$ and $E(\Delta) \subseteq E(\Gamma)$. If $S \subseteq V(\Gamma)$, the *induced subgraph* of Γ on S is the graph $[S]$ with $V([S]) = S$ and $E([S]) = \{\{\alpha, \beta\} \in E(\Gamma) \mid \alpha, \beta \in S\}$, i.e., the set of all edges of Γ which join vertices in S.

A *path of length* n in Γ is a sequence $[\gamma_0, \gamma_1, \ldots, \gamma_n]$ of $n+1$ vertices of Γ such that $\{\gamma_i, \gamma_{i+1}\} \in E(\Gamma)$ for all $i \in \{0, \ldots, n\}$ and $\gamma_{i-1} \neq \gamma_{i+1}$ for all $i \in \{1, \ldots, n-1\}$. Hence an edge determines a path of length 1. A graph is *connected* if any two distinct vertices are connected by a path; otherwise, it is *disconnected*. The *distance* between two vertices α and β is the length of the shortest path that joins α and β. The *diameter* of a connected graph is the smallest positive integer d such that any two vertices are connected by a path of length at most d. In particular, a graph has diameter one if every pair of distinct vertices are adjacent; such a graph is also called *complete*. A graph has diameter 2 if it is not complete, that is, if it has at least one pair of distinct vertices which are not adjacent, and if any two nonadjacent vertices α and β have at least one common neighbour.

An *automorphism* of Γ is a bijection x of the set $V(\Gamma)$ which sends adjacent pairs of vertices to adjacent pairs, and nonadjacent pairs to nonadjacent pairs, that is, $\{\alpha^x, \beta^x\} \in E(\Gamma)$ if and only if $\{\alpha, \beta\} \in E(\Gamma)$. The automorphisms of Γ form a group, which we denote by $\mathrm{Aut}\,(\Gamma)$. Any subgroup of $\mathrm{Aut}\,(\Gamma)$ is called an *automorphism group* of Γ. The graph Γ is *vertex-transitive* if for any $\alpha, \beta \in V(\Gamma)$ there is an element $x \in \mathrm{Aut}(\Gamma)$ with $\alpha^x = \beta$. It is *arc-transitive* or *symmetric* if, for any pair of arcs (α, β) and (γ, δ), we can find $y \in \mathrm{Aut}(\Gamma)$ with $\alpha^y = \gamma$ and $\beta^y = \delta$. If the above statements hold when $\mathrm{Aut}(\Gamma)$ is replaced by some subgroup $G \leq \mathrm{Aut}(\Gamma)$, then Γ is, respectively, *G-vertex-transitive* and *G-arc-transitive* (or *G-symmetric*).

It follows from the definitions above that, in a vertex-transitive graph, every vertex has the same number of neighbours, say v. In this case we say that the graph is *regular* with *valency* v. Also, a connected symmetric graph is necessarily vertex-transitive; the converse, however, is generally not true.

The following theorem is a special case of [**9**, Theorem 17.5], and gives a necessary and sufficient condition for G to be symmetric.

Theorem 2.1.1. [**9**, Theorem 17.5] *A graph Γ is G-symmetric for some $G \leq \mathrm{Aut}(\Gamma)$ if and only if G is transitive on $V(\Gamma)$ and, for any $\alpha \in V(\Gamma)$, G_α is transitive on the neighbours of α.*

An *isomorphism* of graphs Γ and Δ is a bijection from $V(\Gamma)$ onto $V(\Delta)$ which maps edges of Γ to edges of Δ, and non-edges of Γ (i.e., non-adjacent pairs of vertices) to non-edges of Δ. If such a map exists then Γ and Δ are *isomorphic* graphs, written as $\Gamma \cong \Delta$.

A *digraph*, or *directed graph*, is a generalisation of a graph, in which two adjacent vertices are connected by arcs instead of edges, and arcs of the form (γ, γ) (which are called *loops*) are allowed. A digraph is a graph if it has no loops, and if (α, β) is an arc whenever (β, α) is an arc.

Let $G \leq \mathrm{Sym}(\Omega)$. To each nontrivial G-orbital Δ (see Section 1.1) we can associate a digraph which has vertex set Ω and arc set Δ, and is called the *orbital digraph* for G associated with Δ. We also denote this digraph by Δ. Note that Δ is a graph if and only if the orbital Δ is self-paired. Clearly, Δ admits G as a subgroup of automorphisms. The next theorem is another characterisation of arc-transitive graphs that follows easily from the preceding discussion.

Theorem 2.1.2. [**40**, Theorem 2.1] *A graph Γ is G-symmetric for some $G \leq \mathrm{Aut}(\Gamma)$ if and only if Γ is an orbital graph for G, namely, for the nontrivial self-paired orbital $\{(\alpha, \beta) \mid \{\alpha, \beta\} \in E(\Gamma)\}$.*

A *rank* 3 *graph* is a graph Γ with an automorphism group G that acts as a rank 3 group on its vertex set. In this case the nontrivial G-orbitals on $V(\Gamma)$ are precisely the arc set of Γ and the set of nonadjacent vertices of Γ. So Γ is an orbital graph for G and is therefore G-symmetric. A connected rank 3 graph has diameter 2. Indeed, if α and β are nonadjacent vertices, then $\mathrm{dist}_\Gamma(\alpha, \beta) = \mathrm{dist}_\Gamma(\alpha^g, \beta^g)$ for any $g \in G$. Since a connected rank 3 graph clearly contains vertices with distance 2, it follows that all pairs of nonadjacent vertices have distance 2, and thus $\mathrm{diam}(\Gamma) = 2$. Recall from Section 1.4 that all quasiprimitive rank 3 groups are known; those which contain an involution give rise to vertex-quasiprimitive symmetric diameter 2 graphs.

2.2. Cayley graphs

Notation. We denote by $G^{\#}$ the set of all nonidentity elements of a group G.

Definition 2.2.1. Let G be a group and let S be a nonempty subset of G. The *Cayley digraph* of G relative to S is the digraph with vertex set G and arc set $\{(g, sg) \mid g \in G, s \in S\}$.

Let Γ be a Cayley digraph as defined above. It is easy to see from the definition above that Γ contains loops if and only if S contains the identity element 1_G. If $s \in S$ then $(1_G, s)$ is an arc of Γ, and $(s, 1_G)$ is also an arc if and only if it can be written as $(g, s'g)$ for some $g \in G$ and $s' \in S$. Hence we must have $1_G = s's$, and $s' = s^{-1}$. This implies that $s^{-1} \in S$ whenever $s \in S$, that is, $S^{-1} = \{s^{-1} \mid s \in S\} = S$. Conversely, if $S^{-1} = S$ then for any $g \in G$ and $s \in S$, (g, sg) and $(g, s^{-1}g)$ are arcs and thus so is (sg, g). This shows that a Cayley digraph is a graph if and only if the set S consists of nonidentity elements and S is closed under taking inverses. We have the following definition.

Definition 2.2.2. Let G be a group and let S be a nonempty subset of $G^{\#}$ such that $S^{-1} = S$. The *Cayley graph* of G relative to S, denoted by $\mathrm{Cay}(G, S)$, is the graph with vertex set G and edges $\{g, sg\}$, for all $g \in G$ and $s \in S$. Also, a subset S of $G^{\#}$ such that $S^{-1} = S$ is called a *Cayley subset* of G.

All Cayley graphs are vertex-transitive graphs, as shown below. For a finite group G and a subset S of G, define $\mathrm{Aut}\,(G, S)$ to be the subgroup of elements of $\mathrm{Aut}\,(G)$ which fix S setwise.

Theorem 2.2.3. [**9**, Proposition 16.2] *Let G be a group and let S be a Cayley subset of G. Then:*

(1) The graph $\mathrm{Cay}(G, S)$ is vertex-transitive. (In particular, G is a subgroup of $\mathrm{Aut}\,(\mathrm{Cay}(G, S))$, acting regularly on itself by right multiplication.)
(2) The group $\mathrm{Aut}\,(G, S)$ is a subgroup of the stabiliser in $\mathrm{Aut}\,(\mathrm{Cay}(G, S))$ of the vertex 1_G.

The following theorem characterises graphs which can be constructed as Cayley graphs, in terms of their automorphism groups.

Theorem 2.2.4. [**9**, Lemma 16.3] *A graph has an automorphism group G acting regularly on $V(\Gamma)$ if and only if $\Gamma \cong \mathrm{Cay}(G,S)$ for some Cayley subset S of G.*

The following is a direct application of the results above.

Lemma 2.2.5. *Let Γ be a Cayley graph $\mathrm{Cay}(G,S)$ for some finite group G and Cayley subset S of G. Then:*

(1) Γ is connected if and only if S generates G. In particular, Γ has diameter 2 if and only if $S \neq G \setminus \{1_G\}$ and $S^2 \cup S = G$.
(2) If $\mathrm{Aut}\,(G,S)$ is transitive on S, then Γ is symmetric.

Proof. To prove (1), recall from the previous section that Γ is connected if and only if any two distinct vertices are connected by a path; equivalently, there is a path between the vertex 1_G and any other vertex g of Γ. Such a path has form $[1_G, s_1, s_2s_1, \ldots, s_ns_{n-1}\cdots s_1]$, for some integer $n \geq 1$ and elements $s_1, \ldots, s_n \in S$ whose product is g. So Γ is connected if and only if each element of G is expressible as a product of elements of S, i.e., S generates G. Clearly, the set of all neighbours of the vertex 1_G is S, and $\mathrm{diam}(\Gamma) \geq 2$ if and only if $S \subset G \setminus \{1_G\}$. Also, $S^2 = \{s_1s_2 \mid s_1, s_2 \in S\}$ contains all vertices at distance 2 from 1_G, and it follows that $\mathrm{diam}(\Gamma) = 2$ if and only if $S \neq G \setminus \{1_G\}$ and $S^2 \cup S = G$.

Statement (2) follows immediately from Theorems 2.1.1 and 2.2.4. □

Remark. Observe that the condition $S^{-1} = S$ implies that $|S^2| \leq |S|^2 - |S| + 1$. Hence if $G = S \cup S^2$ then $|G| \leq |S|^2 + 1$. This fact will be frequently used.

2.3. Products of graphs

In this section we describe three different ways of combining two graphs to form a third. These will be used later to construct some infinite families of symmetric diameter 2 graphs (see Examples 2.4.1 and 2.4.2).

Definition 2.3.1. Let Γ and Δ be graphs.

(1) The *lexicographic product* $\Gamma[\Delta]$ of Γ and Δ is the graph with vertex set $V(\Gamma) \times V(\Delta)$, and with $(\gamma, \delta) \sim_{\Gamma[\Delta]} (\gamma', \delta')$ if and only if either $\gamma \sim_\Gamma \gamma'$, or $\gamma = \gamma'$ and $\delta \sim_\Delta \delta'$.
(2) The *direct product* $\Gamma \times \Delta$ of Γ and Δ is the graph with vertex set $V(\Gamma) \times V(\Delta)$, and with $(\gamma, \delta) \sim_{\Gamma \times \Delta} (\gamma', \delta')$ if and only if $\gamma \sim_\Gamma \gamma'$ and $\delta \sim_\Delta \delta'$.
(3) The *Cartesian product* $\Gamma \,\square\, \Delta$ of Γ and Δ is the graph with vertex set $V(\Gamma) \times V(\Delta)$, and with $(\gamma, \delta) \sim_{\Gamma \square \Delta} (\gamma', \delta')$ if and only if either $\gamma = \gamma'$ and $\delta \sim_\Delta \delta'$, or $\delta = \delta'$ and $\gamma \sim_\Gamma \gamma'$.

Each of these products is illustrated in Figure 1.

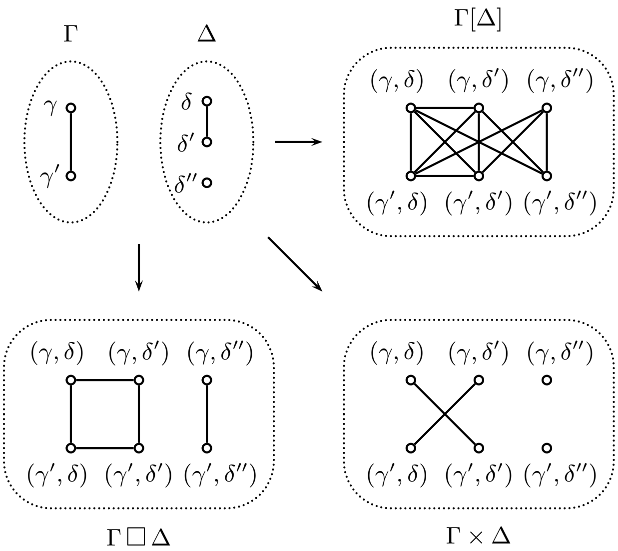

FIGURE 1. Lexicographic, direct, and Cartesian product of graphs

It is easy to see that for any $g \in \mathrm{Aut}\,(\Gamma)$ and $h \in \mathrm{Aut}\,(\Delta)$, the map

$$\begin{aligned} V(\Gamma) \times V(\Delta) &\to V(\Gamma) \times V(\Delta) \\ (\gamma, \delta) &\mapsto (\gamma, \delta)^{(g,h)} := \left(\gamma^g, \delta^h\right) \end{aligned} \tag{2.3.1}$$

is an automorphism of $\Gamma[\Delta]$, $\Gamma \times \Delta$, and $\Gamma \,\square\, \Delta$. Hence $\mathrm{Aut}\,(\Gamma) \times \mathrm{Aut}\,(\Delta) \leq \mathrm{Aut}\,(\Sigma)$, where Σ is one of $\Gamma[\Delta]$, $\Gamma \times \Delta$, and $\Gamma \,\square\, \Delta$, acting on $V(\Sigma)$ via the map (2.3.1).

Observe also that the lexicographic product $\Gamma[\Delta]$ can be constructed by replacing each vertex γ in Γ by a copy Δ_γ of Δ, and each edge $\{\alpha, \beta\}$ of Γ by all possible edges $\{(\alpha, \delta), (\beta, \delta')\}$ where $\delta \in \Delta_\alpha$ and $\delta' \in \Delta_\beta$. For any $g \in \mathrm{Aut}\,(\Gamma)$ and $\overline{h} \in J$, where $J := \prod_{\alpha \in V(\Gamma)} \mathrm{Aut}\,(\Delta_\alpha)$, define the map

$$\begin{aligned} V(\Gamma) \times V(\Delta) &\to V(\Gamma) \times V(\Delta) \\ (\gamma, \delta) &\mapsto (\gamma, \delta)^{(g,\overline{h})} := \left(\gamma^g, \delta^{h(\gamma^g)}\right), \end{aligned} \tag{2.3.2}$$

where $h(\gamma^g)$ is the component of $\overline{h}$ that belongs to $\mathrm{Aut}\,(\Delta_{\gamma^g})$. Then (2.3.2) defines an action of $J \rtimes \mathrm{Aut}\,(\Gamma) \cong \mathrm{Aut}\,(\Delta) \wr \mathrm{Aut}\,(\Gamma)$ on $V(\Gamma) \times V(\Delta)$ which is also an automorphism of $\Gamma[\Delta]$. Hence $\mathrm{Aut}\,(\Delta) \wr \mathrm{Aut}\,(\Gamma) \leq \mathrm{Aut}\,(\Gamma[\Delta])$.

We now proceed to determine necessary and sufficient conditions in order for each of the graph products in Definition 2.3.1 to have diameter 2.

Lemma 2.3.2. *Let Γ and Δ be graphs, each with at least two vertices for (1) and (3) and at least three vertices for (2). Then:*

(1) $\mathrm{diam}(\Gamma[\Delta]) = 2$ *if and only if Γ is connected with diameter at most two and at least one of Γ and Δ is not a complete graph.*

(2) $\operatorname{diam}(\Gamma \times \Delta) = 2$ *if and only if* Γ *and* Δ *are both connected with diameter at most two, and every edge in* Γ *and in* Δ *lies in a triangle of* Γ *and of* Δ*, respectively.*

(3) $\operatorname{diam}(\Gamma \,\Box\, \Delta) = 2$ *if and only if* Γ *and* Δ *are both complete graphs.*

Proof. To prove (1), suppose that $\operatorname{diam}(\Gamma) \leq 2$ and either Γ or Δ is not complete. We consider each case separately.

Case 1.1: Assume that Γ is not complete. Then $\operatorname{diam}(\Gamma) = 2$ and there are distinct $\gamma, \gamma' \in V(\Gamma)$ which are not adjacent. It follows from Definition 2.3.1 that, for any $\delta \in V(\Delta)$, we have $(\gamma, \delta) \nsim_{\Gamma[\Delta]} (\gamma', \delta')$, and thus $\operatorname{diam}(\Gamma[\Delta]) \geq 2$. Let (α, β) and (α', β') be any pair of distinct nonadjacent vertices of $\Gamma[\Delta]$. Then again by Definition 2.3.1 we have $\alpha \nsim_\Gamma \alpha'$, and since Γ has diameter 2 there is an $\alpha'' \in V(\Gamma)$ such that $\alpha \sim_\Gamma \alpha'' \sim_\Gamma \alpha'$. It follows that $(\alpha, \beta) \sim_{\Gamma[\Delta]} (\alpha'', \beta) \sim_{\Gamma[\Delta]} (\alpha', \beta')$, and so $\operatorname{diam}(\Gamma[\Delta]) = 2$.

Case 1.2: Assume that Γ is complete. Then $\operatorname{diam}(\Delta) = 2$, and thus there are distinct and nonadjacent $\delta, \delta' \in V(\Delta)$. For any $\gamma \in V(\Delta)$ the vertices (γ, δ) and (γ, δ') are distinct and nonadjacent in $\Gamma[\Delta]$, so that $\operatorname{diam}(\Gamma[\Delta]) \geq 2$. Let $(\alpha, \beta), (\alpha', \beta')$ be any pair of distinct nonadjacent vertices of $V(\Gamma[\Delta])$. Since Γ is complete, either $\alpha \sim_\Gamma \alpha'$ or $\alpha = \alpha'$; if $\alpha \sim_\Gamma \alpha'$ then $(\alpha, \beta) \sim_{\Gamma[\Delta]} (\alpha', \beta')$, a contradiction. So $\alpha = \alpha'$, which implies that β and β' are distinct and nonadjacent in Δ. Any $\alpha'' \in V(\Gamma)$ with $\alpha'' \neq \alpha$ is adjacent to α, so that $(\alpha, \beta) \sim_{\Gamma[\Delta]} (\alpha'', \beta) \sim_{\Gamma[\Delta]} (\alpha, \beta')$. Therefore $\operatorname{diam}(\Gamma[\Delta]) = 2$.

Conversely, suppose that $\operatorname{diam}(\Gamma[\Delta]) = 2$. Let γ, γ' be distinct vertices of Γ, and let $\delta \in V(\Delta)$. Then (γ, δ) and (γ', δ) are distinct vertices of $\Gamma[\Delta]$, and hence they are either adjacent or are connected by a path of length 2. If $(\gamma, \delta) \sim_{\Gamma[\Delta]} (\gamma', \delta)$ then $\gamma \sim_\Gamma \gamma'$ by Definition 2.3.1. If $(\gamma, \delta) \nsim_{\Gamma[\Delta]} (\gamma', \delta)$ then $\gamma \nsim_\Gamma \gamma'$, and there exists $(\gamma'', \delta'') \in V(\Gamma[\Delta])$ such that $(\gamma, \delta) \sim_{\Gamma[\Delta]} (\gamma'', \delta'') \sim_{\Gamma[\Delta]} (\gamma', \delta)$. Hence $\gamma'' \neq \gamma, \gamma'$, and $\gamma \sim_\Gamma \gamma'' \sim_\Gamma \gamma'$. Thus $\operatorname{diam}(\Gamma) \leq 2$. If Γ and Δ are both complete then $\Gamma[\Delta]$ is complete; since $\operatorname{diam}(\Gamma[\Delta]) = 2$, it follows that either Γ or Δ is not complete. This ends the proof of (1).

To prove (2), suppose that Γ and Δ have diameter at most two, and that every edge in Γ and in Δ lies in a triangle. Observe that $\Gamma \times \Delta$ contains distinct nonadjacent vertices (for instance, the vertices (γ, δ) and (γ, δ'), where $\delta \neq \delta'$), so $\operatorname{diam}(\Gamma \times \Delta) \geq 2$. Let (α, β) and (α', β') be distinct nonadjacent vertices of $\Gamma \times \Delta$. It follows from Definition 2.3.1 that one of the following holds: $\alpha = \alpha'$ and $\beta \neq \beta'$; $\beta = \beta'$ and $\alpha \neq \alpha'$; $\alpha \nsim_\Gamma \alpha'$; or $\beta \nsim_\Delta \beta'$. Since Γ and Δ both have diameter at most two, it follows that for each of these cases there exist $\alpha'' \in V(\Gamma)$ and $\beta'' \in V(\Delta)$ such that $\alpha \sim_\Gamma \alpha'' \sim_\Gamma \alpha'$ and $\beta \sim_\Gamma \beta'' \sim_\Gamma \beta'$. Hence $(\alpha, \beta) \sim_{\Gamma \times \Delta} (\alpha'', \beta'') \sim_{\Gamma \times \Delta} (\alpha', \beta')$, and therefore $\operatorname{diam}(\Gamma \times \Delta) = 2$.

Now suppose that $\operatorname{diam}(\Gamma \times \Delta) = 2$. Clearly the complete graph has diameter less than two and has the property that every edge lies in a triangle, so assume that either Γ or Δ is not complete. Without loss of generality suppose that Γ is not complete. Let $\gamma, \gamma' \in V(\Gamma)$ be distinct, and let $\delta \in V(\Delta)$. Then $(\gamma, \delta), (\gamma', \delta)$ are distinct nonadjacent vertices of $\Gamma \times \Delta$, and there exists $(\gamma'', \delta'') \in \Gamma \times \Delta$ such that $(\gamma, \delta) \sim_{\Gamma \times \Delta} (\gamma'', \delta'') \sim_{\Gamma \times \Delta} (\gamma', \delta)$. It follows from Definition 2.3.1 that $\gamma \sim_\Gamma \gamma'' \sim_\Gamma \gamma'$. If $\gamma \nsim_\Gamma \gamma'$ then $[\gamma, \gamma'', \gamma']$ is a path of length 2 in Γ, and since γ, γ' are arbitrary we conclude that $\mathrm{diam}(\Gamma) = 2$. If $\gamma \sim_\Gamma \gamma'$ then $[\gamma, \gamma'', \gamma', \gamma]$ is a triangle in $\Gamma \times \Delta$, and thus every edge of Γ lies in a triangle. If Δ is not a complete graph then using similar arguments we can show that $\mathrm{diam}(\Delta) = 2$ and every edge of Δ lies in a triangle. This proves (2).

Finally we prove (3). Suppose that Γ and Δ are complete graphs. The graph $\Gamma \,\square\, \Delta$ contains distinct nonadjacent vertices (such as (γ, δ) and (γ', δ'), where $\gamma \neq \gamma'$ and $\delta \neq \delta'$), so $\mathrm{diam}(\Gamma \,\square\, \Delta) \geq 2$. Now, by Definition 2.3.1, two vertices $(\gamma, \delta), (\gamma', \delta')$ of $\Gamma \,\square\, \Delta$ are distinct and nonadjacent if and only if one of the following holds: $\gamma \nsim_\Gamma \gamma'$, $\delta \nsim_\Delta \delta'$, or $\gamma \neq \gamma'$ and $\delta \neq \delta'$. Since both Γ and Δ are complete the last case must hold, and in particular $\gamma \sim_\Gamma \gamma'$ and $\delta \sim_\Delta \delta'$. Hence $(\gamma, \delta) \sim_{\Gamma \square \Delta} (\gamma, \delta') \sim_{\Gamma \square \Delta} (\gamma', \delta')$, and therefore $\mathrm{diam}(\Gamma \,\square\, \Delta) = 2$.

Conversely, suppose that $\mathrm{diam}(\Gamma \,\square\, \Delta) = 2$. Let γ, γ' and δ, δ' be pairs of distinct vertices of Γ and of Δ, respectively. Then (γ, δ) and (γ', δ') are distinct and nonadjacent in $\Gamma \,\square\, \Delta$, and there exists $(\gamma'', \delta'') \in V(\Gamma \,\square\, \Delta)$ such that $(\gamma, \delta) \sim_{\Gamma \square \Delta} (\gamma'', \delta'') \sim_{\Gamma \square \Delta} (\gamma', \delta')$. Then either $(\gamma'', \delta'') = (\gamma, \delta')$ or $(\gamma'', \delta'') = (\gamma', \delta)$. Hence $\gamma \sim_\Gamma \gamma'$ and $\delta \sim_\Delta \delta'$. Therefore Γ and Δ are complete graphs, which proves (3). $\square$

The next result gives sufficient (but not necessary) conditions in order for the products in Definition 2.3.1 to be symmetric. A graph is said to be *empty* if it contains no edges.

Lemma 2.3.3. *Let Γ and Δ be graphs.*

(1) If Γ and Δ are both symmetric and at least one of them is an empty graph, then the lexicographic product $\Gamma[\Delta]$ is symmetric. In particular, $\Gamma[\Delta]$ is G-symmetric for the group $G := \mathrm{Aut}\,(\Delta) \wr \mathrm{Aut}\,(\Gamma)$.

(2) If Γ and Δ are both symmetric then the direct product $\Gamma \times \Delta$ is symmetric. In particular, $\Gamma \times \Delta$ is H-symmetric where $H := \mathrm{Aut}\,(\Gamma) \times \mathrm{Aut}\,(\Delta)$.

(3) If Γ and Δ are both symmetric and $\Gamma \cong \Delta$, then the Cartesian product $\Gamma \,\square\, \Delta$ is symmetric. In particular, $\Gamma \,\square\, \Delta$ is K-symmetric for the group $K := (\mathrm{Aut}\,(\Gamma) \times \mathrm{Aut}\,(\Delta)) \rtimes \mathbb{Z}_2$.

PROOF. To avoid confusion we shall denote $(\gamma, \delta) \in V(\Gamma) \times V(\Delta)$ by $\gamma\delta$.

We first show (1). Recall from the discussion before Lemma 2.3.2 that the group $J := \prod_{x \in V(\Gamma)} \mathrm{Aut}\,(\Delta_x)$ is a subgroup of $\mathrm{Aut}\,(\Gamma[\Delta])$, with the action on $V(\Gamma[\Delta])$ given in (2.3.2). If both Γ and Δ are empty graphs then $\Gamma[\Delta]$ is empty, and is therefore G-symmetric, so from now on assume that one of Γ and Δ is not empty. We consider each case separately.

Case 1.1: Suppose that Γ is not an empty graph. Then Δ is empty. If $(\alpha\beta, \alpha'\beta')$ and $(\gamma\delta, \gamma'\delta')$ are distinct arcs of $\Gamma[\Delta]$, then $\alpha \sim_\Gamma \alpha$ and $\gamma \sim_\Gamma \gamma'$, possibly $\{\alpha, \alpha'\} = \{\gamma, \gamma'\}$. (Indeed, by Definition 2.3.1 either $\alpha \sim_\Gamma \alpha'$, or $\alpha = \alpha'$ and $\beta \sim_\Delta \beta'$; since Δ is empty the first case must hold, and similarly for γ and γ'.) Since Γ is symmetric there exists $g \in \mathrm{Aut}(\Gamma)$ such that $(\alpha, \alpha')^g = (\gamma, \gamma')$. Let $\sigma, \sigma' \in \mathrm{Aut}(\Delta)$ such that $\beta^\sigma = \delta$ and $(\beta')^{\sigma'} = \delta'$, and take $\overline{h} \in J$ such that $h(\alpha^g) = \sigma$ and $h((\alpha')^g) = \sigma'$. Then $(g, \overline{h}) \in G \leq \mathrm{Aut}(\Gamma[\Delta])$, with

$$(\alpha\beta, \alpha'\beta')^{(g,\overline{h})} = \left(\alpha^g \beta^{h(\alpha^g)}, \alpha'^g \beta'^{h(\alpha'^g)}\right) = (\gamma\delta, \gamma'\delta').$$

Therefore $\Gamma[\Delta]$ is G-symmetric.

Case 1.2: Suppose that Δ is not empty, so that Γ is empty. Again let $(\alpha\beta, \alpha'\beta')$ and $(\gamma\delta, \gamma'\delta')$ be distinct arcs of $\Gamma[\Delta]$. Then $\alpha = \alpha'$, $\gamma = \gamma'$, $\beta \sim_\Delta \beta'$, and $\delta \sim_\Delta \delta'$. Since Δ is symmetric there exists $\rho \in \mathrm{Aut}(\Delta)$ such that $(\beta, \beta')^\rho = (\delta, \delta')$. Take $g \in \mathrm{Aut}(\Gamma)$ such that $\alpha^g = \gamma$, and $\overline{h} \in J$ such that $h(\alpha^g) = \rho$. Then as in Case 1.1 we have $(g, \overline{h}) \in G \leq \mathrm{Aut}(\Gamma[\Delta])$ with

$$(\alpha\beta, \alpha'\beta')^{(g,\overline{h})} = \left(\alpha^g \beta^{h(\alpha^g)}, \alpha^g \beta'^{h(\alpha'^g)}\right) = (\gamma\delta, \gamma\delta'),$$

and again $\Gamma[\Delta]$ is G-symmetric. This completes the proof of (1).

To prove (2) let $(\alpha\beta, \alpha'\beta')$ and $(\gamma\delta, \gamma'\delta')$ be distinct arcs of $\Gamma \times \Delta$. Then $\alpha \sim_\Gamma \alpha'$, $\gamma \sim_\Gamma \gamma'$, $\beta \sim_\Delta \beta'$, and $\delta \sim_\Delta \delta'$, and so there exist $g \in \mathrm{Aut}(\Gamma)$ and $h \in \mathrm{Aut}(\Delta)$ with $(\alpha, \alpha')^g = (\gamma, \gamma')$ and $(\beta, \beta')^h = (\delta, \delta')$. Hence $(g, h) \in H \leq \mathrm{Aut}(\Gamma \times \Delta)$, and

$$(\alpha\beta, \alpha'\beta')^{(g,h)} = \left(\alpha^g \beta^h, \alpha'^g \beta'^h\right) = (\gamma\delta, \gamma'\delta').$$

Therefore $\Gamma \times \Delta$ is H-symmetric.

We now prove (3). Let $(\alpha\beta, \alpha'\beta')$ and $(\gamma\delta, \gamma'\delta')$ be distinct arcs of $\Gamma \,\square\, \Delta$, and let $\tau : \Gamma \to \Delta$ be a graph isomorphism. We have two cases.

Case 3.1: Suppose that the two arcs have no common vertex. Then one of the following holds: (i) $\alpha = \alpha'$ and $\gamma = \gamma'$, or (ii) $\beta = \beta'$ and $\delta = \delta'$. If (i) holds then $\beta \sim_\Gamma \beta'$ and $\delta \sim_\Delta \delta'$, and there exist $g \in \mathrm{Aut}(\Gamma)$ and $h \in \mathrm{Aut}(\Delta)$ with $\alpha^g = \gamma$ and $(\beta, \beta')^h = (\delta, \delta')$. Then $(g, h) \in \mathrm{Aut}(\Gamma \,\square\, \Delta)$ and $(\alpha\beta, \alpha'\beta')^{(g,h)} = (\gamma\delta, \gamma'\delta')$. If (ii) holds then the same result is obtained using similar arguments.

Case 3.2: Suppose that the two arcs have a common vertex. Then either: (i) $\alpha = \alpha'$ and $\delta = \delta'$, or (ii) $\beta = \beta'$ and $\gamma = \gamma'$. If (i) holds then $\beta \sim_\Delta \beta'$ and $\gamma \sim_\Gamma \gamma'$. Take $g \in \mathrm{Aut}(\Gamma)$ and $h \in \mathrm{Aut}(\Delta)$ such that $\alpha^g = \delta^{\tau^{-1}}$ and $(\beta, \beta')^h = (\gamma, \gamma')^\tau$. Define the map $\zeta : V(\Gamma \,\square\, \Delta) \to V(\Gamma \,\square\, \Delta)$ by $(xy)^\zeta := y^{\tau^{-1}} x^\tau$ for all $x \in V(\Gamma)$ and $y \in V(\Delta)$. It is easy to show that $\zeta \in \mathrm{Aut}(\Gamma \,\square\, \Delta)$. We have

$$(\alpha\beta, \alpha\beta')^{(g,h)\zeta} = \left(\alpha^g \beta^h, \alpha^g \beta'^h\right)^\zeta = \left(\delta^{\tau^{-1}} \gamma^\tau, \delta^{\tau^{-1}} \gamma'^\tau\right)^\zeta = (\gamma\delta, \gamma'\delta).$$

If (ii) holds then using similar arguments we can find $g' \in \mathrm{Aut}(\Gamma)$ and $h' \in \mathrm{Aut}(\Delta)$ with $(\alpha\beta, \alpha'\beta)^{(g',h')\zeta} = (\gamma\delta, \gamma'\delta)$. Together with Case 3.1 this implies that $\Gamma \,\square\, \Delta$ is K-symmetric, which proves (3). $\square$

We denote the complete graph on n vertices by K_n, and the empty graph with n vertices by $\overline{K_n}$.

A graph is said to be *bipartite* if its vertex set can be partitioned into two parts P and Q such that no two vertices in the same part are adjacent. It is said to be *complete bipartite* if, in addition to the above, every vertex in P is adjacent to every vertex in Q, and vice versa. We denote the complete bipartite graph by $K_{m,n}$, where $m = |P|$ and $n = |Q|$.

In the case where $m = n$, the complete bipartite graph $K_{n,n}$ is isomorphic to the lexicographic product $K_2\left[\overline{K_n}\right]$, which is symmetric with diameter 2 by Lemmas 2.3.2 and 2.3.3. As we show in Lemma 2.3.4, a bipartite graph which is symmetric with diameter 2 is necessarily isomorphic to $K_{n,n}$ for some $n \geq 2$.

Lemma 2.3.4. *Let Γ be a symmetric graph with diameter 2. If Γ is bipartite, then Γ is a complete bipartite graph $K_{n,n}$ for some $n \geq 2$.*

PROOF. Let P and Q be the two elements of the bipartition, and let $\gamma \in P$ and $\gamma' \in Q$. Then either γ and γ' are adjacent, or they are connected by a path of length 2, say $\{\gamma, \delta, \gamma'\}$. The latter is impossible, since δ must belong to either P or Q, but by the definition of a bipartite graph no two vertices in P or in Q are joined by an edge. So every vertex in P is adjacent to every vertex in Q. Since Γ is symmetric it must be regular, and thus $|P| = |Q| = n$ for some n. Therefore $\Gamma = K_{n,n}$. □

Remark. If both Γ and Δ are nonempty graphs, it is unclear whether the lexicographic product $\Gamma[\Delta]$ is M-symmetric for any subgroup M of $\mathrm{Aut}\,(\Gamma[\Delta])$. The converse, however, is clearly not true: for instance, if Γ and Δ are both complete graphs, then $\Gamma[\Delta]$ is also a complete graph and is clearly symmetric. For the Cartesian product of Γ and Δ, if $\Gamma \,\square\, \Delta$ is symmetric it is not necessary that $\Gamma \cong \Delta$, unless Γ and Δ are both complete, as shown in Lemma 2.3.5 below. For example, if C_4 denotes the 4-cycle then the graph $C_4 \,\square\, K_2$ is the cube, which is symmetric.

Lemma 2.3.5. *The graph $K_m \,\square\, K_n$ is symmetric if and only if $m = n$.*

PROOF. If $m = n$ then $K_m \,\square\, K_n$ is symmetric by Lemma 2.3.3. Suppose that $\Sigma := K_m \,\square\, K_n$ is symmetric. As in the proof of Lemma 2.3.3 we denote $(\gamma, \delta) \in V(K_m) \times V(K_n)$ by $\gamma\delta$. Fix $\gamma\delta \in V(\Sigma)$, and let Γ and Δ be the subgraphs of Σ induced on $\{\gamma'\delta \mid \gamma' \in V(K_m)\}$ and $\{\gamma\delta' \mid \delta' \in V(K_n)\}$, respectively. Then $\Gamma \cong K_m$ and $\Delta \cong K_n$, and moreover any complete subgraph of Σ which contains $\gamma\delta$ must be a subgraph of either Γ or Δ. (Indeed, if Λ is a complete subgraph of Σ which contains $\gamma\delta$, then $V(\Lambda) \subseteq V(\Gamma) \cup V(\Delta)$. Clearly any vertex in $V(\Gamma) \setminus \{\gamma\delta\}$ is not adjacent to any vertex in $V(\Delta) \setminus \{\gamma\delta\}$, so either $V(\Lambda) \subseteq V(\Gamma)$ or $V(\Lambda) \subseteq V(\Delta)$. Since Σ is symmetric, for any $\gamma'\delta \in V(\Gamma) \setminus \{\gamma\delta\}$ and $\gamma\delta' \in V(\Delta)$ there exists $\sigma \in \mathrm{Aut}\,(\Sigma)_{\gamma\delta}$ such that $(\gamma'\delta)^\sigma = \gamma\delta'$. Then $\sigma(\Gamma)$ is a complete subgraph of Δ, so $n \geq m$. By a similar argument we have $m \geq n$. Therefore $m = n$, which completes the proof. □

2.4. Normal quotients

Notation. If Γ is a graph and G is a group acting on $V(\Gamma)$, we denote by G^Γ the group induced by the action of G on $V(\Gamma)$.

Let Γ be a graph, G a vertex-transitive subgroup of $\mathrm{Aut}\,(\Gamma)$, and $\mathcal{P}$ a G-invariant partition of $V(\Gamma)$ (see Section 1.1). The *quotient graph* of Γ relative to $\mathcal{P}$ is the graph $\Gamma_\mathcal{P}$ whose vertices are the parts of $\mathcal{P}$, and whose edges are the pairs $\{P, P'\}$ such that there is at least one edge of Γ which joins a vertex in P and a vertex in P'. Hence the graph $\Gamma_\mathcal{P}$ can be obtained from Γ by collapsing into one vertex all the vertices of Γ belonging to the same part P, with the corresponding effect on the edges joining vertices in different parts (all edges between vertices in the same part are ignored; see Figure 2). The quotient graph $\Gamma_\mathcal{P}$ is *nontrivial* if it has more than one vertex, and is *proper* if $|V(\Gamma_\mathcal{P})| < |V(\Gamma)|$. Thus $\Gamma_\mathcal{P}$ is nontrivial and proper if and only if $\mathcal{P}$ is a nontrivial partition. In particular, if G acts primitively on $V(\Gamma)$, then Γ has no proper nontrivial quotient graph corresponding to a G-invariant partition.

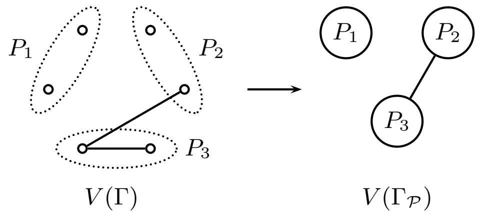

FIGURE 2. Quotient graph of Γ with respect to the partition $\mathcal{P}$

It is known that quotient graphs "inherit" some of the properties of the original graph. For instance, $\Gamma_\mathcal{P}$ is connected if the original graph Γ is connected, and in this case $\mathrm{diam}(\Gamma_\mathcal{P}) \leq \mathrm{diam}(\Gamma)$. We have $G^\mathcal{P} \leq \mathrm{Aut}\,(\Gamma_\mathcal{P})$, and if Γ is G-vertex-transitive or G-symmetric, then $\Gamma_\mathcal{P}$ is $G^\mathcal{P}$-vertex-transitive and $G^\mathcal{P}$-symmetric, respectively.

If Γ is connected and G-symmetric then all edges of Γ join vertices which lie in different parts of $\mathcal{P}$; that is, there is no edge joining vertices which belong in the same part. In other words, the induced subgraph (see Section 2.1) on any $P \in \mathcal{P}$ is an empty graph.

Recall from Theorem 1.2.2 in Section 1.1 that the set of orbits of a normal subgroup N of G forms a G-invariant partition; the quotient graph relative to such a partition is called a *G-normal quotient* of Γ (or simply *normal quotient*, if no confusion arises), and is denoted by Γ_N. It is easy to see that Γ_N is nontrivial exactly when N is intransitive on $V(\Gamma)$, and is proper if and only if N does not lie in the kernel of the action of G on $V(\Gamma)$. One property of normal quotients which is not always guaranteed for ordinary quotient graphs is the following: If Γ is a connected G-symmetric graph and $N \lhd G$, then Γ is an *ℓ-multicover* of Γ_N for some positive integer ℓ, that is, for any two adjacent N-orbits P and P', each vertex of Γ belonging in P has exactly ℓ neighbours in P', and vice versa.

The existence of G-normal quotients depends on the choice of the automorphism group G, as illustrated in Examples 2.4.2 and 2.4.3 below.

Example 2.4.1. Let $\Sigma := \Gamma[\Delta]$, where Γ and Δ are nontrivial graphs, and let $G := \mathrm{Aut}\,(\Delta) \wr \mathrm{Aut}\,(\Gamma) = \mathrm{Aut}\,(\Delta)^{|V(\Gamma)|} \rtimes \mathrm{Aut}\,(\Gamma)$, acting as in (2.3.2). Take $N := \mathrm{Aut}\,(\Delta)^{|V(\Gamma)|} \lhd G$. Then the N-orbits are the sets $\{(\gamma, \delta) \mid \delta \in V(\Delta)\} = V(\Delta_\gamma)$ for each $\gamma \in V(\Gamma)$ (see discussion before Lemma 2.3.2). It follows that $\Sigma_N \cong \Gamma$. The graph Σ is an ℓ-multicover of Σ_N, where $\ell = |V(\Delta)|$.

Consider the special case where $\Gamma = K_m$ and $\Delta = \overline{K_n}$ with $m, n \geq 2$. In this case $G = \mathrm{Sym}\,(n) \wr \mathrm{Sym}\,(m)$ and $N = \mathrm{Sym}\,(n)^m$. By Lemma 2.3.2 the graph Σ has diameter 2, and by Lemma 2.3.3 the graph Σ is G-symmetric. Furthermore Σ is an n-multicover of Σ_N. □

Example 2.4.2. Let $\Sigma := \Gamma \times \Delta$, where Γ and Δ are nontrivial graphs with at least three vertices each, and let $G := \mathrm{Aut}\,(\Gamma) \times \mathrm{Aut}\,(\Delta)$. Let $M := \mathrm{Aut}\,(\Gamma)$ and $N := \mathrm{Aut}\,(\Delta)$. Then the M-orbits are the sets $\{(\gamma, \delta) \mid \gamma \in V(\Gamma)\}$ for each $\delta \in V(\Delta)$, while the N-orbits are $\{(\gamma', \delta') \mid \delta' \in V(\Delta)\}$ for each $\gamma' \in V(\Gamma)$. It follows that $\Sigma_M \cong \Delta$ and $\Sigma_N \cong \Gamma$. The graph Σ is an ℓ_1-multicover of Σ_M where $\ell_1 = \mathrm{val}\,(\Sigma)$, and an ℓ_2-multicover of Σ_N where $\ell_2 = \mathrm{val}\,(\Delta)$.

If $\Gamma = K_m$ and $\Delta = K_n$, where $m, n \geq 3$, then $G = \mathrm{Sym}\,(m) \times \mathrm{Sym}\,(n)$, $M = \mathrm{Sym}\,(m)$, and $N = \mathrm{Sym}\,(n)$. Then Σ is G-symmetric with diameter 2 by Lemmas 2.3.2 and 2.3.3. The graphs Σ_M and Σ_N are G-normal quotients isomorphic to K_n and K_m, respectively; moreover, Σ is an $(m-1)$-multicover of Σ_M and an $(n-1)$-cover of Σ_N. If $m = n$ then $\mathrm{Aut}\,(\Sigma) = \mathrm{Sym}\,(n) \wr \mathbb{Z}_2$, which has rank 3 action on $V(\Sigma)$. The graph Σ does not have a proper nontrivial H-normal quotient for $H = \mathrm{Aut}\,(\Sigma)$. □

Example 2.4.3. Let $\Sigma := \Gamma \,\square\, \Delta$ and $G := \mathrm{Aut}\,(\Gamma) \times \mathrm{Aut}\,(\Delta)$. Taking $M := \mathrm{Aut}\,(\Gamma)$ and $N := \mathrm{Aut}\,(\Delta)$, we again get the G-normal quotients $\Sigma_M \cong \Delta$ and $\Sigma_N \cong \Gamma$. Observe that the induced subgraph on each M-orbit is isomorphic to Γ and the induced subgraph on each N-orbit is isomorphic to Δ. Note that Σ is not G-symmetric for our choice of G. If we take $\Gamma = K_n = \Delta$ for some $n \geq 2$, then it follows from Lemmas 2.3.2 and 2.3.3 that Σ has diameter 2 and is H-symmetric for $H = \mathrm{Aut}\,(\Gamma) \wr \mathbb{Z}_2$, and as in Example 2.4.2, the group H has rank 3 action on $V(\Sigma)$. However, Σ has no nontrivial H-normal quotient. □

Lemma 2.4.4 and Proposition 2.4.5 give some properties of G-symmetric graphs Γ with a proper nontrivial G-normal quotient.

Lemma 2.4.4. *Let Γ be a G-symmetric graph with diameter 2, and suppose that there is an $N \lhd G$ which acts intransitively and nontrivially on $V(\Gamma)$. Then Γ is an ℓ-multicover of Γ_N for some $\ell \geq 2$.*

PROOF. Let $\alpha \in V(\Gamma)$ and $\alpha' \in \alpha^N \setminus \{\alpha\}$. Then $\alpha \nsim_\Gamma \alpha'$ by the discussion above. By our assumption we can find a third vertex β such that $\alpha \sim_\Gamma \beta \sim_\Gamma \alpha'$. So $\beta^N \neq \alpha^N$, and β is adjacent to at least two different vertices in α^N. Therefore $\ell \geq 2$. □

Proposition 2.4.5. *Let Γ be a G-symmetric graph with diameter 2, and suppose that there is an $N \lhd G$ which acts intransitively and nontrivially on $V(\Gamma)$. Then one of the following holds:*

(1) $\Gamma \cong \Gamma_N\left[\overline{K_n}\right]$, where $\mathrm{diam}(\Gamma_N) \leq 2$ and $n := |\gamma^N| \geq 2$ for any $\gamma \in V(\Gamma)$.
(2) N has at least three orbits in $V(\Gamma)$ and every edge of Γ_N lies in a triangle.

PROOF. If N has exactly two orbits in $V(\Gamma)$, then $\Gamma_N \cong K_2$ and Γ is bipartite with the two N-orbits forming the bipartition (since the N-orbits contain no edge of Γ). It follows from Lemma 2.3.4 that $\Gamma \cong K_{n,n} \cong K_2\left[\overline{K_n}\right]$ where n is the length of an N-orbit, with $n \geq 2$ since the action of N is nontrivial.

Assume from now on that N has at least three orbits, and set $n := |\gamma^N|$ for any $\gamma \in V(\Gamma)$. Suppose first that Γ is an n-multicover of Γ_N. Then $\alpha \sim_\Gamma \beta$ if and only if $\alpha^N \sim_{\Gamma_N} \beta^N$. For each N-orbit A, label the elements of A by $\alpha_1, \alpha_2, \ldots, \alpha_n$. It is easy to check that $\Gamma \cong \Gamma_N\left[\overline{K_n}\right]$ via the identification

$$\begin{aligned} V(\Gamma) &\longrightarrow V(\Gamma_N\left[\overline{K_n}\right]) = V(\Gamma_N) \times V(\overline{K_n}) \\ \alpha_i &\longmapsto (A, i) \end{aligned}$$

Now suppose that Γ is an ℓ-multicover of Γ_N for some $\ell < n$. Then for any $\{A, B\} \in E(\Gamma_N)$, there is at least one pair α, β of vertices of Γ with $\alpha \in A$, $\beta \in B$, and $\alpha \nsim_\Gamma \beta$. Since $\mathrm{diam}(\Gamma) = 2$, there is a third vertex γ such that $\alpha \sim_\Gamma \gamma \sim_\Gamma \beta$. Then $\gamma \notin A \cup B$. If $C := \gamma^N$ it follows that $A \sim_{\Gamma_N} C$ and $B \sim_{\Gamma_N} C$. Hence A, B and C form a triangle in Γ_N. Therefore every edge of Γ_N lies in a triangle. □

A special case of Proposition 2.4.5 is considered in Proposition 2.4.6.

Proposition 2.4.6. *Let Γ be a G-symmetric graph with diameter 2, and suppose that there exists an $N \lhd G$ which acts nontrivially on $V(\Gamma)$, such that the following are satisfied:*

(1) the group N has exactly three orbits in $V(\Gamma)$; and
(2) the graph Γ is an $(n-1)$-multicover of Γ_N, where $n := \left|\gamma^N\right| \geq 3$, $\gamma \in V(\Gamma)$.

Then $\Gamma \cong K_3 \times K_n$.

PROOF. Let A, B and C be the distinct N-orbits in $V(\Gamma)$. It follows from Proposition 2.4.5 (2) that $\Gamma_N \cong K_3$. Fix $\alpha_1 \in A$, and take $\beta_1 \in B$ and $\gamma_1 \in C$ such that β_1 and γ_1 are the unique vertices in B and in C which are not adjacent to α_1. We claim that $\beta_1 \nsim_\Gamma \gamma_1$. Suppose not, and let $\gamma' \in C \setminus \{\gamma\}$, so that $\alpha_1 \sim_\Gamma \gamma'$ and $\beta_1 \sim_\Gamma \gamma'$ (see Figure 3). Then

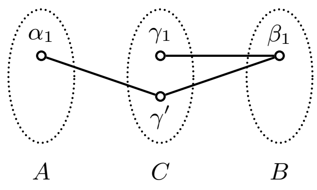

FIGURE 3. Diagram for the proof of Proposition 2.4.5

there exists $g \in G$ such that $(\alpha_1, \gamma')^g = (\beta_1, \gamma_1)$, which implies that $C^g = C$ and g swaps A and B setwise. Hence ${\beta_1}^g \in A$, and ${\beta_1}^g$ is the unique vertex in A which is not adjacent to ${\alpha_1}^g = \beta$. Therefore ${\beta_1}^g = \alpha_1$. This in turn implies that $\alpha_1 = {\beta_1}^g \sim_\Gamma (\gamma')^g = \gamma_1$, contrary to the choice of γ_1. Therefore β_1 and γ_1 must be nonadjacent.

Set $P_1 := \{\alpha_1, \beta_1, \gamma_1\}$. Choose $\alpha_2 \in A \setminus \{\alpha_1\}$, and β_2, γ_2 such that β_2 and γ_2 are the unique vertices in $B \setminus \{\beta_1\}$ and $C \setminus \{\gamma_1\}$, respectively, which are not adjacent to α_2, and set $P_2 := \{\alpha_2, \beta_2, \gamma_2\}$. (Note that $\beta_2 \neq \beta_1$ and $\gamma_2 \neq \gamma_1$ since $\alpha_2 \neq \alpha_1$.) Then arguing as in the above we again conclude that β_2 and γ_2 are nonadjacent. Continuing the process we eventually obtain a partition $\mathcal{P}$ of $V(\Gamma)$ consisting of sets $P_i = \{\alpha_i, \beta_i, \gamma_i\}$, $i = 1, \ldots, n$, where $\alpha_i \in A$, $\beta_i \in B$ and $\gamma_i \in C$ and α_i, β_i, γ_i are pairwise nonadjacent. Clearly $\mathcal{P}$ is G-invariant, and $\Gamma_\mathcal{P}$ is a complete graph on n vertices. It is also easy to see that the map

$$\begin{aligned} V(\Gamma) &\longrightarrow V(\Gamma_N \times \Gamma_\mathcal{P}) = \{A, B, C\} \times \mathcal{P} \\ \delta &\longmapsto \left(\delta^N, P_i\right), \ \delta \in P_i \end{aligned}$$

is a bijection. If $\delta, \delta' \in V(\Gamma)$ with $\delta \in P_i$ and $\delta' \in P_j$, then

$$\begin{aligned} \delta \sim_\Gamma \delta' &\Leftrightarrow \delta^N \neq (\delta')^N \text{ and } P_i \neq P_j \\ &\Leftrightarrow \delta^N \sim_{\Gamma_N} (\delta')^N \text{ and } P_i \sim_{\Gamma_\mathcal{P}} P_j \end{aligned}$$

Therefore $\Gamma \cong \Gamma_N \times \Gamma_\mathcal{P} \cong K_3 \times K_n$. □

It is still unclear what happens in the case where N has more than three orbits in $V(\Gamma)$. Under some additional conditions we have the following.

Proposition 2.4.7. *Let Γ be a G-symmetric graph with diameter 2, where $G := M \times N$ and M and N act intransitively and nontrivially on $V(\Gamma)$. Suppose further that Γ is an $(m-1)$-multicover of Γ_M, where $m := \left|\gamma^M\right|$, and an $(n-1)$-multicover of Γ_N, where $n := \left|\gamma^N\right|$. Then $\Gamma \cong K_n \times K_m$.*

PROOF. We first show that $\alpha^M \cap \alpha^N = \{\alpha\}$ for any $\alpha \in V(\Gamma)$. Suppose that $\alpha^M \subseteq \alpha^N$ for some $\alpha \in V(\Gamma)$. Then for any $g \in M$ there exists $h \in N$ such that $\alpha^g = \alpha^h$, and equivalently $g \in G_\alpha h$. So $M \leq G_\alpha N$, and hence $MN \leq G_\alpha N$. Since $MN = G$ then

$G_\alpha N = MN = G$ and thus N is transitive, a contradiction. Therefore $\alpha^M \nsubseteq \alpha^N$, and by a similar argument $\alpha^N \nsubseteq \alpha^M$. Take $\beta \in \alpha^M \backslash \alpha^N$ and suppose that there is a $\gamma \in \alpha^M \cap \alpha^N$ with $\gamma \neq \alpha$. Since Γ is an $(n-1)$-cover of Γ_N, α is the unique element of α^N which is not adjacent to β. So β must be adjacent to γ, which contradicts the fact that α^M contains no edges of Γ. Therefore $\alpha^M \cap \alpha^N = \{\alpha\}$.

It follows from the preceding paragraph that the map

$$\begin{aligned} V(\Gamma) &\longrightarrow V(\Gamma_M \times \Gamma_N) = V(\Gamma_M) \times V(\Gamma_N) \\ \alpha &\longmapsto \left(\alpha^M, \alpha^N\right) \end{aligned}$$

is a bijection, so that $|V(\Gamma_M)| = n$ and $\mathrm{val}\,(\Gamma_M) = n-1$, and thus $\Gamma_M \cong K_n$. Likewise $\Gamma_N \cong K_m$. For any $\alpha, \beta \in V(\Gamma)$, we have

$$\begin{aligned} \alpha \sim_\Gamma \beta &\Leftrightarrow \alpha^M \neq \beta^M \text{ and } \alpha^N \neq \beta^N \\ &\Leftrightarrow \alpha^M \sim_{\Gamma_M} \beta^M \text{ and } \alpha^N \sim_{\Gamma_N} \beta^N \\ &\Leftrightarrow \left(\alpha^M, \beta^M\right) \sim_{\Gamma_M \times \Gamma_N} \left(\alpha^N, \beta^N\right) \end{aligned}$$

Therefore $\Gamma \cong \Gamma_M \times \Gamma_N = K_n \times K_m$. □

2.4.1. Normal quotient reduction. The family of symmetric diameter 2 graphs being rather large, it is convenient for us to focus our study on those graphs which are, in a sense, the building blocks of all the graphs in the family. We identify these building blocks through *normal quotient reduction*, which has become an important tool in analysing the structure of certain families of graphs (see, for instance, [**19, 36, 37, 39**]). The general idea behind this process is as follows. We begin with a family $\mathcal{F}$ of finite graphs which is closed under taking normal quotients - that is, for any graph $\Gamma \in \mathcal{F}$, the normal quotients of Γ_N are also members of $\mathcal{F}$, as are the normal quotients of these normal quotients, and so on. Now, the class $\mathcal{F}$ contains graphs which are considered to be "degenerate" — in many cases the trivial graph K_1 is degenerate, as is each empty graph, and depending on the context there may be other graphs as well. If Γ is nondegenerate then, since Γ is finite, the process of taking normal quotients repeatedly will eventually yield a graph which is nondegenerate but all of whose proper normal quotients are degenerate. These graphs, which we call *basic*, are the building blocks in which we are interested.

Let $\mathcal{F}$ denote the family of symmetric diameter 2 graphs. Recall that it is possible for the diameter of a normal quotient graph to be less than the diameter of the original graph (see the beginning of this section). In particular, it is possible for a diameter 2 graph to have a complete graph as a normal quotient. Hence, to ensure that our family is closed under normal quotient reduction, we include the complete graphs in $\mathcal{F}$ as degenerate graphs.

The basic graphs in $\mathcal{F}$ are those nondegenerate graphs Γ, which admit an arc-transitive $G \leq \mathrm{Aut}\,(\Gamma)$, which satisfy either of the following:

(1) all G-normal quotients of Γ are complete graphs; or
(2) all nontrivial G-normal quotients of Γ are trivial graphs.

In the first case the graph is said to be *G-quotient-complete*; in the second it is *G-vertex-quasiprimitive* (from the fact that this case occurs if and only if all nontrivial normal subgroups of G are vertex-transitive — in other words, the action of G on $V(\Gamma)$ is quasiprimitive). It turns out that these two cases also arise as basic graphs in the family of vertex-transitive graphs, of which $\mathcal{F}$ is a subfamily, and this fact is stated in Theorem 1. Hence we define quotient-complete graphs formally (accommodating the possibility of disconnected graphs), as follows:

Definition 2.4.8. Let Γ be a graph and let $G \leq \mathrm{Aut}\,(\Gamma)$. We say that Γ is *G-quotient-complete* if it has at least one nontrivial complete G-normal quotient, and if each of its other proper G-normal quotients is either a complete graph or an empty graph.

Clearly, the complete graph K_n on n vertices is G-quotient-complete with $G = \mathrm{Sym}\,(n)$; on the other hand its complement, the empty graph $\overline{K_n}$ on n vertices, is not quotient-complete for any n. Note also that there is no restriction on the orders of complete graphs that occur as normal quotient graphs, and there is no upper bound on the number of complete normal quotients of a graph. For instance, for arbitrary positive integers m and n, Example 2.4.2 gives a connected graph Γ with complete normal quotients of orders m and n. Also, for a prime power c, Example 4.2.1 (1) gives a subgroup of $\mathrm{Aut}\,(c.K_c) = \mathrm{Sym}\,(c) \wr \mathrm{Sym}\,(c)$ that admits $c+1$ normal quotients, with c of them isomorphic to K_c and the remaining one isomorphic to $\overline{K_c}$.

The proof of Theorem 1 makes use of the following observation. Suppose that $N \leq G$ is intransitive on $V(\Gamma)$, and let $M \trianglelefteq G$ with $M \geq N$. Then any M-orbit in $V(\Gamma)$ is a union of N-orbits, so Γ_M is itself a G^{Γ_N}-normal quotient of Γ_N. Thus the minimal normal quotients with at least two vertices, which are obtained after a sequence of these operations, can also be obtained by choosing the normal subgroup N to be maximal in G such that N is intransitive on $V(\Gamma)$ (possibly $N = 1$). For such an N, the quotient Γ_N is called a *minimal G-normal quotient*.

Note that in the above, it is possible to have $\Gamma_M = \Gamma_N$ with $M \neq N$. For example, if Γ is the cycle C_4 and $G = D_8$, then for $N = Z(G) \cong \mathbb{Z}_2$, we have $\Gamma_N = C_2$. The kernel of the action of G on $V(\Gamma_N)$ is $M \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, giving $\Gamma_M = \Gamma_N$. In this case Γ_N is a minimal G-normal quotient with N properly contained in the maximal intransitive normal subgroup M.

If G acts quasiprimitively on $V(\Gamma)$, then all nontrivial normal subgroups of G are transitive and Γ is its own unique minimal G-normal quotient.

Lemma 2.4.9. *Let Γ be a graph, $G \leq \mathrm{Aut}(\Gamma)$, and $N \trianglelefteq G$ such that N is intransitive on $V(\Gamma)$. If N is maximal subject to being intransitive on $V(\Gamma)$, then $G^{\Gamma_N} \cong G/N$ and acts quasiprimitively on $V(\Gamma)$.*

Proof. Suppose that Γ_N is a minimal G-normal quotient of Γ, with N is maximal in G with respect to being vertex-intransitive on Γ. Then N is the kernel of the action of G on $V(\Gamma_N)$, and hence $G^{\Gamma_N} \cong G/N$. Also, by the discussion above, Γ_N has no nontrivial G^{Γ_N}-normal quotients, and so is G^{Γ_N}-vertex-quasiprimitive. □

The main result in this section is Theorem 1, which we now prove.

Proof of Theorem 1. If Γ is G-vertex-quasiprimitive then we have case (2) if Γ is not complete and case (1) if it is, with $N = 1$ in each case. If Γ is G-quotient-complete then we have case (1), again with $N = 1$. So assume that Γ is neither G-vertex-quasiprimitive nor G-quotient complete. Let N be a maximal vertex-intransitive normal subgroup of G. Then by Lemma 2.4.9, $G/N \leq \mathrm{Aut}(\Gamma_N)$ and is quasiprimitive on $V(\Gamma_N)$. If Γ_N is not complete then we have case (2), so suppose that Γ_N is complete for all maximal vertex-intransitive $N \trianglelefteq G$. Since Γ is not G-quotient complete, it follows from Definition 2.4.8 that there exists a nontrivial normal subgroup M of G such that M is vertex-intransitive on Γ and Γ_M is not complete; we choose M such that it is maximal in G having these properties. Since Γ is connected so is Γ_M, and it follows from the maximality of M that $G/M \leq \mathrm{Aut}(\Gamma_M)$ and Γ_M is not G/M-vertex-quasiprimitive. We claim that Γ_M is G/M-quotient-complete.

Let L' be a nontrivial normal subgroup of G/M such that L' is intransitive on $V(\Gamma_M)$. Then $(\Gamma_M)_{L'}$ is a proper nontrivial G/M-normal quotient of Γ_M. Now $L' = L/M$ for some L such that $M < L \trianglelefteq G$ and L is intransitive on $V(\Gamma)$, and $(\Gamma_M)_{L'} = \Gamma_L$. Since M is maximal in G such that Γ_M is not complete and nontrivial, Γ_L must be complete. It follows that all proper (G/M)-normal quotients of Γ_M are complete graphs, and thus Γ_M is G/M-quotient-complete as claimed. Therefore case (1) holds, as required. □

CHAPTER 3

Linear algebra and geometries

It is shown in Chapter 4 and 5 that some families of basic symmetric diameter 2 graphs (in particular, the quotient-complete graphs and the graphs with affine vertex-quasiprimtive automorphism group; see Theorem 1) can be organised according to the classification of finite transitive linear groups and of subgroups of finite classical groups, which are given, respectively, by Hering's Theorem and Aschbacher's Theorem. This chapter is devoted to the exposition of these two theorems, together with some related technical results. Section 3.1 discusses tensor product spaces, which are structures preserved by some of the subgroups in Aschbacher's classification. Sections 3.2 to 3.4 give background on linear, semilinear, affine, and classical groups, as well as the exceptional group $G_2(q)$, which are among the types of subgroups described in both theorems. Finally, we present Hering's Theorem (Theorem 3.5.1) in Section 3.5 and Aschbacher's Theorem (Theorem 3.6.1) in Section 3.6.

Notation. Throughout this chapter $\mathbb{F}$ denotes a finite field; if we need to be specific about the order then we write $\mathbb{F}_q$ for a field of order q. If V is a vector space over $\mathbb{F}$ and $S \subseteq V$, then $\langle S\rangle_{\mathbb{F}}$ is the $\mathbb{F}$-span of S. The dimension of V over $\mathbb{F}$ is written $\dim(V)$ or $\dim_{\mathbb{F}}(V)$, as necessary. The zero vector is denoted by $\mathbf{0}_V$, or simply $\mathbf{0}$ if there is no confusion. The set of nonzero vectors is denoted by $V^{\#}$, and similarly the set of nonzero field elements is written as $\mathbb{F}^{\#}$ or $\mathbb{F}_q^{\#}$, as appropriate.

If $a_1, \dots, a_n \in \mathbb{F}$ then $\mathrm{diag}(a_1, \dots, a_n)$ is the $n\times n$ matrix $[g_{ij}]_{n\times n}$ with diagonal entries $g_{ii} = a_i$ and 0 everywhere else. The $n \times n$ identity matrix is denoted by I_n. The general linear group of V is denoted by $\mathrm{GL}(V)$.

3.1. Tensor product spaces

Let U and W be vector spaces over $\mathbb{F}$, with bases $\{u_1, \dots, u_m\}$ and $\{w_1, \dots, w_n\}$, respectively. The *tensor product* of U and W is the vector space $U \otimes W$ of dimension mn over $\mathbb{F}$, with basis $\mathcal{B} := \{u_i \otimes w_j \mid 1 \le i \le m,\ 1 \le j \le n\}$. For $u \in U$ and $w \in W$, with $u = \sum_{i=1}^m \alpha_i u_i$ and $w = \sum_{j=1}^n \beta_j w_j$, we write

$$u \otimes w = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_i\beta_j(u_i \otimes w_j), \qquad (3.1.1)$$

and such elements of $U \otimes W$ are called *simple*. By [**27**, Corollary IV.5.3], the definition of $U \otimes W$ is independent of the choice of bases for U and W, and the map $U \times W \to U \otimes W$,

$(u, w) \mapsto u \otimes w$, is bilinear. That is, for any $u, u' \in U$, $w, w' \in W$ and $\alpha \in \mathbb{F}$ we have

$$(u + u') \otimes w = u \otimes w + u' \otimes w\ ;$$
$$u \otimes (w + w') = u \otimes w + u \otimes w'\ ; \text{ and}$$
$$\alpha u \otimes w = u \otimes \alpha w = \alpha(u \otimes w).$$

We shall refer to the basis $\mathcal{B}$ as a *tensor product basis* of $U \otimes W$.

It follows from (3.1.1) that the group $\mathrm{GL}(U) \times \mathrm{GL}(W)$ acts on $U \otimes W$, where, for any $g \in \mathrm{GL}(U)$, $h \in \mathrm{GL}(W)$, and $v = \sum_{i,j} \alpha_{i,j} u_i \otimes w_j$,

$$v^{(g,h)} = \sum_{i,j} \alpha_{i,j} u_i^g \otimes w_j^h.$$

In particular, for $u \in U$ and $w \in W$,

$$(u \otimes w)^{(g,h)} := u^g \otimes w^h.$$

This action is not faithful, and its kernel is the subspace $K := \{(\lambda I_m, \lambda^{-1} I_n) \mid \lambda \in \mathbb{F}^\#\}$. If $g = [g_{ij}]_{m\times m}$ and $h = [h_{ij}]_{n\times n}$ are the matrices of g and h with respect to the ordered bases $(u_1, \ldots, u_m)$ and $(w_1, \ldots, w_n)$, respectively, then with respect to the ordered basis $(u_1 \otimes w_1, \ldots, u_1 \otimes w_n, u_2 \otimes w_1, \ldots, u_m \otimes w_n)$ of $U \otimes W$, (g, h) in its action on $U \otimes W$ corresponds to the matrix in $\mathrm{GL}(U \otimes W) = \mathrm{GL}(mn, \mathbb{F})$ with block structure

$$\begin{pmatrix} g_{11}h & \ldots & g_{1m}h \\ \vdots & & \vdots \\ g_{m1}h & \ldots & g_{mm}h \end{pmatrix} \tag{3.1.2}$$

The matrix in (3.1.2) is usually denoted by $g \otimes h$; extending this notation, we denote the image of $\mathrm{GL}(U) \times \mathrm{GL}(W)$ in its action on $U \otimes W$ by $\mathrm{GL}(U) \otimes \mathrm{GL}(W)$. Note that $\mathrm{GL}(U) \otimes \mathrm{GL}(W) \cong (\mathrm{GL}(U) \times \mathrm{GL}(W))/K$, and that K is isomorphic to a diagonal subgroup of $Z(\mathrm{GL}(U)) \times Z(\mathrm{GL}(W))$. Note that K is contained in the centre of $\mathrm{GL}(U) \times \mathrm{GL}(W)$ and that $(\lambda I_m, I_n)K = (I_m, \lambda I_n)K$ for all $\lambda \in \mathbb{F}^\#$. The group $\mathrm{GL}(U) \otimes \mathrm{GL}(W)$ is called a *central product* of $\mathrm{GL}(U)$ and $\mathrm{GL}(W)$, and is written as $\mathrm{GL}(U) \circ \mathrm{GL}(W)$.

Recall from above that a simple vector in $U \otimes W$ is a nonzero vector which can be written as $u \otimes w$ for some $u \in U$ and $w \in W$. The *weight* $\mathrm{wt}\,(v)$ of a nonzero vector $v \in U \otimes W$ is the least number k such that v is the sum of k simple vectors.

Lemma 3.1.1. [**20**, Lemma 4.3] *Let $V = U \otimes W$, where U and W are vector spaces over a finite field $\mathbb{F}$ with (possibly not equal) finite dimensions, and let $v \in V^\#$ with $v := \sum_{i=1}^k (u_i \otimes w_i)$. Then $\mathrm{wt}\,(v) = k$ if and only if $\{u_1, \ldots, u_k\}$ and $\{w_1, \ldots, w_k\}$ are linearly independent over $\mathbb{F}$. Furthermore, if v has another representation $v = \sum_{i=1}^k (u_i' \otimes w_i')$, then $\langle u_1, \ldots, u_k\rangle_\mathbb{F} = \langle u_1', \ldots, u_k'\rangle_\mathbb{F}$ and $\langle w_1, \ldots, w_k\rangle_\mathbb{F} = \langle w_1', \ldots, w_k'\rangle_\mathbb{F}$.*

The operation of taking tensor products is associative [**27**, Theorem IV.5.8], that is, for vector spaces U, V and W over $\mathbb{F}$,

$$(U \otimes V) \otimes W \cong U \otimes (V \otimes W).$$

Hence we can extend the definition of a tensor product of two $\mathbb{F}$-spaces to that involving t spaces for arbitrary $t \geq 2$, as follows. For each $i \in \{1, \dots, t\}$, let U_i be a vector space over $\mathbb{F}$ with dimension m_i, and let $B_i := \{b_{i,1}, \dots, b_{i,m_i}\}$ be a basis for U_i. The tensor product of $U_1, \dots, U_t$ is the vector space $\otimes_{i=1}^t U_i$ over $\mathbb{F}$ with dimension $\prod_{i=1}^t m_i$ and basis $\mathcal{B} := \{\otimes_{i=1}^t b_{i,j_i} \mid 1 \leq j_i \leq m_i\}$. In particular, for $u_i = \sum_{j_i=1}^{m_i} \alpha_{i,j_i} b_{i,j_i} \in U_i$ we write

$$\otimes_{i=1}^t u_i = \sum_{j_1=1}^{m} \cdots \sum_{j_t=1}^{m} \alpha_{1,j_1} \cdots \alpha_{t,j_t} \left(\otimes_{i=1}^t b_{i,j_i}\right).$$

It follows that the map $U_1 \times \cdots \times U_t \to \otimes_{i=1}^t U_i$, $(u_1, \dots, u_t) \mapsto \otimes_{i=1}^t u_i$, is t-linear. That is, for any $i \in \{1, \dots, t\}$, $u_i, u_i' \in U_i$, and $\alpha \in \mathbb{F}$,

$$x \otimes (u_i + u_i') \otimes y = x \otimes u_i \otimes y + x \otimes u_i' \otimes y \quad \text{and}$$
$$x \otimes \alpha u_i \otimes y = \alpha(u_1 \otimes \cdots \otimes u_t),$$

where $x := \otimes_{j=1}^{i-1} u_j$ and $y := \otimes_{j=i+1}^t u_j$. The simple vectors in $\otimes_{i=1}^t U_i$ are those nonzero vectors which can be written as $\otimes_{i=1}^t u_i$ for some $u_i \in U_i$, and the (tensor) weight $\mathrm{wt}\,(v)$ of a nonzero vector v is the smallest number k such that v is the sum of k simple vectors. The basis $\mathcal{B}$ is again called a *tensor product basis.*

The group $\mathrm{GL}(U_1) \times \cdots \times \mathrm{GL}(U_t)$ acts on $\otimes_{i=1}^t U_i$ with

$$\left(\otimes_{i=1}^t u_i\right)^{(g_1,\dots,g_t)} := \otimes_{i=1}^t u_i^{g_i}$$

for any $u_i \in U_i$ and $g_i \in \mathrm{GL}(U_i)$, extended linearly to the whole space. We denote the image of $(g_1, \dots, g_t)$ under the corresponding representation by $\otimes_{i=1}^t g_i$, and the image of $\mathrm{GL}(U_1) \times \cdots \times \mathrm{GL}(U_t)$ by $\otimes_{i=1}^t \mathrm{GL}(U_i)$. The kernel of this representation is $K = \left\{(\lambda_1 I_{m_1}, \dots, \lambda_t I_{m_t}) \,\middle|\, \lambda_1 \cdots \lambda_t = 1,\ \lambda_i \in \mathbb{F}^\#\right\}$, which is a subgroup of the centre, so $\otimes_{i=1}^t \mathrm{GL}(U_i)$ is again the central product $\mathrm{GL}(U_1) \circ \cdots \circ \mathrm{GL}(U_t)$.

The next result is a basic property of $\otimes_{i=1}^t U_i$, and is proved in [**45**].

Lemma 3.1.2. [**45**, Lemma 3.1.4] *Let $t \geq 2$ and $V = \otimes_{i=1}^t U_i$, where U_i is a finite-dimensional vector space over $\mathbb{F}$ for all i. Let $u, w \in V^\#$ with $u := \otimes_{i=1}^t u_i$ and $w := \otimes_{i=1}^t w_i$. Then $u + w$ is simple if and only if u_i is a scalar multiple of w_i for all but at most one i.*

The following are easy observations about the relationship between the tensor weights of the same vector in two different tensor product decompositions of V. To distinguish between these weights, we use the notation $\mathrm{wt}_{U\otimes W}(v)$ to denote the weight of v in $U \otimes W$.

Lemma 3.1.3. *Let $t \geq 3$ and $V = \otimes_{i=1}^{t} U_i$, where U_i is a finite-dimensional vector space over $\mathbb{F}$ for all i.*

(1) If $X := \otimes_{i=1}^{s} U_i$ and $Y := \otimes_{i=s+1}^{t} U_i$ for some $s \in \{1, \dots, t-1\}$, then $\mathrm{wt}_{\otimes_{i=1}^{t} U_i}(v) \geq \mathrm{wt}_{X \otimes Y}(v)$ for any $v \in V^{\#}$.

(2) If $v = \sum_{i=1}^{k} (v_{i,1} \otimes \cdots \otimes v_{i,t-1} \otimes w)$, then $\mathrm{wt}_{\otimes_{j=1}^{t} U_j}(v) \leq \mathrm{wt}_{\otimes_{j=1}^{t-1} U_j}(u)$, where $u := \sum_{i=1}^{k} (v_{i,1} \otimes \cdots \otimes v_{i,t-1})$.

Proof. Statement (1) follows immediately from the fact that a simple vector in $\otimes_{i=1}^{t} U_i$ is also simple in $X \otimes Y$.

To prove statement (2), let $X := \otimes_{j=1}^{t-1} U_j$. Then in $X \otimes U_t$, v can be written as $v = u \otimes w$, and u in turn can be written as a sum of ℓ simple vectors in $\otimes_{j=1}^{t-1} U_j$, where $\ell := \mathrm{wt}_{\otimes_{j=1}^{t-1} U_j}(u)$. Since the tensor product of a simple vector in X and a vector in U_t is a simple vector in $\otimes_{j=1}^{t} U_j$, it follows that $\mathrm{wt}_{\otimes_{j=1}^{t} U_j}(v) \leq \ell$. □

For the rest of the section, assume that $m_i = m$ for all i. In this case the symmetric group $\mathrm{Sym}\,(t)$ acts on $\otimes_{i=1}^{t} U_i$ by permuting the tensor factors. Thus we get an action of $\mathrm{GL}(U_i) \wr \mathrm{Sym}\,(t)$ on $\otimes_{i=1}^{t} U_i$ that is similar to the product action defined in (1.3.2); we denote the image of this wreath product in this action by $\mathrm{GL}(U_i) \wr_{\otimes} \mathrm{Sym}\,(t)$.

Lemma 3.1.4. *Let $t \geq 2$ and $V = \otimes_{i=1}^{t} U_i$, where $U_i = \mathbb{F}^m$ for all i. Then for any $v \in V^{\#}$, $g \in \otimes_{i=1}^{t} \mathrm{GL}(U_i)$ and $\pi \in \mathrm{Sym}\,(t)$, we have $\mathrm{wt}\,(v^{g \cdot \pi}) = \mathrm{wt}\,(v)$.*

Proof. Let $u := \otimes_{i=1}^{t} u_i$ be a simple vector in V. Then for any $g := \otimes_{i=1}^{t} g_i \in \otimes_{i=1}^{t} \mathrm{GL}(U_i)$ and $\pi \in \mathrm{Sym}\,(t)$, $u^{g \cdot \pi} = \otimes_{i=1}^{t} u_{i'}{}^{g_{i'}}$ where $i' := i^{\pi^{-1}}$ for each i. So $u^{g \cdot \pi}$ is also simple. It follows that $\mathrm{wt}\,(v^{g \cdot \pi}) \leq \mathrm{wt}\,(v)$ for any $v \in V$. Similarly, since v, g and π are arbitrary, $\mathrm{wt}\,(v) = \mathrm{wt}\left((v^{g \cdot \pi})^{(g \cdot \pi)^{-1}}\right) \leq \mathrm{wt}\,(v^{g \cdot \pi})$. Therefore $\mathrm{wt}\,(v^{g \cdot \pi}) = \mathrm{wt}\,(v)$. □

Lemma 3.1.5. *Let $t \geq 2$ and $V = \otimes_{i=1}^{t} U_i$, where $U_i = \mathbb{F}^m$ for all i, and let $v = \sum_{i=1}^{k} \left(\otimes_{j=1}^{t} v_{i,j}\right) \in V^{\#}$. If $\mathrm{wt}\,(v) = k$, then the set*

$$\{v_{i,1} \otimes \cdots \otimes v_{i,\ell-1} \otimes v_{i,\ell+1} \otimes \cdots \otimes v_{i,t} \mid 1 \leq i \leq k\}$$

is an $\mathbb{F}$-linearly independent subset of $\otimes_{j \neq \ell} U_j$ for each $\ell \in \{1, \dots, t\}$.

Proof. If $t = 2$ then this is true by Lemmas 3.1.1 and 3.1.2, so assume from now on that $t \geq 3$. It follows from Lemma 3.1.4 that we only need to prove the result for $\ell = 1$. Let $A := \{\otimes_{j=2}^{t} v_{i,j} \mid 1 \leq i \leq k\}$. Suppose that A is $\mathbb{F}$-dependent. Then $a := \dim(\langle A \rangle_{\mathbb{F}}) < k$. Reorder the elements of A so that $\{\otimes_{j=2}^{t} v_{i,j} \mid 1 \leq i \leq a\}$ is a basis for $\langle A \rangle_{\mathbb{F}}$, and for each $i \in \{1, \dots, k\}$ write

$$\otimes_{j=2}^{t} v_{i,j} = \sum_{r=1}^{a} \alpha_{i,r} \left(\otimes_{j=2}^{t} u_{r,j}\right),$$

where $\alpha_{i,r} \in \mathbb{F}$ for all i and r. Applying Lemma 3.1.2 we get

$$v = \sum_{i=1}^{k} \left(v_{i,1} \otimes \sum_{r=1}^{a} \alpha_{i,r} \left(\otimes_{j=2}^{t} v_{r,j} \right) \right)$$
$$= \sum_{r=1}^{a} \left(\left(\sum_{i=1}^{k} \alpha_{i,r} v_{i,1} \right) \otimes v_{r,2} \otimes \cdots \otimes v_{r,t} \right),$$

so that $\mathrm{wt}\,(v) = a < k$, a contradiction. Hence A is $\mathbb{F}$-independent, and it follows from Lemma 3.1.4 that so is $\{\otimes_{j \neq \ell} v_{i,j} \mid 1 \leq i \leq k\}$ for all $\ell \in \{2, \dots, t\}$. □

If $t = 2$ then by Lemma 3.1.1 the converse of Lemma 3.1.5 holds, but it does not hold in general when $t \geq 3$. A special case for which the converse is true is the following.

Lemma 3.1.6. *Let $t \geq 2$ and $V = \otimes_{i=1}^{t} U_i$, where $U_i = \mathbb{F}^m$ for all i. Let $v := \sum_{i=1}^{k} (\otimes_{j=1}^{t} v_{i,j})$, where $k \leq m$ and $\{v_{i,j} \mid 1 \leq i \leq k\}$ is linearly independent in U_j for all j. Then* $\mathrm{wt}\,(v) = k$.

Proof. Clearly $\mathrm{wt}\,(v) \leq k$. Consider the decomposition $V = U_1 \otimes W$, where $W := \otimes_{j=2}^{t} U_j$, and for each $i \in \{1, \dots, k\}$ set $w_i := \otimes_{j=2}^{t} v_{i,j}$. Now the set $\{w_i \mid 1 \leq i \leq k\}$ is linearly independent in W, so by Lemma 3.1.1 applied to $U_1 \otimes W$, the vector v has weight k in $U_1 \otimes W$. Therefore $\mathrm{wt}\,(v) \geq k$ by Lemma 3.1.3 (1), and thus $\mathrm{wt}\,(v) = k$. □

Lemma 3.1.5 implies that $\mathrm{wt}\,(v) \leq m^{t-1}$ for all $v \in V^{\#}$, and by Lemma 3.1.1, this bound is achieved if $t = 2$. It is not achieved when $t \geq 3$, as implied by the next result, which gives an improvement on this bound when $t \geq 3$.

Lemma 3.1.7. *Let $t \geq 3$ and $V = \otimes_{i=1}^{t} U_i$, where $U_i = \mathbb{F}^m$ and $m \geq 2$. Then for any $v \in V^{\#}$,*

$$\mathrm{wt}\,(v) \leq m^{t-3} \left(m^2 - \left\lfloor \frac{m}{2} \right\rfloor \right).$$

Proof. Assume first that $t = 3$. For each $i \in \{1, \dots, t\}$ let

$$B_i := \{b_{i,j_i} \mid 1 \leq j_i \leq m\} \tag{3.1.3}$$

be a basis for U_i. Then $\{b_{2,j_2} \otimes b_{3,j_3} \mid 1 \leq j_i \leq m \text{ for } i = 2, 3\}$ is a basis for $U_2 \otimes U_3$, and applying Lemma 3.1.2 we can write

$$v = \sum_{j_3=1}^{m} \left(\sum_{j_2=1}^{m} (u_{j_2,j_3} \otimes b_{2,j_2} \otimes b_{3,j_3}) \right),$$

with $u_{j_2,j_3} \in U_1$ for all j_2 and j_3. For each j_3 set $w_{j_3} := \sum_{j_2=1}^{m} (u_{j_2,j_3} \otimes b_{2,j_2} \otimes b_{3,j_3})$ and $A_{j_3} := \{u_{j_2,j_3} \mid 1 \leq j_2 \leq m\}$ (that is, A_{j_3} is the set of U_1-projections of the terms in w_{j_3}). Then $\mathrm{wt}\,(v) \leq \sum_{j_3=1}^{m} \mathrm{wt}\,(w_{j_3})$. *Claim: For all $j_3 \in \{1, \dots, m\}$, $\mathrm{wt}\,(w_{j_3}) \leq \dim(\langle A_{j_3} \rangle_{\mathbb{F}})$.* Indeed, if $d(j_3) := \dim(\langle A_{j_3} \rangle_{\mathbb{F}})$, then by Lemma 3.1.3 (2),

$$\mathrm{wt}\,(w_{j_3}) \leq \mathrm{wt}_{U_1 \otimes U_2}(u_{j_2,j_3} \otimes b_{2,j_2}) \leq \min\{d(j_3), m\} = d(j_3).$$

In particular, $\mathrm{wt}\,(w_{j_3}) \le m$ if A_{j_3} is linearly independent, and $\mathrm{wt}\,(w_{j_3}) \le m-1$ if A_{j_3} is linearly dependent.

In finding an upper bound for $\mathrm{wt}\,(v)$ we consider two cases, according to the number ℓ of sets A_{j_3}, where $1 \le j_3 \le m$, such that A_{j_3} is linearly independent.

Case 1: Suppose that $\ell = 0$ or $\ell = 1$. It follows from the claim that

$$\begin{aligned}\mathrm{wt}\,(v) &\le \ell m + (m-\ell)(m-1)\\ &= m(m-1) + \ell\\ &\le m^2 - (m-1)\\ &\le m^2 - \lfloor m/2 \rfloor\end{aligned}$$

Case 2: Suppose that $\ell \ge 2$. Without loss of generality suppose that A_{j_3} is linearly independent for $1 \le j_3 \le \ell$, and linearly dependent otherwise. Form the pairs $\{A_1, A_2\}$, $\{A_3, A_4\}$, ... up to $\{A_{\ell-1}, A_\ell\}$ if ℓ is even, or $\{A_{\ell-2}, A_\ell\}$ if ℓ is odd. For any pair $\{A_r, A_s\}$ take $a \in U_1$ such that $a \notin \langle A_r \setminus \{u_{1,r}\}\rangle_{\mathbb{F}} \cup \langle A_s \setminus \{u_{1,s}\}\rangle_{\mathbb{F}}$. (Such an a exists because two proper subspaces do not cover U_1.) Then $\{a, u_{2,r}, \ldots, u_{m,r}\}$ and $\{a, u_{2,s}, \ldots, u_{m,s}\}$ are bases for U_1. Writing $u_{1,r} = \alpha_1 a + \sum_{j_2=2}^m \alpha_{j_2} u_{j_2,r}$ and $u_{1,s} = \beta_1 a + \sum_{j_2=2}^m \beta_{j_2} u_{j_2,s}$, where $\alpha_{j_2}, \beta_{j_2} \in \mathbb{F}$ for all j_2, we get

$$\begin{aligned}w_r + w_s &= \sum_{j_2=1}^m (u_{j_2,r} \otimes b_{2,j_2} \otimes b_{3,r}) + \sum_{j_2=1}^m (u_{j_2,s} \otimes b_{2,j_2} \otimes b_{3,s})\\ &= \left(\alpha_1 a + \sum_{j_2=2}^m \alpha_{j_2} u_{j_2,r}\right) \otimes b_{2,1} \otimes b_{3,r} + \sum_{j_2=2}^m (u_{j_2,r} \otimes b_{2,j_2} \otimes b_{3,r})\\ &\quad + \left(\beta_1 a + \sum_{j_2=2}^m \beta_{j_2} u_{j_2,s}\right) \otimes b_{2,1} \otimes b_{3,s} + \sum_{j_2=2}^m (u_{j_2,s} \otimes b_{2,j_2} \otimes b_{3,s})\\ &= a \otimes b_{2,1} \otimes (\alpha_1 b_{3,r} + \beta_1 b_{3,s}) + \sum_{j_2=2}^m (u_{j_2,r} \otimes (\alpha_{j_2} b_{2,1} + b_{2,j_2}) \otimes b_{3,r})\\ &\quad + \sum_{j_2=2}^m (u_{j_2,s} \otimes (\beta_{j_2} b_{2,1} + b_{2,j_2}) \otimes b_{3,s})\,.\end{aligned}$$

So $\mathrm{wt}\,(w_r + w_s) \le 2m - 1$. This together with the claim gives us

$$\begin{aligned}\mathrm{wt}\,(v) &\le \lfloor \ell/2 \rfloor (2m-1) + (\ell - 2\lfloor \ell/2 \rfloor)m + (m-\ell)(m-1)\\ &= m^2 - m + \ell - \lfloor \ell/2 \rfloor\\ &\le m^2 - \lfloor \ell/2 \rfloor.\end{aligned}$$

This completes the proof for the case where $t = 3$.

Now suppose that $t > 3$. Let B_i be as in (3.1.3) for $i \in \{1, \ldots, t\}$. Then $\overline{B} := \{\otimes_{i=4}^t b_{i,j_i} \mid 1 \le j_i \le m\}$ is a basis for $\otimes_{i=4}^t U_i$, and $\{b_{2,j_2} \otimes b_{3,j_3} \otimes \overline{b} \mid \overline{b} \in \overline{B}; 1 \le j_2, j_3 \le m\}$

is a basis for $\otimes_{i=2}^{t} U_i$. Hence we can write

$$v = \sum_{\overline{b} \in \overline{B}} \left(\sum_{1 \le j_2, j_3 \le m} \left(u_{j_2,j_3,\overline{b}} \otimes b_{2,j_2} \otimes b_{3,j_3} \otimes \overline{b} \right) \right),$$

for some $u_{j_2,j_3,\overline{b}} \in U_1$. For each $\overline{b}$ set $w_{\overline{b}} := \sum_{1 \le j_2, j_3 \le m} (u_{j_2,j_3,\overline{b}} \otimes b_{2,j_2} \otimes b_{3,j_3} \otimes \overline{b})$, and consider the decomposition $V = U_1 \otimes U_2 \otimes U_3 \otimes Y$, where $Y := \otimes_{i=4}^{t} U_i$. If $u := \sum_{1 \le j_2, j_3 \le m} (u_{j_2,j_3,\overline{b}} \otimes b_{2,j_2} \otimes b_{3,j_3})$, then $\mathrm{wt}\left(w_{\overline{b}}\right) \le \mathrm{wt}_{\otimes_{i=1}^{3} U_i}(u)$ by Lemma 3.1.3 (2). It was shown above that the weight of any vector in $\otimes_{i=1}^{3} U_i$ is at most $m^2 - \lfloor m/2 \rfloor$. Hence

$$\mathrm{wt}\,(v) \le \sum_{\overline{b} \in \overline{B}} \mathrm{wt}\left(w_{\overline{b}}\right) \le m^{t-3}\left(m^2 - \lfloor m/2 \rfloor\right).$$

□

The next result shows that the upper bound in Lemma 3.1.7 is met when $(m, t) = (2, 3)$. Moreover, computer calculations using MAGMA [**1**] have shown that it is also met when $(m, t) = (2, 4)$ and $\mathbb{F} = \mathbb{F}_2$.

Lemma 3.1.8. *Let $V = \otimes_{i=1}^{3} U_i$, where $U_i = \mathbb{F}^2$ for all i. For each i let $\{b_{i,1}, b_{i,2}\}$ be a basis of U_i, and define*

$$v := b_{1,1} \otimes b_{2,1} \otimes b_{3,1} + b_{1,2} \otimes b_{2,1} \otimes b_{3,2} + b_{1,1} \otimes b_{2,2} \otimes b_{3,2}.$$

Then $\mathrm{wt}\,(v) = 3$.

PROOF. Let $W := U_2 \otimes U_3$. Then $V = U_1 \otimes W$, and in this decomposition we can write

$$v = b_{1,1} \otimes (b_{2,1} \otimes b_{3,1} + b_{2,2} \otimes b_{3,2}) + b_{1,2} \otimes (b_{2,1} \otimes b_{3,2}).$$

Both $\{b_{1,1}, b_{1,2}\}$ and $\{b_{2,1} \otimes b_{3,1} + b_{2,2} \otimes b_{3,2},\ b_{2,1} \otimes b_{3,2}\}$ are linearly independent by the choice of the vectors $b_{i,j}$, so $\mathrm{wt}_{U_1 \otimes W}(v) = 2$ by Lemma 3.1.1. Hence $\mathrm{wt}_{\otimes_{j=1}^{3} U_j}(v) \ge 2$ by Lemma 3.1.3 (1).

Suppose that $\mathrm{wt}_{\otimes_{j=1}^{3} U_j}(v) = 2$. Then $v = \sum_{i=1}^{2} (\otimes_{j=1}^{3} v_{i,j})$ for some simple vectors $\otimes_{j=1}^{3} v_{1,j}, \otimes_{j=1}^{3} v_{2,j} \in V$. By Lemma 3.1.1 and the above, $\langle v_{1,1}, v_{1,2} \rangle_{\mathbb{F}} = \langle b_{1,1}, b_{1,2} \rangle_{\mathbb{F}}$ and $\langle v_{1,2} \otimes v_{1,3},\ v_{2,2} \otimes v_{2,3} \rangle_{\mathbb{F}} = \langle b_{2,1} \otimes b_{3,1} + b_{2,2} \otimes b_{3,2},\ b_{2,1} \otimes b_{3,2} \rangle_{\mathbb{F}}$. Then for some $\alpha, \beta, \gamma, \delta \in \mathbb{F}$ we have $v_{1,1} = \alpha b_{1,1} + \beta b_{1,2}$ and

$$\begin{aligned} v_{1,2} \otimes v_{1,3} &= \gamma\,(b_{2,1} \otimes b_{3,1} + b_{2,2} \otimes b_{3,2}) + \delta\,(b_{2,1} \otimes b_{3,2}) \\ &= b_{2,1} \otimes (\gamma b_{3,1} + \delta b_{3,2}) + b_{2,2} \otimes \gamma b_{3,2}. \end{aligned}$$

By Lemma 3.1.2 the set $\{\gamma b_{3,1} + \delta b_{3,2},\ \gamma b_{3,2}\}$ is linearly dependent, so $\gamma = 0$ and $\delta \ne 0$. Let $u := \otimes_{j=1}^{3} v_{2,j} = v - \otimes_{j=1}^{3} v_{1,j}$. Then

$$\begin{aligned} u &= v - \delta\,(\alpha b_{1,1} + \beta b_{1,2}) \otimes b_{2,1} \otimes b_{3,2} \\ &= b_{1,1} \otimes (b_{2,1} \otimes b_{3,1} + b_{2,2} \otimes b_{3,2} - \alpha\delta b_{2,1} \otimes b_{3,2}) + (1 - \beta\delta) b_{1,2} \otimes b_{2,1} \otimes b_{3,2}. \end{aligned}$$

We have two cases.

Case 1: Suppose that $\beta\delta = 1$. Then $1 - \beta\delta = 0$ and

$$u = b_{1,1} \otimes b_{2,1} \otimes (b_{3,1} - \alpha\delta b_{3,2}) + b_{1,1} \otimes b_{2,2} \otimes b_{3,2}.$$

Note that $\{b_{2,1}, b_{2,2}\}$ and $\{b_{3,1} - \alpha\delta b_{3,2},\ b_{3,2}\}$ are both linearly independent, and thus $\mathrm{wt}_{\otimes_{j=1}^{3} U_j}(u) > 1$ by Lemma 3.1.2, a contradiction.

Case 2: Suppose that $\beta\delta \neq 1$. In this case $\{b_{1,1}, (1-\beta\delta)b_{1,2}\}$ and $\{b_{2,1} \otimes b_{3,1} + b_{2,2} \otimes b_{3,2} - \alpha\delta b_{2,1} \otimes b_{3,2},\ b_{2,1} \otimes b_{3,2}\}$ are both linearly independent, so $\mathrm{wt}_{U_1 \otimes W}(u) = 2$ by Lemma 3.1.1. It follows from Lemma 3.1.3 (1) that $\mathrm{wt}_{\otimes_{j=1}^{3} U_j}(u) \geq 2$, a contradiction.

From cases 1 and 2 we conclude that $\mathrm{wt}_{\otimes_{j=1}^{3} U_j}(v) \neq 2$. Therefore $\mathrm{wt}_{\otimes_{j=1}^{3} U_j}(v) = 3$ by Lemma 3.1.7. □

3.2. Linear, semilinear, and affine groups

In this section assume that $V = \mathbb{F}_q^n$ with $q = p^\ell$ for some prime p. Then the general linear group $\mathrm{GL}(V)$ of V may be identified with the group $\mathrm{GL}(n, q)$ of all invertible $n \times n$ matrices over $\mathbb{F}_q$, and the centre of $\mathrm{GL}(V)$ consists of all nonzero scalar transformations (or all scalar matrices $\lambda I_n, \lambda \in \mathbb{F}_q^{\#}$). The centre of $\mathrm{GL}(V)$, which we denote by Z_{q-1}, is thus isomorphic to $\mathbb{F}_q^{\#}$, which is a cyclic group of order $q - 1$. The *special linear group* $\mathrm{SL}(V)$ (or $\mathrm{SL}(n, q)$) of V is the subgroup of $\mathrm{GL}(V)$ consisting of all elements with determinant 1, and its centre is $Z_{q-1} \cap \mathrm{SL}(n, q) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^{\#},\ \lambda^n = 1\}$. The group $\mathrm{SL}(V)$ is normal in $\mathrm{GL}(V)$.

The *general semilinear group* of V is the group $\Gamma\mathrm{L}(V)$ (or $\Gamma\mathrm{L}(n, q)$) of all invertible $\mathbb{F}_q$-semilinear transformations of V, that is, all maps $g : V \to V$ that satisfy the following:

(i) there exists $\sigma(g) \in \mathrm{Aut}\,(\mathbb{F}_q)$, dependent only on g, such that

$$(\lambda u + v)^g = \lambda^{\sigma(g)} u^g + v^g \quad \forall\ \lambda \in \mathbb{F}_q \text{ and } u, v \in V;$$

and

(ii) $\{v \in V \mid v^g = \mathbf{0}_V\} = \{\mathbf{0}_V\}$.

The map

$$\sigma : \Gamma\mathrm{L}(n, q) \to \mathrm{Aut}\,(\mathbb{F}_q)\,, \tag{3.2.1}$$

with $\sigma(g)$ as in (i) for any g, is an epimorphism with kernel $\mathrm{GL}(n, q)$, and $\Gamma\mathrm{L}(n, q) = \mathrm{GL}(n, q) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$. The group $\mathrm{Aut}\,(\mathbb{F}_q)$ is a cyclic group of order ℓ generated by the Frobenius automorphism τ, which is the map $\tau : \alpha \mapsto \alpha^p$ for all $\alpha \in \mathbb{F}_q$, and the action of $\Gamma\mathrm{L}(V)$ on V is determined by the actions on V of $\mathrm{GL}(V)$ and of τ. For any fixed basis $\mathcal{B} := \{v_1, \ldots, v_n\}$ of V, we can define an action of τ on V by setting

$$\left(\sum_{i=1}^{n} \lambda_i v_i\right)^{\tau} := \sum_{i=1}^{n} \lambda_i^{\tau} v_i \tag{3.2.2}$$

for any $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q$. Note that this action of τ depends on the choice of the basis $\mathcal{B}$, and all actions of τ obtained as $\mathcal{B}$ varies over all bases of V are equivalent (i.e., conjugate by elements of $\mathrm{GL}(V)$).

The orders of $\mathrm{SL}(n,q)$, $\mathrm{GL}(n,q)$ and $\Gamma\mathrm{L}(n,q)$ are summarised in the next lemma.

Lemma 3.2.1. [**43**, Section 3.3] *Let $\ell, n \geq 1$ and $q = p^\ell$ for some prime p. Then:*

(1) $|\mathrm{GL}(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i) = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)$

(2) $|\mathrm{SL}(n,q)| = |\mathrm{GL}(n,q)|/(q-1)$

(3) $|\Gamma\mathrm{L}(n,q)| = \ell|\mathrm{GL}(n,q)|$

Let $\mathrm{X} \in \{\mathrm{GL}, \mathrm{SL}, \Gamma\mathrm{L}\}$. Then $\mathrm{X}(V)$ induces a permutation action on the set of 1-dimensional subspaces of V, and the kernel of this action is $\mathrm{X}(V) \cap Z_{q-1}$. The permutation group induced by $\mathrm{X}(V)$ on the set of 1-spaces of V is called the *projective semilinear group* (respectively, *projective general linear group* and *projective special linear group*) of V if $\mathrm{X} = \Gamma\mathrm{L}$ (respectively, $\mathrm{X} = \mathrm{GL}$ and $\mathrm{X} = \mathrm{SL}$), and is denoted by $\mathrm{PX}(V)$ (or $\mathrm{PX}(n,q)$). Hence

$$\mathrm{PX}(n,q) \cong \mathrm{X}(n,q)/(\mathrm{X}(n,q) \cap Z_{q-1}).$$

Let T_V denote the translation group of V. The *affine semilinear group* (or *affine general linear group*, *affine special linear group*) of V is the group $\mathrm{AX}(V)$ (or $\mathrm{AX}(n,q)$) generated by T_V and $\mathrm{X}(V)$, where $\mathrm{X} = \Gamma\mathrm{L}$ (respectively, $\mathrm{X} = \mathrm{GL}$ and $\mathrm{X} = \mathrm{SL}$). So $\mathrm{AX}(V)$ consists of all maps $t_{w,g} : v \mapsto v^g + w$ ($v \in V$), where $w \in V$ and $g \in \mathrm{X}(V)$. The group T_V is a regular normal subgroup of $\mathrm{AX}(V)$, and we have

$$\mathrm{AX}(V) \cong T_V \rtimes \mathrm{X}(V).$$

Since $\mathrm{Aut}\,(V) = \mathrm{GL}(V)$, we have from Theorem 1.1.8 that

$$\mathrm{AGL}(V) \cong N_{\mathrm{Sym}(V)}(T_V),$$

and $\mathrm{GL}(V)$ is the stabiliser in $\mathrm{AGL}(V)$ of $\mathbf{0}_V$. Thus $\mathrm{AGL}(V) = \mathrm{Hol}\,(V)$, as defined in Section 1.2, where V is identified with T_V. This fact will be used later.

For any subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$ and $\mathrm{X} \in \{\mathrm{GL}, \Gamma\mathrm{L}\}$, it is easy to see that the group $\mathrm{X}(n,q)$ contains a subgroup isomorphic to $\mathrm{X}(n,q_0)$. Likewise, if $k > 1$ is a divisor of n, then $\mathrm{X}(n,q)$ contains a subgroup isomorphic to $\mathrm{X}(n/k,q^k)$. Indeed, V can be viewed as a vector space of dimension $m := n/k$ over the extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. If $\mathbb{F}_{q^k} = \mathbb{F}_q[\omega]$ and $B := (u_1, \ldots, u_m)$ is an ordered $\mathbb{F}_{q^k}$-basis of V, then

$$\mathcal{B}_0 := \{\omega^i u_j \mid 0 \leq i \leq k-1,\ 1 \leq j \leq m\}$$

is an $\mathbb{F}_q$-basis of V. For any $g \in \mathrm{GL}(m,q^k)$ and $v = \sum_{i,j}\lambda_{ij}\omega^i u_j \in V$ (where $\lambda_{ij} \in \mathbb{F}_q$ for all i and j) we have $v^g = \sum_{i,j}\lambda_{ij}\omega^i(u_j)^g$, so g induces an $\mathbb{F}_q$-linear map on $\mathbb{F}_q^n$. So $\mathrm{GL}(n/k,q^k) \lesssim \mathrm{GL}(n,q)$. If τ' is the Frobenius automorphism of $\mathbb{F}_{q^k}$, acting on V with respect to the basis B, then $\tau' = h\tau$, where $h \in \mathrm{GL}(n,q)$ and $(\omega^i u_j)^h = (\omega^i)^p u_j$ for each i and j, and τ acts as in (3.2.2) with $\mathcal{B} = \mathcal{B}_0$. Hence $\Gamma\mathrm{L}(n/k,q^k) \lesssim \Gamma\mathrm{L}(n,q)$. It follows immediately that $\mathrm{AX}(n,q_0) \lesssim \mathrm{AX}(n,q)$ and $\mathrm{AX}(n/k,q^k) \lesssim \mathrm{AX}(n,q)$ for $\mathrm{X} \in \{\mathrm{GL}, \Gamma\mathrm{L}\}$. Observe also that the $\mathbb{F}_{q^k}$-automorphism $(\tau')^\ell$ is $\mathbb{F}_q$-linear on V. Hence $\mathrm{GL}(n,q)$ contains a subgroup isomorphic to $\mathrm{GL}(n/k, q^k) \rtimes \mathrm{Gal}\left(\mathbb{F}_{q^k}/\mathbb{F}_q\right)$, where $\mathrm{Gal}\left(\mathbb{F}_{q^k}/\mathbb{F}_q\right) = \langle(\tau')^\ell\rangle$ is the Galois group of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and is cyclic of order k. In particular, if $q = p$, then $\Gamma\mathrm{L}(n/k, p^k) \lesssim \mathrm{GL}(n, p)$.

The next two results concern certain families of subgroups of $\mathrm{AGL}(V)$. In particular, we consider the case where $\dim(V)$ is even and look at subgroups of the form $T_V \rtimes G_0$ for some $G_0 \leq \mathrm{GL}(V)$. In this case V has a direct sum decomposition $U \oplus U$ for some vector space U; a *diagonal subspace* of V (with respect to this decomposition) is a subspace of the form $\{(u, u^\varphi) \mid u \in U\}$ for some $\varphi \in \mathrm{GL}(U)$. For any subgroup L of T_V, we denote by V_L the subspace of V identified with L.

Lemma 3.2.2. *Let U be a finite vector space, $V := U \oplus U$, $G_0 \leq \mathrm{GL}(V)$, and $G = T_V \rtimes G_0$. Suppose that $T_{U\oplus\{\mathbf{0}_U\}}$ and $T_{\{\mathbf{0}_U\}\oplus U}$ are minimal normal subgroups of G, and let $L < G$ such that $L \neq T_{U\oplus\{\mathbf{0}_U\}}, T_{\{\mathbf{0}_U\}\oplus U}$. Then L is a minimal normal subgroup of G if and only if $L < T_V$ and V_L is a G_0-invariant diagonal subspace of V. In particular, if $\{(u, u) \mid u \in U\}$ is G_0-invariant, then the following hold:*

(1) *the group $G_0 = \{(h, h) \mid h \in H\}$ for some $H \leq \mathrm{GL}(U)$ which is irreducible on $U^\#$; and*

(2) *the minimal normal subgroups of G are precisely the groups T_W, where W is the subspace $U \oplus \{\mathbf{0}_U\}$, $\{\mathbf{0}_U\} \oplus U$, or $\{(u, u^\varphi) \mid u \in U\}$ for some $\varphi \in C_{\mathrm{GL}(U)}(H)$.*

Proof. We first show that L is a minimal normal subgroup of G, distinct from $T_{U\oplus\{\mathbf{0}_U\}}$ and $T_{\{\mathbf{0}_U\}\oplus U}$, if and only if $L < T_V$ and V_L is a G_0-invariant diagonal subspace of V. Since G_0 acts faithfully on V, each minimal normal subgroup L of G is contained in T_V. Also, a subgroup of T_V is normal in G if and only if the corresponding subspace is G_0-invariant. Thus it remains only to show that L is minimal normal in G if and only if V_L is a diagonal subspace.

Suppose that L is minimal normal in G distinct from $T_{U\oplus\{\mathbf{0}_U\}}$ and $T_{\{\mathbf{0}_U\}\oplus U}$. Denote by π_1 and π_2 the projection maps from V_L to $U \oplus \{\mathbf{0}_U\}$ and to $\{\mathbf{0}_U\} \oplus U$, respectively, and let $X := \pi_1(V_L)$. Since V_L is G_0-invariant, so is X, and hence $T_X \trianglelefteq G$. Now $T_X \leq T_{U\oplus\{\mathbf{0}_U\}}$, and thus, since $T_{U\oplus\{\mathbf{0}_U\}}$ is minimal normal in G, either $T_X = 1$ or $T_X = T_{U\oplus\{\mathbf{0}_U\}}$. Equivalently, either $X = \{\mathbf{0}_V\}$ or $X = U \oplus \{\mathbf{0}_U\}$. If $X = \{\mathbf{0}_V\}$ then $V_L \leq \{\mathbf{0}_U\} \oplus U$, so $L \leq T_{\{\mathbf{0}_U\}\oplus U}$. Since $T_{\{\mathbf{0}_U\}\oplus U}$ is minimal normal equality holds, contrary to the choice of L. So $\pi_1(V_L) = X = U \oplus \{\mathbf{0}_U\}$, and similarly $\pi_2(V_L) = \{\mathbf{0}_U\} \oplus U$; therefore $\pi_1|_{V_L}$ and $\pi_2|_{V_L}$ are surjective. Observe that $L \cap T_{U\oplus\{\mathbf{0}_U\}}$ is trivial since L and $T_{U\oplus\{\mathbf{0}_U\}}$ are distinct minimal normal subgroups of G, so that $V_L \cap \{\mathbf{0}_U\} = \{\mathbf{0}_V\}$ and the kernel of $\pi_1|_{V_L}$ is trivial. Hence $\pi_1|_{V_L}$ is one-to-one, and similarly so is $\pi_2|_{V_L}$. Therefore $\pi_1|_{V_L}$ and $\pi_2|_{V_L}$ are bijections, which shows that V_L is a diagonal subspace of V.

Conversely, suppose that V_L is a G_0-invariant diagonal subspace of V. Then L is a nontrivial normal subgroup of G. Let L' be a minimal normal subgroup of G which is contained in L. Then by the preceding paragraph $V_{L'}$ is a G_0-invariant diagonal subspace of V, and $V_L \geq V_{L'}$. It follows that $V_L = V_{L'}$ and thus $L = L'$. Therefore L is minimal normal in G.

Now suppose that $W_0 := \{(u,u) \mid u \in U\}$ is G_0-invariant. Then for any $u \in U$ and any $(g_1, g_2) \in G_0$ with $g_1, g_2 \in \mathrm{GL}(U)$, we have $(u,u)^{(g_1,g_2)} = (u^{g_1}, u^{g_2}) \in W_0$. So $u^{g_1} = u^{g_2}$ for all $u \in U$, and hence $g_1 = g_2$. Thus $G_0 = \{(h,h) \mid h \in H\}$ for some $H \leq \mathrm{GL}(U)$, where H is irreducible because of the minimality of $T_{U \oplus \{\mathbf{0}_U\}}$ and $T_{\{\mathbf{0}_U\} \oplus U}$. This proves (1).

Finally we show (2). Let L be a minimal normal subgroup of G. We have already proved that L is $T_{U \oplus \{\mathbf{0}_U\}}$, $T_{\{\mathbf{0}_U\} \oplus U}$, or $T_{Y(\rho)}$ for some G_0-invariant diagonal subspace $Y(\rho) := \{(u, u^\rho) \mid u \in U\}$ of V, and to complete the proof we need to show that the G_0-invariant diagonal subspaces are precisely the $Y(\rho)$ with $\rho \in C_{\mathrm{GL}(U)}(H)$. Suppose that $Y(\rho)$ is G_0-invariant. Then for all $u \in U$ and $h \in H$ we have $(u, u^\rho)^{(h,h)} = \left(u^h, u^{\rho h}\right) \in Y(\rho)$. It follows from the definition of $Y(\rho)$ that $u^{\rho h} = u^{h \rho}$ for all $u \in U$ and $h \in H$. Thus $\rho h = h \rho$ for all $h \in H$; that is, $\rho \in C_{\mathrm{GL}(U)}(H)$. Conversely, if $\rho \in C_{\mathrm{GL}(U)}(H)$, then for any $u \in U$ and $h \in H$ we have $(u, u^\rho)^{(h,h)} = \left(u^h, u^{\rho h}\right) = \left(u^h, u^{h\rho}\right) \in Y(\rho)$. So $Y(\rho)$ is G_0-invariant, which completes the proof of (2). □

The next result gives more information about the action of G_0 in Lemma 3.2.2 in the case where H is transitive on $U^\#$.

Lemma 3.2.3. *Let U be a finite vector space, $V = U \oplus U$, $H \leq \mathrm{GL}(U)$ which is transitive on $U^\#$, $G_0 = \{(h,h) \mid h \in H\} \leq \mathrm{GL}(V)$, and S a G_0-orbit in $V^\#$. Then $\langle S \rangle = V$ if and only if S is not $(U \oplus \{\mathbf{0}_U\})^\#$, $(\{\mathbf{0}_U\} \oplus U)^\#$, or $W^\#$ for a G_0-invariant diagonal subspace W of V.*

Proof. Throughout this proof $\langle S \rangle$ denotes the subspace of V generated by $S \subseteq V$.

Claim 1: $\langle S \rangle = V$ if and only if $\langle S \rangle \neq S \cup \{\mathbf{0}_V\}$. Suppose that $\langle S \rangle = V$. Since $(U \oplus \{\mathbf{0}_U\})^\#$ is a proper G_0-invariant subset of $V^\#$, G_0 is not transitive on $V^\#$ and thus $S \cup \{\mathbf{0}_U\} \neq V = \langle S \rangle$. Conversely, suppose that $\langle S \rangle \neq S \cup \{\mathbf{0}_V\}$. Let $v = (u_1, u_2) \in S$. If $u_2 = \mathbf{0}_U$ then we must have $u_1 \neq \mathbf{0}_U$, so that $v \in (U \oplus \{\mathbf{0}_U\})^\#$. Since H is transitive on $U^\#$ we have $S = v^{G_0} = (U \oplus \{\mathbf{0}_U\})^\#$, so $\langle S \rangle = U \oplus \{\mathbf{0}_U\} = S \cup \{\mathbf{0}_V\}$, contrary to our choice of S. Similarly if $u_1 = \mathbf{0}_U$ then $\langle S \rangle = U \oplus \{\mathbf{0}_U\}$, also a contradiction. Thus $u_1, u_2 \neq \mathbf{0}_U$, and moreover $(U \oplus \{\mathbf{0}_U\})^\#, (\{\mathbf{0}_U\} \oplus U)^\# \subseteq V \setminus S$. Let π_1 and π_2 be the projection maps from S to $U \oplus \{\mathbf{0}_U\}$ and to $\{\mathbf{0}_U\} \oplus U$, respectively. Arguing as before we get that $\pi_i(S) \subseteq U^\#$ for each i; moreover, since each $\pi_i(S)$ is H-invariant and H is transitive on $U^\#$, we have $\pi_i(S) = U^\#$ for each i. It follows that $\pi_i(\langle S \rangle) = \langle \pi_i(S) \rangle = U$. For each $u \in U^\#$ let $B(u) := \{v' \in S \mid \pi_1(v') = u\}$. Then $B(u)$ is nonempty for each u and is a block of imprimitivity for the action of G_0 on S. Hence

$$|S| = (|U| - 1)|B(u)| \geq |U| - 1.$$

Clearly we have $|S| + 1 \leq |\langle S \rangle|$, so if $\langle S \rangle$ were a diagonal subspace then $|\langle S \rangle| = |U| \leq |S| + 1$ and thus $|S| + 1 = |\langle S \rangle|$. Consequently $\langle S \rangle = S \cup \{\mathbf{0}_V\}$, a contradiction, and therefore $\langle S\rangle$ is not a diagonal subspace. Since $\pi_1(\langle S\rangle) = U$ by the above, there exist vectors $u, w_1, w_2 \in U$ with $w_1 \neq w_2$ and $(u, w_1), (u, w_2) \in \langle S\rangle$. So $(\mathbf{0}_U, w_1 - w_2) \in \langle S\rangle$, and $(\mathbf{0}_U, w_1 - w_2)^{G_0} = (\{\mathbf{0}_U\} \oplus U)^{\#} \subseteq \langle S\rangle$. Similarly $(U \oplus \{\mathbf{0}_U\})^{\#} \subseteq \langle S\rangle$, and hence $V = U \oplus U \subseteq \langle S\rangle$. Therefore $\langle S\rangle = V$, which proves Claim 1.

Claim 2: $\langle S\rangle = S \cup \{\mathbf{0}_V\}$ *if and only if* S *is* $(U \oplus \{\mathbf{0}_U\})^{\#}$, $\left(\{\mathbf{0}_U\} \oplus U^{\#}\right)$, *or is a* G_0*-invariant diagonal subspace.* It was shown above that if $\langle S\rangle$ has one of these forms then $\langle S\rangle = S \cup \{\mathbf{0}_V\}$. Suppose now that $\langle S\rangle = S \cup \{\mathbf{0}_V\}$. Then $\langle S\rangle$ is G_0-invariant, with G_0 transitive on $\langle S\rangle^{\#}$ and thus irreducible on $\langle S\rangle$. It follows that $T_{\langle S\rangle}$ is a minimal normal subgroup of G, and by Lemma 3.2.2, $\langle S\rangle$ is $U \oplus \{\mathbf{0}_U\}$, $\{\mathbf{0}_U\} \oplus U$, or a G_0-invariant diagonal subspace. Therefore Claim 2 holds, which completes the proof. □

3.3. Classical groups and their geometries

Throughout this section $V = \mathbb{F}_q^n$ where q is a prime power.

Let $f : V \times V \to \mathbb{F}_q$. Then f is a *left-linear form* on V if

$$f(\alpha u + \beta v, w) = \alpha f(u, w) + \beta f(v, w) \quad \forall\, u, v, w \in V,\ \forall\, \alpha, \beta \in \mathbb{F}_q.$$

That is, for each $v \in V$ the map $V \to \mathbb{F}_q, u \mapsto f(u, v)$, is linear. Similarly, f is a *right-linear form* if for each $u \in V$ the map $V \to \mathbb{F}_q, v \mapsto f(u, v)$ is linear. The map f is said to be

bilinear if it is both left-linear and right-linear;
symmetric if $f(u, v) = f(v, u) \quad \forall\, u, v \in V$;
skew-symmetric if $f(u, v) = -f(v, u) \quad \forall\, u, v \in V$;
alternating if $f(v, v) = 0 \quad \forall\, v \in V$;
conjugate-symmetric sesquilinear if there exists $\sigma \in \mathrm{Aut}\,(\mathbb{F}_q)$, $\sigma \neq 1$, such that $f(u, v) = f(v, u)^{\sigma} \quad \forall\, u, v \in V$.

Note that the definition of conjugate-symmetric implies that $\sigma^2 = 1$; in this case q must be a square and $\sigma : \alpha \mapsto \alpha^{\sqrt{q}}$ for all $\alpha \in \mathbb{F}_q$. The *left radical* of f is the set $\{u \in V \mid f(u, v) = 0\ \forall\, v \in V\}$, and its *right radical* is $\{v \in V \mid f(u, v) = 0\ \forall\, u \in V\}$. The map f is *nondegenerate* if its left and right radicals are both zero. It is easy to see that if f is symmetric, skew-symmetric, alternating, or conjugate-symmetric, then its left and right radicals coincide, and the radical of f is denoted by $\mathrm{rad}(f)$.

A *quadratic form* on V is a map $Q : V \to \mathbb{F}_q$ such that

$$Q(\alpha u + v) = \alpha^2 Q(u) + Q(v) + \alpha f(u, v) \quad \forall\, u, v \in V,\ \forall\, \alpha \in \mathbb{F}_q,$$

where f is a symmetric bilinear form on V. The map f in this case is called the *associated bilinear form* of Q. It follows from the definition that $2Q(v) = f(v, v)$ for all $v \in V$. Hence if $\mathrm{char}\,(\mathbb{F}_q) \neq 2$ then $Q(v) = \frac{1}{2} f(v, v)$, that is, f uniquely determines the quadratic form Q. On the other hand, if $\mathrm{char}\,(\mathbb{F}_q) = 2$ then f is alternating, and there is more than one quadratic form Q having f as its associated bilinear form. The quadratic form Q is *nondegenerate* if f is nondegenerate (i.e., $\mathrm{rad}(f) = \{\mathbf{0}_V\}$), and is *nonsingular* if the set $\mathrm{rad}(Q) := \{v \in \mathrm{rad}(f) \mid Q(v) = 0\}$ is zero. In odd characteristic, the terms "nondegenerate" and "nonsingular" are equivalent; in characteristic 2, all nondegenerate forms are nonsingular, but not conversely.

We write (V, ϕ) to signify that there is a map $\phi : V \times V \to \mathbb{F}_q$ or $\phi : V \to \mathbb{F}_q$ defined on V. We are interested in the following cases:

(1) (V, f), where f is a nondegenerate alternating bilinear form;
(2) (V, f), where f is nondegenerate conjugate-symmetric sesquilinear form;
(3) (V, Q), where Q is a nondegenerate quadratic form with associated bilinear form f.

The space V and its underlying geometry is called *symplectic* in case (1), *unitary* in case (2), and *orthogonal* in case (3).

If f is a left-linear form on V and U is any subspace of V, define

$$U^{\perp} := \{v \in V \mid f(u, v) = 0 \ \forall \ u \in U\}.$$

Then $U^{\perp}$ is a subspace of V. If f is nondegenerate, then by [**31**, Lemma 2.1.5], the spaces U and $U^{\perp}$ have the following properties:

(i) $\dim(U) + \dim\left(U^{\perp}\right) = \dim(V)$;
(ii) $(U^{\perp})^{\perp} = U$;
(iii) U is totally isotropic if and only if $U \leq U^{\perp}$;
(iv) U is nondegenerate (that is, the restriction $f|_U$ is nondegenerate) if and only if $V = U \oplus U^{\perp}$.

The space V is an *orthogonal direct sum* of its subspaces U and W, written $V = U \perp W$, if $V = U \oplus W$ and $f(u, w) = 0$ for all $u \in U$, $w \in W$. A nonzero vector v is said to be *isotropic* if $f(v, v) = 0$, and *anisotropic* otherwise. If f is symplectic or unitary, then an isotropic vector is also called *singular*. If f is symmetric bilinear with quadratic form Q, then a singular vector is a nonzero vector v such that $Q(v) = 0$. Hence, in general, all isotropic vectors are singular and vice versa, unless V is orthogonal and q is even. If V is orthogonal and q is even then all vectors are isotropic but not all are singular. If f is symplectic or unitary then a subspace U is *totally isotropic* or *totally singular* if $f|_U \equiv 0$; if f is symmetric bilinear with quadratic form Q, then U is totally isotropic if $f|_U \equiv 0$ and totally singular if $Q|_U \equiv 0$. On the other extreme, a subspace U is *anisotropic* if all nonzero vectors in U are anisotropic. A *hyperbolic pair* in V is a pair $\{x, y\}$ of singular vectors such that $f(x, y) = 1$. A *hyperbolic plane* is a two-dimensional subspace spanned by a hyperbolic pair.

Suppose that f_1 and f_2 are two left-linear forms on V which are of the same type (i.e., symplectic, unitary, or symmetric bilinear associated with a nonsingular quadratic form). Then f_1 and f_2 are *similar* if there exists $g \in \mathrm{GL}(V)$ such that, for some $\lambda(g) \in \mathbb{F}_q^{\#}$ which depends only on g,

$$f_1(u^g, v^g) = \lambda(g) f_2(u, v) \quad \forall \ u, v \in V.$$

Likewise, two quadratic forms Q_1 and Q_2 on V are similar if there is a $g \in \mathrm{GL}(V)$ such that for some $\lambda(g) \in \mathbb{F}_q^{\#}$,

$$Q_1(v^g) = \lambda(g)Q_2(v) \quad \forall\, v \in V.$$

In both cases the element g is called a *similarity* from (V, ϕ_1) to (V, ϕ_2), where $\phi_i = f_i$ or $\phi_i = Q_i$ for $i = 1, 2$. If $\lambda(g) = 1$ then g is called an *isometry.* Observe that a similarity from (V, Q_1) to (V, Q_2) is a similarity from (V, f_1) to (V, f_2), where f_i is the associated bilinear form of Q_i; the converse is true only if char $(\mathbb{F}_q)$ is odd. If $\phi_1 = \phi_2 = \phi$ then a similarity (respectively, isometry) of (V, ϕ) is called a *ϕ-similarity* (respectively, *ϕ-isometry*).

Theorem 3.3.1. [**31**, Propositions 2.3.2, 2.4.1, 2.5.3] *Let $V = \mathbb{F}_q^n$, and let f be a left-linear form on V which is symplectic, unitary, or a symmetric bilinear form associated with a nondegenerate quadratic form Q. Then*

$$V = \langle x_1, y_1 \rangle \perp \ldots \perp \langle x_m, y_m \rangle \perp U$$

where $\{x_i, y_i\}$ is a hyperbolic pair for each i and U is an anisotropic subspace. Moreover:

(1) If f is symplectic then $U = 0$. Hence n is even and, up to equivalence, there is a unique symplectic geometry in dimension n over $\mathbb{F}_q$.
(2) If f is unitary then $U = 0$ if n is even and $\dim(U) = 1$ *if n is odd. Hence up to equivalence, there is a unique unitary geometry in dimension n over $\mathbb{F}_q$.*
(3) If f is symmetric bilinear with quadratic form Q and n is odd, then $\dim(U) = 1$ *and there are two isometry classes of quadratic forms in dimension n over $\mathbb{F}_q$, one a non-square multiple of the other. Hence all orthogonal geometries in dimension n over $\mathbb{F}_q$ are equivalent.*
(4) If f is symmetric bilinear with quadratic form Q and n is even, then $U = 0$ or $\dim(U) = 2$. *For each n there are exactly two isometry classes of orthogonal geometries over $\mathbb{F}_q$, which are distinguished by* $\dim(U)$.

In Theorem 3.3.1 (4), the quadratic form Q and the corresponding geometry is said to be of *plus type* if $U = 0$, and of *minus type* if $\dim(U) = 2$. The order of the isometry group of (V, f) or (V, Q) is determined by counting the number of possible bases $\{x_1, \ldots, x_{n/2}, y_1, \ldots, y_{n/2}\}$ satisfying the conditions of Theorem 3.3.1; these orders are given in Table 3.3.2.

The group of isometries of (V, ϕ) is called the *symplectic group* if ϕ is symplectic, the *unitary group* if ϕ is unitary, and the *orthogonal group* if ϕ is nonsingular quadratic. Following the convention of [**31**], we denote the isometry group by $\mathrm{I}(V)$, $\mathrm{I}(V, \phi)$, $\mathrm{I}(n, q)$ or $\mathrm{I}(n, q, \phi)$, as convenient, where I is given in Table 3.3.1. *In particular, note that our notation for the unitary group is nonstandard* - in the literature, including [**31**], $\mathrm{U}(n, q)$ (or, in many cases, $\mathrm{GU}(n, q)$) denotes the unitary group on a vector space of dimension n over $\mathbb{F}_{q^2}$, whereas we use $\mathrm{U}(n, q)$ to refer to the unitary group on $\mathbb{F}_q^n$. Recall that if q is even and

ϕ	I
trivial	GL
symplectic	Sp
unitary	U
nonsingular quadratic, odd dimension	O
nonsingular quadratic, even dimension, plus type	O^+
nonsingular quadratic, even dimension, minus type	O^-

TABLE 3.3.1. Isometry groups $I(V, \phi)$

$\phi = Q$ is nonsingular quadratic, then the associated bilinear form f of Q is alternating, and any Q-isometry is an f-isometry. Observe that the restriction $Q : \mathrm{rad}(f) \to \mathbb{F}_q$ is semilinear with (trivial) kernel $\mathrm{rad}(Q)$, so $\dim(\mathrm{rad}(f)) = \dim\left(\mathrm{Im}\, Q|_{\mathrm{rad}(f)}\right) \leq 1$. If Q is nondegenerate then f is symplectic, so n is even and $O^{\pm}(n, q) < \mathrm{Sp}(n, q)$. If Q is degenerate (but nonsingular) then $\dim(\mathrm{rad}(f)) = 1$, and f induces a symplectic form f' on $V/\mathrm{rad}(f)$. So $n-1$ is even, that is, n is odd. It can be shown that the isometry groups of (V, Q) and $(V/\mathrm{rad}(f), f')$ are isomorphic, so $O(n, q) \cong \mathrm{Sp}(n-1, q)$. For this reason we only consider the case where Q is nondegenerate, so that n is even whenever q is even.

Group	Order
$\mathrm{Sp}(n, q)$	$q^{n^2/4} \prod_{i=1}^{n/2} (q^{2i} - 1)$
$\mathrm{U}(n, q)$	$q^{n(n-1)/4} \prod_{i=1}^{n} (q^{i/2} - (-1)^i)$
$\mathrm{O}(n, q)$	$2q^{(n-1)^2/4} \prod_{i=1}^{(n-1)/2} (q^{2i} - 1)$
$\mathrm{O}^+(n, q)$	$2q^{n(n-2)/4}(q^{n/2} - 1) \prod_{i=1}^{n/2-1} (q^{2i} - 1)$
$\mathrm{O}^-(n, q)$	$2q^{n(n-2)/4}(q^{n/2} + 1) \prod_{i=1}^{n/2-1} (q^{2i} - 1)$

TABLE 3.3.2. Orders of the isometry groups

The next theorem is a well-known and fundamental result on classical geometries, and which can be found in various sources such as [**31**, Proposition 2.1.6] and [**43**, Theorem 3.3].

Theorem 3.3.2 (Witt's Lemma)**.** *Let V be a vector space and ϕ a form on V, where ϕ is a symplectic, unitary, or nondegenerate quadratic form. Then any isometry between subspaces of V extends to an isometry of V.*

The following is a consequence of Witt's Lemma, and can also be found in [**44**].

Theorem 3.3.3. [**44**, Propositions 3.11, 5.12, 6.8 and 7.10] *Let $V = \mathbb{F}_q^n$ and ϕ a symplectic, unitary, or nondegenerate quadratic form on V. Then the orbits in $V^{\#}$ of the isometry group of (V, ϕ) are the sets S_λ for each $\lambda \in \mathrm{Im}\, \overline{\phi}$, where*

$$S_\lambda := \{v \in V^{\#} \mid \overline{\phi}(v) = \lambda\} \tag{3.3.1}$$

and

$$\overline{\phi}(v) = \begin{cases} f(v,v) & \text{if } \phi = f \text{ is symplectic or unitary;} \\ Q(v) & \text{if } \phi = Q \text{ is quadratic.} \end{cases} \tag{3.3.2}$$

PROOF. Let I be as given in Table 3.3.1, and let $v \in S_\lambda$. Then clearly $v^{\mathrm{I}(V)} \subseteq S_\lambda$. For any other $w \in S_\lambda$, define the map $g : \langle v \rangle \to \langle w \rangle$ by $\alpha v \to \alpha w$ for any $\alpha \in \mathbb{F}_q$. Then g is an isometry from $\langle v \rangle$ to $\langle w \rangle$, and by Theorem 3.3.2, g extends to an isometry of V. So $w \in v^{\mathrm{I}(V)}$, and thus $S_\lambda \subseteq v^{\mathrm{I}(V)}$. Therefore $S_\lambda = v^{\mathrm{I}(V)}$, and the sets S_λ are all the $\mathrm{I}(V)$-orbits in $V^\#$. □

Recall that if $\phi = f$ is symplectic then the map $\overline{\phi}$ in (3.3.2) is identically zero, so that $V^\# = S_0$ and $\mathrm{Sp}(V)$ is transitive on $V^\#$ by Theorem 3.3.3. For ϕ unitary or orthogonal, the image of $\overline{\phi}$ is given by the next result. Statement (2) of Lemma 3.3.4 follows from the arguments in the proof of [**31**, Lemma 2.5.2 (ii)], which we present here. We denote by $\mathbb{F}_q^\square$ the set of all squares in $\mathbb{F}_q^\#$, and by $\mathbb{F}_q^\boxtimes$ the set $\mathbb{F}_q^\# \setminus \mathbb{F}_q^\square$.

Lemma 3.3.4. *Let $V = \mathbb{F}_q^n$, ϕ a unitary or nondegenerate quadratic form on V, and $\overline{\phi}$ as in (3.3.2).*

(1) If ϕ is unitary then $\mathrm{Im}\,\overline{\phi} = \mathbb{F}_{q_0}$, the subfield of index 2 in $\mathbb{F}_q$.

(2) If ϕ is quadratic then $\mathrm{Im}\,\overline{\phi} = \mathbb{F}_q^\theta \cup \{\mathbf{0}\}$ for some $\theta \in \{\square, \boxtimes\}$ if $n = 1$, and $\mathrm{Im}\,\overline{\phi} = \mathbb{F}_q$ if $n \geq 2$.

PROOF. Suppose first that $\phi = f$ is unitary. Then $f(v,v)^{\sqrt{q}} = f(v,v)$ for any $v \in V$, so $\mathrm{Im}\,\overline{\phi} \leq \mathbb{F}_{q_0}$. Observe that Theorem 3.3.1 implies that V contains a nonsingular vector, say u. So $f(\alpha u, \alpha u) = \alpha^{\sqrt{q}+1} f(u,u) = \eta(\alpha) f(u,u)$ for any $\alpha \in \mathbb{F}_q$, where $\eta : \mathbb{F}_q \to \mathbb{F}_{q_0}$ is the norm map. Since η is surjective so is $\overline{\phi}$, which proves (1).

Now suppose that $\phi = Q$ is quadratic. If $n = 1$ then V is anisotropic, and for some nonsingular vector u we have $\mathrm{Im}\,\overline{\phi} = \{\alpha^2 Q(u) \mid \alpha \in \mathbb{F}_q\} = Q(u)\mathbb{F}_q^\square \cup \{0\}$. If $n \geq 2$ then Theorem 3.3.1 implies that the space V contains nonzero vectors x and y such that either $\{x, y\}$ is a hyperbolic pair, or $\langle x, y \rangle$ is a nondegenerate anisotropic subspace. If $\{x, y\}$ is a hyperbolic pair then $Q(x + \alpha y) = \alpha$ for all $\alpha \in \mathbb{F}_q$, so $\mathrm{Im}\,\overline{\phi} = \mathbb{F}_q$, as required. Suppose that $\langle x, y \rangle$ is anisotropic. Then in particular $Q(x) \neq 0$, and since $\langle x, y \rangle$ is nondegenerate we can choose y such that $f(x, y) = Q(x)$, where f is the associated bilinear form of Q. Then for all $\lambda \in \mathbb{F}_q$ we have $Q(\lambda x - y) = Q(x)(\lambda^2 - \lambda + \zeta)$, where $\zeta := Q(y)Q(x)^{-1}$. Now $Q(\lambda x - y) \neq 0$ since $\langle x, y \rangle$ is anisotropic, so the polynomial $P(X) := X^2 - X + \zeta$ is irreducible over $\mathbb{F}_q$. Let ω be a root of P in the extension field $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. Then ω^q is the other root of P, so $P(X) = (X - \omega)(X - \omega^q)$, which gives $\omega + \omega^q = 1$ and $\omega^{q+1} = \zeta$. Hence for any $\lambda, \mu \in \mathbb{F}_q$, we have $Q(\lambda x + \mu y) = Q(x)(\lambda^2 + \mu^2\zeta + \lambda\mu) = Q(x)\,\eta'(\lambda + \mu\omega)$, where $\eta' : \mathbb{F}_{q^2} \to \mathbb{F}_q$ is the norm map. Since η' is surjective so is $\overline{\phi}$. This completes the proof of (2). □

We are also interested in determining $\operatorname{Im}\overline{\phi}|_{\langle v\rangle^{\perp}}$ for any $v \in V^{\#}$. This is given in Corollary 3.3.5, which follows immediately from Lemma 3.3.4 and the following observations.

Suppose that f is a symplectic, unitary, or nondegenerate symmetric bilinear form on V with quadratic form Q. If $v \in V^{\#}$ is nonsingular, then $\langle v\rangle^{\perp}$ is nondegenerate, and by the remarks above, $V = \langle v\rangle \perp \langle v\rangle^{\perp}$. If v is singular then $\langle v\rangle$ is totaly singular, so that $\langle v\rangle \leq \langle v\rangle^{\perp}$. By the remarks in [**31**, pp. 17-18], the form f induces a nondegenerate form f_U, of the same type as f, on the space $U := \langle v\rangle^{\perp}/\langle v\rangle$, defined by $f_U(x+\langle v\rangle, y+\langle v\rangle) := f(x,y)$ for all $x, y \in \langle v\rangle^{\perp}$. For f symmetric bilinear, the quadratic form Q likewise induces a nondegenerate quadratic form Q_U on U, where $Q(x+\langle v\rangle) := Q(x)$ for all $x \in \langle v\rangle^{\perp}$, and f_U is the associated bilinear form of Q_U. It follows from Theorems 3.3.2 and 3.3.1 that all maximal totally isotropic subspaces of V have the same dimension, which, in all cases, is at most $n/2$, so in particular $v^{\perp}$ contains a nonsingular vector whenever $n \geq 3$.

Corollary 3.3.5. *Let $V = \mathbb{F}_q^n$, ϕ a unitary or nondegenerate quadratic form on V, $\overline{\phi}$ as in* (3.3.2), *and $v \in V^{\#}$.*

(1) Suppose that ϕ is unitary, and let $\mathbb{F}_{q_0}$ denote the subfield of $\mathbb{F}_q$ of index 2. Then $\operatorname{Im}\overline{\phi}|_{\langle v\rangle^{\perp}} = \mathbb{F}_{q_0}$ if v is nonsingular and $n \geq 2$, or if v is singular and $n \geq 3$.

(2) Suppose that ϕ is quadratic.

(i) If q is even, then $\operatorname{Im}\overline{\phi}|_{\langle v\rangle^{\perp}} = \mathbb{F}_q$ if v is nonsingular and $n \geq 2$, or if v is singular and $n \geq 3$.

(ii) If q is odd, then $\operatorname{Im}\overline{\phi}|_{\langle v\rangle^{\perp}} = \mathbb{F}_q$ if v is nonsingular and $n \geq 3$, or if v is singular and $n \geq 4$.

(iii) If v is singular and $n = 3$, then $\operatorname{Im}\overline{\phi}|_{\langle v\rangle^{\perp}} = \mathbb{F}_q^{\theta} \cup \{0\}$ for some $\theta \in \{\square, \boxtimes\}$.

Proof. This follows immediately from Lemma 3.3.4 applied to $\langle v\rangle^{\perp}$, and the remarks above. $\square$

Recall that for each dimension n, there are exactly two isometry classes of orthogonal geometries over $\mathbb{F}_q$. If n is even these are distinguished by the dimension of a maximal totally isotropic subspace (which is $n/2$ when Q is of plus type, and $(n-2)/2$ when Q is of minus type). If n is odd then there is a unique quadratic form up to similarity, and the isometry classes are distinguished by the value of $Q(u)$ (mod $\mathbb{F}_q^{\square}$), where $\langle u\rangle = U$, the 1-dimensional anisotropic subspace in part (3) of Theorem 3.3.1. Another way of distinguishing the two types of orthogonal geometries in odd characteristic for a given n is via the discriminant, which is defined as follows. Let f be the associated bilinear of Q, and let $\mathcal{B} := \{v_1, \ldots, v_n\}$ be a fixed ordered basis of V. If $f_{\mathcal{B}}$ is the matrix of f with respect to $\mathcal{B}$, the *discriminant* $D(Q)$ of Q is defined to be the coset of $\mathbb{F}_q^{\square}$ in $\mathbb{F}_q^{\#}$ which contains $\det f_{\mathcal{B}}$. The discriminant of a quadratic form is well defined, and for any n and q, where q is odd, two quadratic forms Q_1 and Q_2 are isometric if and only if $D(Q_1) = D(Q_2)$ [**31**, Proposition 2.5.10]. Moreover, we have the following from [**31**, Propositions 2.5.11 (ii) and 2.5.12].

Theorem 3.3.6. *Let $V = \mathbb{F}_q^n$ with q odd, and let Q be a nondegenerate quadratic form on V.*

(1) If $V = V_1 \perp \ldots \perp V_t$, where each V_i is a nondegenerate subspace of V, then

$$D(Q) = \prod_{i=1}^{t} D(Q|_{V_i}),$$

with the multiplication in the quotient group $\mathbb{F}_q^{\#}/\mathbb{F}_q^{\square}$.

(2) There is a basis $\mathcal{B}$ for V such that

$$f_{\mathcal{B}} = \begin{cases} I_n & \text{if } D(Q) = \mathbb{F}_q^{\square}; \\ \operatorname{diag}(\mu, 1, \ldots, 1) & \text{if } D(Q) = \mathbb{F}_q^{\boxtimes}, \end{cases}$$

where $\mu \in \mathbb{F}_q^{\#}$ and $\langle \mu \rangle = \mathbb{F}_q^{\#}$.

3.3.1. Other classical groups. A *semisimilarity* of (V, ϕ) is an element $g \in \Gamma\mathrm{L}(V)$ such that, for some $\gamma(g) \in \mathbb{F}_q^{\#}$ and $\overline{\sigma}(g) \in \operatorname{Aut}(\mathbb{F}_q)$ which both depend only on g,

$$f(u^g, v^g) = \gamma(g) f(u, v)^{\overline{\sigma}(g)} \quad \forall\, u, v \in V \tag{3.3.3}$$

if $\phi = f$ is symplectic or unitary, and

$$Q(v^g) = \gamma(g) Q(v)^{\overline{\sigma}(g)} \quad \forall\, v \in V$$

if $\phi = Q$ is quadratic. The set of semisimilarities of (V, ϕ) forms a subgroup of $\Gamma\mathrm{L}(V)$ which is denoted by $\Gamma\mathrm{I}(V)$ or $\Gamma\mathrm{I}(n, q)$, with I as given in Table 3.3.1. It can be shown that, with a suitable choice of basis, $\overline{\sigma}(g) = \sigma(g)$ for all $g \in \Gamma\mathrm{I}(V)$, where $\sigma(g)$ is as given in (3.2.1). Hence the map $\sigma : \Gamma\mathrm{I}(n, q) \to \operatorname{Aut}(\mathbb{F}_q)$ is an epimorphism whose kernel is the *similarity group* $\mathrm{GI}(n, q)$ of V, which we call the *general symplectic*, *general unitary* or *general orthogonal group*, according to the type of ϕ. The map $\gamma : \mathrm{GI}(n, q) \to \mathbb{F}_q^{\#}$ is an epimorphism whose kernel is the isometry group $\mathrm{I}(n, q)$.

If ϕ is unitary or orthogonal, the subgroup $\mathrm{I}(V) \cap \mathrm{SL}(V)$ of elements with determinant 1 is denoted by $\mathrm{SI}(V)$. If ϕ is symplectic then $\mathrm{Sp}(n, q) \leq \mathrm{SL}(n, q)$ for all even n, with equality if $n = 2$.

The next theorem further describes the relationship among the groups $\mathrm{I}(V)$, $\mathrm{GI}(V)$, and $\Gamma\mathrm{I}(V)$.

Theorem 3.3.7. [**31**, Propositions 2.3.4, 2.4.3, 2.6.2, 2.7.1] *Let $n \geq 2$ and let q be a prime power, subject to the appropriate restrictions such that $V = \mathbb{F}_q^n$ is equipped with a symplectic, unitary or nonsingular quadratic form ϕ. Let τ be the Frobenius automorphism*

I	$\mathrm{GI}(n,q)$	$\Gamma\mathrm{I}(n,q)$
Sp	$\begin{cases} \mathrm{I}(n,q) \times Z_{q-1} & \text{if } q \text{ is even} \\ \mathrm{I}(n,q) \rtimes \langle g \rangle & \text{if } q \text{ is odd,} \end{cases}$ $g = \begin{pmatrix} \mu I_{n/2} & 0 \\ 0 & I_{n/2} \end{pmatrix}$	$\mathrm{GI}(n,q) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$
U	$\mathrm{I}(n,q) \circ Z_{q-1} = (\mathrm{I}(n,q).Z_{q-1})/\langle \mu^{\sqrt{q}-1} I_{n/2} \rangle$	$\mathrm{GI}(n,q) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$
O	$\mathrm{I}(n,q) \circ Z_{q-1} = (\mathrm{I}(n,q).Z_{q-1})\,/\langle -I_{n/2} \rangle$	$\mathrm{GI}(n,q) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$
O^+	$\begin{cases} \mathrm{I}(n,q) \times Z_{q-1} & \text{if } q \text{ is even} \\ \mathrm{I}(n,q) \rtimes \langle g \rangle & \text{if } q \text{ is odd,} \end{cases}$ $g = \begin{pmatrix} \mu I_{n/2} & 0 \\ 0 & I_{n/2} \end{pmatrix}$	$\mathrm{GI}(n,q) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$
O^-	$\begin{cases} \mathrm{I}(n,q) \times Z_{q-1} & \text{if } q \text{ is even} \\ \mathrm{I}(n,q) \rtimes \langle h \rangle & \text{if } q \text{ is odd,} \end{cases}$ $h = \begin{cases} \mathrm{diag}(\underbrace{h_2, \ldots, h_2}_{n/2}) & \text{if } D(\phi) = \mathbb{F}_q^{\square} \\ \mathrm{diag}(h_1, \underbrace{h_2, \ldots, h_2}_{n/2-1}) & \text{if } D(\phi) = \mathbb{F}_q^{\boxtimes} \end{cases}$	$\begin{cases} \mathrm{GI}(n,q) \rtimes Z_{q-1} & \text{if } D(\phi) = \mathbb{F}_q^{\square} \\ \mathrm{GI}(n,q).\langle m\tau \rangle & \text{if } D(\phi) = \mathbb{F}_q^{\boxtimes}, \end{cases}$ $m = \mathrm{diag}(\mu^{(q-1)/2}, 1, \ldots, 1)$

TABLE 3.3.3. Similarity and semisimilarity groups

of $\mathbb{F}_q$, $\mu \in \mathbb{F}_q^{\#}$ *such that* $\mathbb{F}_q^{\#} = \langle \mu \rangle$, *and* $h_1 := \begin{pmatrix} 0 & \mu \\ 1 & 0 \end{pmatrix}$. *If* q *is odd, let* $\alpha, \beta \in \mathbb{F}_q^{\#}$ *such that* $\alpha^2 + \beta^2 = \mu$ *and* $h_2 := \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$. *Then* $\mathrm{GI}(n,q)$ *and* $\Gamma\mathrm{I}(n,q)$ *are as given in Table* 3.3.3.

The special orthogonal group $\mathrm{SO}(V)$ or $\mathrm{SO}^{\pm}(V)$ contains a subgroup of index 2, which is usually denoted by $\Omega(V)$ or $\Omega^{\pm}(V)$, as appropriate. For a more detailed description of this subgroup see [**31**, Section 2.5] or [**43**, Sections 3.7 and 3.8].

Let $\mathrm{X} \in \{\Omega, \Omega^{\pm}, \mathrm{SI}, \mathrm{I}, \mathrm{GI}, \Gamma\mathrm{I}\}$. Then $\mathrm{X}(V)$ modulo scalars yields the projective group $\mathrm{PX}(V)$. It is known that the simple classical groups are precisely the following:

$\mathrm{PSL}(n,q)$, $n \geq 2$, $(n,q) \neq (2,2), (2,3)$;
$\mathrm{PSp}(n,q)$, n even and $n \geq 4$, $(n,q) \neq (4,2)$;
$\mathrm{PSU}(n,q)$, $n \geq 3$, $(n,q) \neq (3,4)$;
$\mathrm{P}\Omega(n,q)$, $n \geq 7$, nq odd;
$\mathrm{P}\Omega^{\pm}(n,q)$, n even and $n \geq 8$.

3.3.2. Tensor products. Suppose that $V = U \otimes W$, where $U = \mathbb{F}_q^k$ and $W = \mathbb{F}_q^m$, possibly $k \neq m$. Recall from Section 3.1 that $\mathrm{GL}(U) \otimes \mathrm{GL}(W) \leq \mathrm{GL}(V)$; if U and W are equipped with forms ϕ_U and ϕ_W, respectively, then it can be shown analogously that,

$\mathrm{I}(U, \phi_U)$	$\mathrm{I}(W, \phi_W)$	$\mathrm{I}(U \otimes W, \phi_U \otimes \phi_W)$
Sp	O^{ϵ}	$\begin{cases} \mathrm{Sp} & \text{if the characteristic is odd;} \\ \mathrm{O}^{+} & \text{else} \end{cases}$
Sp	Sp	O^{+}
O^{ϵ_1}	O^{ϵ_2}	$\begin{cases} \mathrm{O}^{+} & \text{if } \epsilon_i = + \text{ for some } i, \text{ or } \epsilon_i = - \text{ for both } i; \\ \mathrm{O} & \text{if } \dim(U) \text{ and } \dim(W) \text{ are odd;} \\ \mathrm{O}^{-} & \text{else} \end{cases}$
U	U	U

TABLE 3.3.4. Tensor products of classical groups

under certain conditions, the inclusion $\mathrm{I}(U, \phi_U) \otimes \mathrm{I}(W, \phi_W) \leq \mathrm{I}(V, \phi_U \otimes \phi_W)$ holds, where $\phi_U \otimes \phi_W$ is a form on V defined below.

Assume that ϕ_U and ϕ_W are both bilinear or both conjugate-symmetric sesquilinear forms. Define the form $\phi_U \otimes \phi_W$ on V by

$$(\phi_U \otimes \phi_W)(u \otimes w, u' \otimes w') := \phi_U(u, u')\phi_W(w, w')$$

for all $u \otimes w$ and $u' \otimes w'$ in a tensor product basis of V (see Section 3.1), extended bilinearly if ϕ_U and ϕ_W are bilinear, and sesquilinearly if ϕ_U and ϕ_W are sesquilinear. Then $\phi_U \otimes \phi_W$ is bilinear or sesquilinear if ϕ_U and ϕ_W are both bilinear or both sesquilinear, respectively, and nondegenerate if and only if both ϕ_U and ϕ_W are nondegenerate. Hence $\phi_U \otimes \phi_W$ is unitary if ϕ_U and ϕ_W are both unitary. For the bilinear case, $\phi_U \otimes \phi_W$ is alternating if at least one of ϕ_U and ϕ_W is alternating, and $\phi_U \otimes \phi_W$ is symmetric if both ϕ_U and ϕ_W are symmetric.

Table 3.3.4 summarises the types of forms $\phi_U \otimes \phi_W$ that arise according to the various possibilities for ϕ_U and ϕ_W, and it presents the possible inclusions $\mathrm{I}(U, \phi_U) \otimes \mathrm{I}(W, \phi_W) \leq \mathrm{I}(V, \phi_U \otimes \phi_W)$. The details can be found in [**31**, Section 4.4] and [**43**, Section 3.10.5]. The symbol O^{ϵ} denotes any of O, O^{+} or O^{-}.

We can extend the above to tensor products of an arbitrary number of subspaces. If $V = U_1 \otimes \cdots \otimes U_t$ and ϕ_i is a nondegenerate form on U_i for each i, which are all bilinear or all sesquilinear, define $\phi_1 \otimes \cdots \otimes \phi_t$ by

$$\left(\otimes_{i=1}^{t} \phi_i\right) \left(\otimes_{i=1}^{t} u_i, \otimes_{i=1}^{t} w_i\right) = \prod_{i=1}^{t} \phi_i(u_i, w_i)$$

as $\otimes_{i=1}^{t} u_i$ and $\otimes_{i=1}^{t} w_i$ vary over a tensor product basis of V, extended bilinearly if the ϕ_i are bilinear, and sesquilinearly if they are sesquilinear. Then $\otimes_{i=1}^{t} \phi_i$ is a nondegenerate bilinear (respectively, sesquilinear) form on V. If the spaces (U_i, ϕ_i) are all isometric, then we can extend the results of Table 3.3.4 to the following (see [**31, 43**]):

$$\otimes_{i=1}^{t}\mathrm{Sp}(m,q) < \begin{cases} \mathrm{Sp}(m^t,q) & \text{if } qt \text{ odd;} \\ \mathrm{O}^{+}(m^t,q) & \text{else} \end{cases}$$

$$\otimes_{i=1}^{t}\mathrm{O}^{\epsilon}(m,q) < \begin{cases} \mathrm{O}(m^t,q) & \text{if } qm \text{ is odd;} \\ \mathrm{O}^{-}(m^t,q) & \text{if } \epsilon = - \text{ and } t \text{ is odd;} \\ \mathrm{O}^{+}(m^t,q) & \text{else} \end{cases}$$

$$\otimes_{i=1}^{t}\mathrm{U}(m,q) < \mathrm{U}(m^t,q)$$

3.4. The exceptional group $G_2(q)$ and its geometry

Throughout this section $U = \mathbb{F}_q^n$, where q is a power of 2 and $n = 6$.

Recall from Section 3.3 that there is a symplectic form f defined on U. It is known [**14, 43**] that the geometry of (U, f) admits a structure $\mathcal{H}(q)$, called a *generalised hexagon* with parameters (q, q), which is a point-line incidence structure whose incidence graph has diameter 6 and girth 12, such that each line contains $q+1$ points and each point lies in $q+1$ lines. The points of $\mathcal{H}(q)$ are the one-dimensional subspaces of U, and the lines are the totally isotropic two-dimensional subspaces of U. The group $G_2(q)$ is a subgroup of $\mathrm{Sp}(6,q)$ and acts on $\mathcal{H}(q)$.

Notation. Denote by $\mathcal{P}$ the point set of $\mathcal{H}(q)$ (equivalently, the set of one-dimensional subspaces of U); by $\mathcal{L}$ the line set of $\mathcal{H}(q)$; by $\mathcal{L}'$ the set of totally isotropic two-dimensional subspaces of U which are not in $\mathcal{L}$; and by $\mathcal{N}$ the set of nondegenerate two-dimensional subspaces of U.

Observe that $\mathcal{L} \cup \mathcal{L}' \cup \mathcal{N}$ comprises the set of all two-dimensional subspaces of U, and we have $|\mathcal{P}| = |\mathcal{L}| = (q^6-1)/(q-1)$, $|\mathcal{L}'| = q^2(q^6-1)/(q-1)$, and $|\mathcal{N}| = q^4(q^6-1)/(q^2-1)$, see [**14**, Section 5]. The following result describes the action of $G_2(q)$ on these sets and is proved in [**14**, Lemmas 5.1, 5.2 and 5.4] and [**13**, Lemma 3.1] for parts (1) and (2), respectively.

Lemma 3.4.1. *Let q be a power of 2 and let $\mathcal{P}$, $\mathcal{L}$, $\mathcal{L}'$ and $\mathcal{N}$ be as defined above.*

(1) The group $G_2(q)$ acts transitively on each of the sets $\mathcal{P}$, $\mathcal{L}$, $\mathcal{L}'$ and $\mathcal{N}$.
(2) The action of $G_2(q)$ on $\mathcal{P}$ has rank 4 with subdegrees 1, $q(q+1)$, $q^3(q+1)$ and q^5.

Following the notation of [**14**], for a fixed point X in $\mathcal{P}$, let $\Delta_i(X)$ $(i = 1, 2, 3)$ denote the set of points $Y \in \mathcal{P}$ which are at distance i from X in the point graph of $\mathcal{H}(q)$. Clearly,

$$\Delta_1(X) = \{Y \in \mathcal{P} \mid \langle X, Y\rangle \in \mathcal{L}\}.$$

The proof of Lemma 5.2 in [**14**] gives a description of each of the sets $\Delta_2(X)$ and $\Delta_3(X)$, which we state below as a lemma.

Lemma 3.4.2. *Let $X \in \mathcal{P}$ be fixed, and let $\Delta_2(X)$ and $\Delta_3(X)$ be as defined above. Then*

$$\Delta_2(X) = \left\{Y \in \mathcal{P} \mid \langle X, Y\rangle \in \mathcal{L}'\right\}$$

and

$$\Delta_3(X) = \{Y \in \mathcal{P} \mid \langle X, Y\rangle \in \mathcal{N}\}\,.$$

The action of $G_2(q)$ on the three-dimensional totally isotropic subspaces of U is also described in [**14**]. We give this in the next lemma.

Theorem 3.4.3. *The group $G_2(q)$ has two orbits on maximal totally isotropic subspaces of U (of dimension 3), with representatives W_3 and W_3' and lengths $(q^6-1)/(q-1)$ and $q^3(q^3+1)$, respectively. Furthermore:*

(1) there exists a unique point X of $\mathcal{H}(q)$ in W_3 such that W_3 is the union of all lines in $\mathcal{L}$ that pass through X; and

(2) no two points in W_3' lie in the same line of $\mathcal{H}(q)$. In other words, all two-dimensional subspaces of W_3' belong to $\mathcal{L}'$.

Proof. The first part is [**14**, Lemma 5.3]. Let U_3 be a totally isotropic three-dimensional subspace of U. If there is a two-dimensional subspace U_2 of U_3 such that $U_2 \in \mathcal{L}$, then (1) holds by line 5 of the proof of [**14**, Lemma 5.3]. Otherwise (2) holds. $\square$

3.4.1. Alternative definition of $G_2(q)$. The group $G_2(q)$ can also be defined as the automorphism group of the octonion algebra $\mathbb{O}$. Following [**43**, Section 4.4.3], $\mathbb{O}$ can be defined as the algebra over $\mathbb{F}_q$ with basis $\{x_1, \ldots, x_8\}$ and multiplication given by Table 3.4.1 (blank entries are $\mathbf{0}_{\mathbb{O}}$). Note that $x_4 + x_5 = \mathbf{1}$, and for each $x \in \mathbb{O}$ write

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	.	.	.	.	x_1	x_2	x_3	x_4
x_2	.	.	x_1	x_2	.	.	x_5	x_6
x_3	.	x_1	.	x_3	.	x_5	.	x_7
x_4	x_1	.	.	x_4	.	x_6	x_7	.
x_5	.	x_2	x_3	.	x_5	.	.	x_8
x_6	x_2	.	x_4	.	x_6	.	x_8	.
x_7	x_3	x_4	.	.	x_7	x_8	.	.
x_8	x_5	x_6	x_7	x_8	.	.	.	.

Table 3.4.1. Octonion algebra

$\overline{x} := x + \langle x_4 + x_5 \rangle$. The bilinear form B' defined on $\mathbb{O}$ by

$$B'(x_i, x_j) = \begin{cases} 1 & \text{if } i + j = 9; \\ 0 & \text{else} \end{cases}$$

induces an alternating bilinear form B on $U_0 := \langle x_4 + x_5 \rangle^{\perp} / \langle x_4 + x_5 \rangle$ defined by

$$B(\overline{x_i}, \overline{x_j}) = B'(x_i, x_j),$$

with respect to which $\{\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_6}, \overline{x_7}, \overline{x_8}\}$ form a symplectic basis. The points of the generalised hexagon $\mathcal{H}(q)$ are the one-dimensional subspaces in U_0, and the lines of $\mathcal{H}(q)$ are the two-dimensional subspaces $\langle \overline{x}, \overline{y} \rangle$ where the product of x and y in $\mathbb{O}$ is $\mathbf{0}_{\mathbb{O}}$ [**43**, Section 4.3.8]. Hence, for instance, $\langle \overline{x_1}, \overline{x_2} \rangle \in \mathcal{L}$ while $\langle \overline{x_2}, \overline{x_3} \rangle \in \mathcal{L}'$.

From the second definition we can obtain explicit descriptions of some elements of $G_2(q)$. Those that we use in our proofs in Subsection 4.3.3 are

$$r : (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \mapsto (x_1, x_3, x_2, x_4, x_5, x_7, x_6, x_8);$$
$$s : (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \mapsto (x_2, x_1, x_6, x_5, x_4, x_3, x_8, x_7);$$

and, for any $\lambda \in \mathbb{F}_q$,

$$\begin{aligned} E(\lambda) : {} & x_3 \mapsto x_3 + \lambda x_2, \quad x_7 \mapsto x_7 + \lambda x_6, \\ & x_i \mapsto x_i \text{ for all other } i; \\ F(\lambda) : {} & x_2 \mapsto x_2 + \lambda x_1, \quad x_4 \mapsto x_4 + \lambda x_3, \\ & x_5 \mapsto x_5 + \lambda x_3, \quad x_8 \mapsto x_8 + \lambda x_7, \\ & x_6 \mapsto x_6 + \lambda x_4 + \lambda x_5 + \lambda^2 x_3, \\ & x_i \mapsto x_i \text{ for all other } i. \end{aligned}$$

We also use the subgroup

$$T := \left\{ \operatorname{diag}(\lambda, \mu, \lambda\mu^{-1}, 1, 1, \lambda^{-1}\mu, \mu^{-1}, \lambda^{-1}) \,\middle|\, \lambda, \mu \in \mathbb{F}_q^{\#} \right\}$$

of $\mathrm{GL}(8, q)$. Observe that s, T, and the maps $F(\lambda)$ for all $\lambda \in \mathbb{F}_q$ stabilise $\langle x_1, x_2 \rangle$ (and consequently $\langle \overline{x_1}, \overline{x_2} \rangle$), while r, T, and all the $E(\lambda)$ stabilise $\langle x_2, x_3 \rangle$ (and $\langle \overline{x_2}, \overline{x_3} \rangle$). This fact will be useful later.

3.5. The transitive finite linear groups

By Theorem 4.1.1, the quotient-complete graphs which have at least three nontrivial complete normal quotients arise from transitive finite linear groups. All these groups were determined by C. Hering in [**25**], and are presented in Theorem 3.5.1 below.

Theorem 3.5.1. [**34**, Appendix 1] *Let U be a vector space of dimension d over $\mathbb{F}_p$, where p is prime, and let $H \leq \mathrm{GL}(d, p)$ where H acts transitively on $U^{\#}$. Then H is one* *of the types given in Table* 3.5.1*, or, setting* $q = p^{d/n}$ *for some divisor* n *of* d*,* H *belongs to one of the following classes:*

(1) $H \le \Gamma\mathrm{L}(1, q)$*,* $n = 1$*;*
(2) $H \trianglerighteq \mathrm{SL}(n, q)$*,* $n \ge 2$*;*
(3) $H \trianglerighteq \mathrm{Sp}(n, q)$*,* d *and* n *even;*
(4) $H \trianglerighteq G_2(q)$*,* $n = 6$ *and* $p = 2$*.*

	p	d	H
1	5, 7, 11, 23	2	$H \le N_{\mathrm{GL}(d,p)}(Q_8)$
2	11, 19, 29, 59	2	$H \trianglerighteq \mathrm{SL}(2, 5)$
3	3	4	$\mathrm{SL}(2, 5) \trianglelefteq H \le \Gamma\mathrm{L}(2, 9)$
4	3	4	$H \le N_{\mathrm{GL}(4,3)}(D_8 \circ Q_8)$
5	2	4	Alt (6)
6	2	4	Alt (7)
7	3	6	$\mathrm{SL}(2, 13)$

TABLE 3.5.1. Sporadic transitive finite linear groups

3.6. Aschbacher's classification

The subgroups of the finite classical groups are classified by Aschbacher's Theorem. In this result eight classes of subgroups are identified, and it is asserted that an arbitrary subgroup either belongs to one of these eight types or is almost simple and subject to certain conditions. Theorem 3.6.1 presents the original statement of this result, which concerns almost simple classical groups. The classes $\mathcal{C}_1$ to $\mathcal{C}_8$ are described in Subsection 3.6.1. The maximal subgroups of $\Gamma\mathrm{L}(n, q)$ and $\Gamma\mathrm{Sp}(n, q)$ are given in [**31**], and these are listed in Theorems 3.6.2 and 3.6.3, respectively.

Theorem 3.6.1 (Aschbacher's Theorem)**.** [**6, 30**] *Let* $G_0 \le \mathrm{P}\Gamma\mathrm{L}(n, q)$ *be a simple classical group and* $G_0 \le G \le \mathrm{P}\Gamma\mathrm{L}(n, q)$*. If* $H < G$ *such that* H *does not contain* G_0*, then either* H *is contained in one of the classes* $\mathcal{C}_1, \dots, \mathcal{C}_8$*, or the following hold:*

(1) $T \le H \le \mathrm{Aut}\,(T)$ *for some nonabelian simple group* T *(i.e.,* H *is almost simple).*
(2) If L *is the preimage of* T *in* $\mathrm{GL}(n, q)$*, then the representation of* L *is absolutely irreducible and cannot be realised over a proper subfield of* $\mathbb{F}_q$*.*
(3) If L *fixes a form on* $V(n, q)$ *then* G_0 *is the group* $\mathrm{PSL}(n, q)$*,* $\mathrm{PSp}(n, q)$*,* $\mathrm{PSU}(n, q)$*,* $\mathrm{P}\Omega(n, q)$*, or* $\mathrm{P}\Omega^{\pm}(n, q)$ *corresponding to the form.*

3.6.1. Description of the classes $\mathcal{C}_i$. Assume throughout that $V = \mathbb{F}_q^n$ and ϕ is a left-linear form on V which is one of the following: the trivial form, a symplectic form, a unitary form, or a nondegenerate quadratic form. For each i the description given refers to the members of $\mathcal{C}_i$.

Class $\mathcal{C}_1$: Reducible subgroups. Stabilisers of nontrivial proper subspaces U of V, where U is one of the following: a nondegenerate subspace not isometric to $U^\perp$; a nonsingular, totally isotropic one-dimensional subspace (which arises if ϕ is quadratic and $p = 2$); or a totally singular subspace.

Class $\mathcal{C}_2$: Imprimitive subgroups. Stabilisers of direct sum decompositions $V = \oplus_{i=1}^t U_i$, where $t \geq 2$, $U_i = \mathbb{F}_q^m$ for each i, $n = mt$, and one of the following holds:

(i) The U_i's are pairwise orthogonal and isometric.

(ii) The form ϕ is quadratic and p is odd, $t = 2$, $\dim(U_i)$ is odd, and U_1 and U_2 are orthogonal and similar.

(iii) The dimension n is even, $t = 2$, U_1 and U_2 are totally singular of dimension $n/2$. If ϕ is symplectic and $n = 4$ then p is odd.

Class $\mathcal{C}_3$: Superfield subgroups. Stabilisers of vector space structures $V = \mathbb{F}_{q^r}^{n/r}$ over an extension field $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$, where r varies over the prime divisors of n.

Class $\mathcal{C}_4$: Tensor product subgroups. Stabilisers of tensor product decompositions $V = U \otimes W$, where $U = \mathbb{F}_q^k$ and $W = \mathbb{F}_q^m$ with forms ϕ_U and ϕ_W, respectively, such that $\phi = \phi_U \otimes \phi_W$, (U, ϕ_U) and (W, ϕ_W) are non-isometric, $n = km$, and $k \neq m$.

Class $\mathcal{C}_5$: Subfield subgroups. Stabilisers of vector space structures $\mathbb{F}_q V_0$, where $V_0 = \mathbb{F}_{q^{1/r}}^n$ and $\mathbb{F}_{q^{1/r}}$ varies over the subfields of $\mathbb{F}_q$ of prime index r.

Class $\mathcal{C}_6$: Normalisers of symplectic-type subgroups. Groups with extraspecial normal subgroups R, where R varies over the groups in Table 3.6.1 such that r is a prime not equal to p and $n = r^t$, R acts irreducibly on V, and one of the following holds:

(i) The group R is of type 1 or type 2, and $q = p^e$ where e is the smallest integer such that $p^e \equiv 1 \pmod{|Z(R)|}$. The form ϕ is trivial if e is odd, and is unitary if e is even.

(ii) The form ϕ is symplectic, $q = p$, and R is of type 4.

(iii) The form ϕ is quadratic of plus type, $q = p$, and R is of type 3.

Class $\mathcal{C}_7$: Wreathed tensor product subgroups. Stabilisers of tensor product decompositions $V = \otimes_{i=1}^t U_i$, where $t \geq 2$, $U_i = \mathbb{F}_q^m$ with a form ϕ_i for each i, $n = mt$, $\phi = \otimes_{i=1}^t \phi_i$, and the spaces (U_i, ϕ_i) are all isometric.

Class $\mathcal{C}_8$: Classical subgroups. Groups $\Gamma\mathrm{I}(n, q, \phi_0)$, with I given in Table 3.3.1 corresponding to ϕ_0, as ϕ_0 varies over the $\mathbb{F}_q$-forms on V subject to one of the following:

(i) The form ϕ is trivial and ϕ_0 is quadratic with p odd, symplectic, or unitary.

(ii) The form ϕ is symplectic, $p = 2$, and ϕ_0 is quadratic with associated bilinear form ϕ.

In addition to these eight classes, we define the class $\mathcal{C}_9$ to consist of all subgroups which do not belong to $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_8$.

	r	R	T
Type 1	odd	$\underbrace{R_0 \circ \cdots \circ R_0}_{t}$, $R_0 := r_+^{1+2}$	$\mathrm{Sp}(2t, r)$
Type 2	2	$Z_4 \circ \underbrace{Q_8 \circ \cdots \circ Q_8}_{t}$	$\mathrm{Sp}(2t, 2)$
Type 3	2	$\underbrace{D_8 \circ \cdots \circ D_8}_{t}$	$\mathrm{O}^+(2t, 2)$
Type 4	2	$\underbrace{D_8 \circ \cdots \circ D_8}_{t-1} \circ Q_8$	$\mathrm{O}^-(2t, 2)$

TABLE 3.6.1. Normalisers of symplectic-type r-groups

3.6.2. Maximal subgroups of $\Gamma\mathrm{L}(n,q)$ and $\Gamma\mathrm{Sp}(n,q)$. In the following let τ denote the Frobenius automorphism of $\mathbb{F}_q$, with the action defined in (3.2.2).

Theorem 3.6.2. *If M is a maximal subgroup of $\Gamma\mathrm{L}(n,q)$ not containing $\mathrm{SL}(n,q)$, then M is one of the following groups:*

($\mathcal{C}_1$) $\left(\left[q^{m(n-m)}\right].(\mathrm{GL}(m,q) \times \mathrm{GL}(n-m,q))\right) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* $1 < m < n$*;*
($\mathcal{C}_2$) $(\mathrm{GL}(m,q) \wr \mathrm{Sym}\,(t)) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* $mt = n$*;*
($\mathcal{C}_3$) $\Gamma\mathrm{L}(m,q^r)$, *where r is prime and* $mr = n$*;*
($\mathcal{C}_4$) $(\mathrm{GL}(k,q) \otimes \mathrm{GL}(m,q)) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where $km = n$ and $k \neq m$, and the action of τ is defined with respect to a tensor product basis of* $\mathbb{F}_q^k \otimes \mathbb{F}_q^m$*;*
($\mathcal{C}_5$) $\left(\mathrm{GL}(n,q^{1/r}) \circ Z_{q-1}\right) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where $n \geq 2$, q is an rth power and r is prime;*
($\mathcal{C}_6$) $((Z_{q-1} \circ R).T) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where $n = r^t$ with r prime, q is the smallest power of p such that $q \equiv 1 \pmod r$, and R and T are as given in Table* 3.6.1*;*
($\mathcal{C}_7$) $(\mathrm{GL}(m,q) \wr_{\otimes} \mathrm{Sym}\,(t)) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where $m^t = n$ and the action of τ is defined with respect to a tensor product basis of* $\otimes_{i=1}^t \mathbb{F}_q^m$*;*
($\mathcal{C}_8$) $\Gamma\mathrm{O}(n,q)$ *or* $\Gamma\mathrm{O}^{\pm}(n,q)$ *with q odd,* $\Gamma\mathrm{Sp}(n,q)$*, or* $\Gamma\mathrm{U}(n,q)$*;*
($\mathcal{C}_9$) *the preimage of an almost simple group $H \leq \mathrm{P}\Gamma\mathrm{L}(n,q)$ satisfying conditions (1) and (2) of Theorem* 3.6.1.

Remark. In case ($\mathcal{C}_1$), the symbol $\left[q^{m(n-m)}\right]$ denotes the subgroup of all matrices with block structure $\begin{pmatrix} I_m & 0 \\ C & I_{n-m} \end{pmatrix}$, where C is an arbitrary $(n-m) \times m$ matrix over $\mathbb{F}_q$.

Theorem 3.6.3. *If M is a maximal subgroup of $\Gamma\mathrm{Sp}(n,q)$, then M is one of the following groups:*

($\mathcal{C}_1$.1) $([q-1].(\mathrm{Sp}(m,q) \times \mathrm{Sp}(n-m,q)) \rtimes \mathrm{Aut}\,(\mathbb{F}_q))$*;*
($\mathcal{C}_1$.2) $\left(\left[q^{m/2+mn-3m^2/2}\right].(\mathrm{GL}(m,q) \times \mathrm{GSp}(n-2m,q))\right) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$*;*
($\mathcal{C}_2$.1) $\left((\mathrm{Sp}(m,q)^t.[q-1].\mathrm{Sym}\,(t))\right) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* $m = n/t$*;*
($\mathcal{C}_2$.2) $(\mathrm{GL}(m,q).[2]) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* $m = n/2$*;*

($\mathcal{C}_3$.1) $(\mathrm{Sp}(m,q^r).[q-1]) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* r *is prime and* $m = n/r$*;*

($\mathcal{C}_3$.2) $\Gamma\mathrm{U}(m,q^2)$, *where* $m = n/2$ *and* q *is odd;*

($\mathcal{C}_4$) $(\mathrm{GSp}(k,q) \times \mathrm{GO}^{\epsilon}(m,q)) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* q *is odd and* $m \geq 3$*;*

($\mathcal{C}_5$) $\left(\mathrm{GSp}(n,q^{1/r}) \circ Z_{q-1}\right) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$

($\mathcal{C}_6$) $(Z_{q-1} \circ R)\,.\mathrm{O}^-(2t,2)$, *where* $q \geq 3$ *and is prime, and* R *is of type 4 in Table* 3.6.1*;*

($\mathcal{C}_7$) $(\mathrm{GSp}(m,q) \wr_{\otimes} \mathrm{Sym}\,(t)) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, *where* qt *is odd;*

($\mathcal{C}_8$) $\Gamma\mathrm{O}^{\pm}(n,q)$, *where* q *is even;*

($\mathcal{C}_9$) *the preimage of an almost simple group* $H \leq \mathrm{P}\Gamma\mathrm{L}(n,q)$ *satisfying conditions (1) and (2) of Theorem* 3.6.1*, with* L *symplectic.*

Remark. Assume that $V = \langle x_1, y_1\rangle \perp \ldots \perp \langle x_{n/2}, y_{n/2}\rangle$, where (x_i, y_i) is a hyperbolic pair for each i, and $\mathbb{F}_q^{\#} = \langle \mu \rangle$. Then in Theorem 3.6.3, the symbol $[q-1]$ denotes the group $\langle \delta_\mu \rangle$, where

$$\delta_\mu \;: x_i \mapsto \mu x_i,\; y_i \mapsto y_i$$

for all x_i and y_i. In case ($\mathcal{C}_1$.2) the group $\left[q^{m/2+mn-3m^2/2}\right]$ is generated by all maps $\alpha_{i,j}(\mu)$ and $\beta_{i,j}(\mu)$, with $1 \leq i \leq m < j \leq n/2$, where

$$\alpha_{i,j}(\mu) \;: y_i \mapsto y_i + \mu y_j,\; x_j \mapsto x_j - \mu x_i;$$

$$\beta_{i,j}(\mu) \;: y_i \mapsto y_i + \mu x_j,\, y_j \mapsto y_j + \mu x_i$$

and $\alpha_{i,j}(\mu)$, $\beta_{i,j}(\mu)$ fix all other basis vectors. Finally, in case ($\mathcal{C}_4$), GO^{ϵ} can be any of $\mathrm{GO}, \mathrm{GO}^+,$ or GO^-.

CHAPTER 4

Quotient-complete symmetric graphs

4.1. Overview and main results

In this chapter we explore the structure of quotient-complete graphs in the case where there are at least 3 distinct nontrivial complete normal quotients. That is to say, we consider Case (1) of Theorem 1 with $N = 1$. Recall from Definition 2.4.8 that Γ is G-quotient-complete if it has at least one proper nontrivial G-normal quotient, and if each of its proper nontrivial G-normal quotients is either a complete graph or an empty graph.

Our technical version of Theorem 2, given below, describes the structure of G when a G-symmetric, G-quotient complete graph has at least three nontrivial complete G-normal quotients.

Theorem 4.1.1. *Let Γ be a graph and $G \leq \mathrm{Aut}(\Gamma)$. The graph Γ is connected, G-symmetric and G-quotient-complete with at least three distinct, nontrivial, complete G-normal quotients if and only if $\Gamma \cong \mathrm{Cay}(V, S)$ and $G \cong T_V \rtimes G_0$, where:*

(1) $V = U \oplus U$, with $U = \mathbb{F}_p^d$ for some prime p and integer d,
(2) $G_0 = \{(h, h) \mid h \in H\} \leq \mathrm{GL}(V)$ for some $H \leq \mathrm{GL}(U)$ which is transitive on $U^\#$, and
(3) S is a G_0-orbit in $V^\#$ with $S = -S$ and $\langle S \rangle = V$.

In particular, either $H \leq \Gamma\mathrm{L}(1, q)$ (where $q = p^d$), or H and S are as in Tables 4.1.1 *or* 4.1.2*. Furthermore, Γ has exactly $|C_{\mathrm{GL}(U)}(H)|+2$ nontrivial complete G-normal quotients, each of which has order $|U|$.*

The rest of the chapter is organised as follows: In Section 4.2 we analyse the general structure of quotient-complete, symmetric graphs with at least 3 nontrivial complete normal quotients, and prove Theorem 2 and parts (1), (2) and (3) of Theorem 4.1.1. In Section 4.3 we consider the different cases which arise from (1), (2) and (3) of Theorem 4.1.1, corresponding to each possible transitive linear group H with $H \not\leq \Gamma\mathrm{L}(1, p^d)$, and we determine the entries of Tables 4.1.1 and 4.1.2. The diameter 2 graphs in Tables 4.1.1 and 4.1.2 are identified in Section 4.4. Finally, we consider the case where $H \leq \Gamma\mathrm{L}(1, p^d)$ in Section 4.5 — we do not treat this case completely, but rather we consider the subcases where H belongs to certain infinite families of subgroups of $\Gamma\mathrm{L}(1, p^d)$, and construct the graphs with the above properties which arise from these.

4.1.1. Tables. For Tables 4.1.1 and 4.1.2 we have $G \cong T_V \rtimes G_0$ and $\Gamma \cong \mathrm{Cay}(V, S)$, with G, V, G_0 and S as in Theorem 4.1.1 (1) – (3). The integer n is a divisor of d and $q = p^{d/n}$ such that H can be viewed as a subgroup of $\Gamma\mathrm{L}(n, q)$. The graphs marked with a "†" have diameter 2. In Table 4.1.1, V_λ, V_{ind} and $\alpha(H)$ are as defined in (4.3.1) to (3.2.1), respectively, while $A(\lambda)$, $C(\lambda)$, S_λ, $S_{\mathcal{L}}$, and $S_{\mathcal{L}'}$ are as in (4.3.3) to (4.3.7), respectively.

Table 4.1.2 lists the conjugacy class representatives of the possible groups H and the valency of the graphs Γ, which are grouped according to isomorphism class. For instance, in line 5 of Table 4.1.2, the group $H = N_{\mathrm{GL}(2,5)}(Q_8)$ has 42 orbits of length 96 which yield connected Cayley graphs, and all these graphs are isomorphic; in lines 42 and 43 the group H has 9 orbits of length 640, and the corresponding graphs are divided into two isomorphism classes of sizes 3 and 6. Unless otherwise stated, distinct lines of Table 4.1.2 correspond to distinct isomorphism classes of graphs. Wherever it is known, we use the symbol "$\subset$" to denote subgraphs; i.e., "$\Gamma(i) \subset \Gamma(j)$" means that the graphs in line i are subgraphs of graphs in line j. We do not check exhaustively for all such relationships, and wherever indicated, $\Gamma(i) \subset \Gamma(j)$ follows from the fact that the H-orbit corresponding to $\Gamma(i)$ is contained in the H-orbit corresponding to $\Gamma(j)$. Note also that $A(1)$, $A(3)$ and $A(4)$ are maximal subgroups of $N_{\mathrm{GL}(4,3)}(D_8 \circ Q_8)$. All entries of Table 4.1.2 were obtained using MAGMA [**1**].

	(n,q)	H	S	val (Γ)
†1	$n \geq 3$	$H \trianglerighteq \mathrm{SL}(n,q)$	V_{ind}	$(q^n-1)(q^n-q)$
†2			$\bigcup_{\lambda' \in A(\lambda)} V_{\lambda'}^{\#}$, $\lambda \notin \mathrm{Fix}(\alpha(H))$	$\lvert A(\lambda)\rvert (q^n-1)$
†3	n even	$H \trianglerighteq \mathrm{Sp}(n,q)$	S_0	$q\left(q^6-1\right)\left(q^4-1\right)$
†4			$\bigcup_{\lambda' \in C(\lambda)} S_{\lambda'}$, $\lambda \in \mathbb{F}_q^{\#}$	$\lvert C(\lambda)\rvert q^5\left(q^6-1\right)$
†5			$\bigcup_{\lambda' \in A(\lambda)} V_{\lambda'}^{\#}$, $\lambda \notin \mathrm{Fix}(\alpha(H))$	$\lvert A(\lambda)\rvert (q^n-1)$
†6	$n=6$, q even	$H \trianglerighteq G_2(q)$	$S_{\mathcal{L}}$	$q\left(q^6-1\right)\left(q^2-1\right)$
†7			$S_{\mathcal{L}'}$	$q^3\left(q^6-1\right)\left(q^2-1\right)$
†8			$\bigcup_{\lambda' \in C(\lambda)} S_{\lambda'}$, $\lambda \in \mathbb{F}_q^{\#}$	$\lvert C(\lambda)\rvert q^5\left(q^6-1\right)$
†9			$\bigcup_{\lambda' \in A(\lambda)} V_{\lambda'}^{\#}$, $\lambda \notin \mathrm{Fix}(\alpha(H))$	$\lvert A(\lambda)\rvert (q^n-1)$

TABLE 4.1.1. H as in Theorem 3.5.1 (2), (3), (4)

4.2. Examples and general structure

We first look at the general structure of quotient-complete symmetric graphs. Example 2.4.1 gives an infinite family of quotient-complete symmetric graphs with exactly one nontrivial complete normal quotient, while Examples 2.4.2 and 2.4.3 give infinite families of examples with exactly two nontrivial complete normal quotients. It should be emphasised that the property of quotient-completeness is dependent on the choice of the group G. For instance, recall from Example 2.4.2 that the full automorphism group of $\Sigma = K_n \times K_n$ is $H = \mathrm{Sym}\,(n) \wr \mathbb{Z}_2$. However, Σ does not have an H-normal complete quotient.

i	(n,q)	$H = H(i)$	val $(\Gamma(i))$	Class size	Comments
1	$(2,5)$	$H(1) < H(4)$, index 4	24	20	
2		$H(2) < H(4)$, index 4	24	20	$H(2) \not\cong H(1)$
3		$H(3) < H(4)$, index 2	48	10	
†4		$N_{\mathrm{GL}(2,5)}(Q_8)$	96	5	
5	$(2,7)$	$H(5) < H(7)$, index 3	48	42	
6		$H(6) < H(7)$, index 3	48	42	$H(6) \not\cong H(5)$
†7		$N_{\mathrm{GL}(2,7)}(Q_8)$	144	14	
8	$(2,11)$	$H(8) < H(9)$, index 2	120	110	
9		$N_{\mathrm{GL}(2,11)}(Q_8)$	240	55	
10	$(2,23)$	$N_{\mathrm{GL}(2,23)}(Q_8)$	528	506	
11	$(2,11)$	$H(11) < H(13)$, index 5	120	110	$H(11) \not\cong H(8)$
12		$H(12) < H(13)$, index 5	120	110	$H(12), H(8)$ conjugate under $\mathrm{GL}(2,11)$; $\Gamma(12) \cong \Gamma(8)$
13		$N_{\mathrm{GL}(2,11)}(\mathrm{SL}(2,5))$	600	22	
14	$(2,19)$	$N_{\mathrm{GL}(2,19)}(\mathrm{SL}(2,5))$	1080	114	
15	$(2,29)$	$H(15) < H(16)$, index 2	840	812	
16		$N_{\mathrm{GL}(2,29)}(\mathrm{SL}(2,5))$	1680	406	
17	$(2,59)$	$N_{\mathrm{GL}(2,59)}(\mathrm{SL}(2,5))$	3480	3422	

TABLE 4.1.2. H as in Table 3.5.1

The rest of this section considers quotient-complete, symmetric graphs with at least three nontrivial complete normal quotients. Two families of such graphs, having k nontrivial complete normal quotients with k greater than or equal to some given prime power, are given in the next example.

Example 4.2.1. Let $U = \mathbb{F}_q^n$ for some prime power q and integer n, $c = q^n$, and $V = U \oplus U$. In each case below, $\Gamma = \mathrm{Cay}(V,S)$ and $G = T_V \rtimes G_0$, where $G_0 = \{(h,h) \mid h \in H \leq \mathrm{GL}(U)\}$, and H and S are as given.

Suppose first that $n = 1$ and $c = q \geq 3$. Take $H = \mathrm{GL}(1,q) = \mathrm{GL}(U)$ (noting that $H \cong \mathbb{Z}_{q-1}$) and $S = \{(u,\lambda u) \mid u \in U^{\#}\}$ for some $\lambda \in \mathbb{F}_q^{\#}$. Then S is an orbit of G_0, so Γ is G-arc-transitive. The graph Γ is disconnected since $\langle S\rangle \neq V$ and each connected component is isomorphic to K_q. By Lemma 3.2.2 the minimal normal subgroups of G are precisely the groups T_W, where W is $\{\mathbf{0}_U\} \oplus U$ or $\{(u,\eta u) \mid u \in U\}$ for some $\eta \in \mathbb{F}_q$, and exactly one of these minimal normal subgroups is $T_{\langle S\rangle}$. We have $\Gamma_{T_{\langle S\rangle}} \cong \overline{K_q}$, while $\Gamma_{T_W} \cong K_q$ for the other q minimal normal subgroups T_W. Since distinct minimal normal subgroups yield distinct normal quotients, Γ has exactly $q+1$ nontrivial G-normal quotients. So Γ is G-quotient-complete with q distinct, nontrivial, complete G-normal quotients.

Now suppose that $n = 2$, and take $H = \mathrm{GL}(2,q)$ and $S = \{(u,v) \mid \{u,v\}$ linearly independent in U$\}$. Again S is a G_0-orbit so Γ is G-arc-transitive; this time $\langle S\rangle = V$ so Γ is connected. As in (1) the minimal normal subgroups of G are the groups T_W with

i	(n, q)	H	val $(\Gamma(i))$	Class size	Comments
18	$(2, 9)$	$A(1) < N_{\Gamma L(2,9)}(SL(2, 5))$, index 6; $A(1) \not\leq GL(2, 9)$	80	6	$\Gamma(18) \subset \Gamma(31)$
†19			160	24	$\Gamma(19) \subset \Gamma(33)$
20			160	12	$\Gamma(20) \subset \Gamma(26) \subset \Gamma(33)$;
21		$A(2) < A(4)$, index 2; $A(2) \not\leq GL(2, 9)$	80	6	$\Gamma(21) \cong \Gamma(27) \subset \Gamma(31)$ $\Gamma(21) \subset \Gamma(42)$
22			240	8	$\Gamma(22) \cong \Gamma(44) \subset \Gamma(47)$; $\Gamma(22) \subset \Gamma(26), \Gamma(49)$
†23			240	6	$\Gamma(23) \subset \Gamma(29) \subset \Gamma(33)$; $\Gamma(23) \subset \Gamma(49)$
†24			240	4	$\Gamma(24) \subset \Gamma(30) \subset \Gamma(33)$; $\Gamma(24) \subset \Gamma(47), \Gamma(49)$
25			240	6	$\Gamma(25) \subset \Gamma(33), \Gamma(42)$
26		$A(3) < N_{\Gamma L(2,9)}(SL(2, 5))$, index 2; $A(3) \leq GL(2, 9)$	480	12	$\Gamma(26) \cong \Gamma(28) \cong \Gamma(32)$ $\Gamma(26) \subset \Gamma(33)$
27		$A(4) < N_{\Gamma L(2,9)}(SL(2, 5))$, index 2; $A(4) \not\leq GL(2, 9)$	80	6	$\Gamma(27) \cong \Gamma(21)$
†28			480	4	$\Gamma(28) \cong \Gamma(26) \cong \Gamma(32)$
†29			480	6	$\Gamma(29) \subset \Gamma(33)$
†30			480	2	$\Gamma(30) \subset \Gamma(33)$
†31		$N_{\Gamma L(2,9)}(SL(2, 5))$	160	3	
†32			480	4	$\Gamma(32) \cong \Gamma(26) \cong \Gamma(28)$
†33			960	4	
34	$(4, 3)$	$B(1) < N_{GL(4,3)}(D_8 \circ Q_8)$, index 16			$B(1)$, $A(2)$ conjugate under $GL(4, 3)$
35		$B(2) < B(3)$, index 2	80	6	$\Gamma(35) \cong \Gamma(38) \subset \Gamma(44)$ $\subset \Gamma(47)$
36			160	12	$\Gamma(36) \subset \Gamma(39) \subset \Gamma(42)$
37			160	24	$\Gamma(37) \subset \Gamma(40) \subset \Gamma(46)$ $\subset \Gamma(49)$
38		$B(3) < B(5)$, index 6	80	6	$\Gamma(38) \subset \Gamma(44) \subset \Gamma(47)$
†39			320	6	$\Gamma(39) \subset \Gamma(42)$
40			320	12	$\Gamma(40) \subset \Gamma(46) \subset \Gamma(49)$
†41		$B(4) < N_{GL(4,3)}(D_8 \circ Q_8)$, index 6	160	3	$\Gamma(41) \subset \Gamma(47)$
†42			640	3	$\Gamma(42) \cong \Gamma(45) \cong \Gamma(48)$
†43			640	6	$\Gamma(43) \subset \Gamma(49)$
44		$B(5) < N_{GL(4,3)}(D_8 \circ Q_8)$, index 2	240	2	$\Gamma(44) \cong \Gamma(22) \subset \Gamma(26), \Gamma(49)$; $\Gamma(44) \subset \Gamma(47)$
†45			640	3	$\Gamma(45) \cong \Gamma(42) \cong \Gamma(48)$
†46			1920	2	$\Gamma(46) \subset \Gamma(49)$
†47		$N_{GL(4,3)}(D_8 \circ Q_8)$	480	1	
†48			640	3	$\Gamma(48) \cong \Gamma(42) \cong \Gamma(45)$
†49			3840	1	

TABLE 4.1.2 (cont.). H as in Table 3.5.1

$W = \{\mathbf{0}_U\} \oplus U$ or $\{(u, \eta u) \mid u \in U\}$ for $\eta \in \mathbb{F}_q$. For each minimal normal subgroup T_W, the graph Γ_{T_W} is connected and G_0 acts transitively on $V(\Gamma_{T_W}) \setminus \{W\}$, so Γ_{T_W} is the

i	(n,q)	H	val $(\Gamma(i))$	Class size	Comments
†50	(4,2)	Alt (6)	120	1	$\Gamma(38) \subset \Gamma(40)$
†51			90	1	$\Gamma(39) \subset \Gamma(40)$
†52		Alt (7)	210	1	
53	(6,3)	SL(2, 13)	728	6	
54			2184	6	
55			2184	2	possibly isomorphic to $\Gamma(56)$
56			2184	6	possibly isomorphic to $\Gamma(55)$
57			2184	6	
58			2184	24	
59			2184	12	
60			2184	12	
61			2184	24	possibly isomorphic to $\Gamma(62)$, $\Gamma(63)$
62			2184	12	possibly isomorphic to $\Gamma(61)$, $\Gamma(63)$
63			2184	12	possibly isomorphic to $\Gamma(61)$, $\Gamma(62)$
64			2184	24	
65			2184	12	
66			2184	12	
67			2184	12	
68			2184	12	possibly isomorphic to $\Gamma(69)$
69			2184	24	possibly isomorphic to $\Gamma(68)$
70			2184	8	
71			2184	12	
72			2184	8	

TABLE 4.1.2 (cont.). H as in Table 3.5.1

complete graph K_c. Therefore Γ is G-quotient-complete with $q+1=\sqrt{c}+1$ distinct, nontrivial complete G-normal quotients. □

The remainder of this section is devoted to the proof of Theorem 2 and part of Theorem 4.1.1. Recall that if Γ_N is a complete G-normal quotient of Γ, the group G^{Γ_N} acts 2-transitively on $V(\Gamma_N)$. For the rest of the section we assume that the following hypothesis holds.

Hypothesis 4.2.2. The graph Γ is G-arc-transitive and G-quotient-complete with exactly $k \geq 3$ distinct nontrivial, complete G-normal quotients.

Lemma 4.2.3. *Let Γ be a graph and let $G \leq \mathrm{Aut}(\Gamma)$, such that Γ and G satisfy Hypothesis 4.2.2. Let M and N be nontrivial normal subgroups of G which are intransitive on $V(\Gamma)$, such that Γ_M and Γ_N are complete graphs and $\Gamma_M \neq \Gamma_N$. Then the following hold:*

(1) If $1 \neq K \lhd G$ and $K \leq M$, then $\Gamma_K = \Gamma_M$.
(2) $M \cap N = 1$ and MN is transitive on $V(\Gamma)$.
(3) If M is a minimal normal subgroup of G, then $M \cong M^{\Gamma_N} = \mathrm{soc}(G^{\Gamma_N})$.

Proof. Let $1 \neq K \lhd G$ with $K \leq M$. Since Γ_M is complete, the quotient Γ_K is not an empty graph, so by Definition 2.4.8 the graph Γ_K is complete. Hence G^{Γ_K} is 2-transitive and is thus primitive. Since $M^{\Gamma_K} \lhd G^{\Gamma_K}$, it follows that either M^{Γ_K} is transitive or M^{Γ_K} lies in the kernel of the action of G on $V(\Gamma_K)$. If M^{Γ_K} is transitive then M^{Γ} must also be transitive, contrary to the assumption. So M^{Γ_K} must lie in the kernel of the action of G on $V(\Gamma_K)$, and since $K \leq M$ it follows that the K-orbits and M-orbits in $V(\Gamma)$ coincide. In particular, $\Gamma_K = \Gamma_M$, which proves (1).

Suppose that $M \cap N \neq 1$. Then $M \cap N$ is a nontrivial normal subgroup of G contained in both M and N, and by (1) we have $\Gamma_M = \Gamma_{M\cap N} = \Gamma_N$, a contradiction. Therefore $M \cap N = 1$. Now $MN \trianglelefteq G$ and $M, N \leq MN$. If MN is intransitive on $V(\Gamma)$ then again by (1) we have $\Gamma_M = \Gamma_{MN} = \Gamma_N$, a contradiction. So MN is transitive on $V(\Gamma)$, which proves (2).

Suppose that M is minimal normal in G. Let $\widehat{N}$ denote the kernel of the action of G on $V(\Gamma_N)$, so that $M^{\Gamma_N} = M\widehat{N}/\widehat{N}$. Since $M \cap \widehat{N} = 1$ by (2), it follows that $M^{\Gamma_N} \cong M$ and $M\widehat{N} \cong M \times \widehat{N}$. Observe that each subgroup R satisfying $\widehat{N} \leq R \leq M\widehat{N}$ has the form $R = (R \cap M)\widehat{N}$. If M^{Γ_N} is not minimal normal in G, there exists $1 \neq L \trianglelefteq G^{\Gamma_N}$ with $L < M^{\Gamma_N}$. Then $L = L'/\widehat{N}$ for some $L' \trianglelefteq G$ with $\widehat{N} < L' < M\widehat{N}$. By the observation above we have $L' = (L' \cap M)\widehat{N}$. Hence $1 \neq L' \cap M \lhd G$ and $L' \cap M \neq M$, contrary to the minimality of M. So M^{Γ_N} must be minimal normal in G^{Γ_N}, and hence $M = \mathrm{soc}(G^{\Gamma_N})$ by Theorem 1.3.3. Therefore (3) holds. □

Proposition 4.2.4. *Let Γ be a graph and let $G \leq \mathrm{Aut}(\Gamma)$, such that Γ and G satisfy Hypothesis 4.2.2. Let L, M and N be vertex-intransitive minimal normal subgroups of G, such that Γ_L, Γ_M and Γ_N are complete and pairwise distinct. Then the following hold:*

(1) $L \cong M \cong N$ and L, M and N are elementary abelian;
(2) $|L| = |M| = |N| =: c$ and $\Gamma_L \cong \Gamma_M \cong \Gamma_N \cong K_c$;
(3) $|V(\Gamma)| = c^2$; and
(4) $\mathrm{soc}(G) = M \times N$ and acts regularly on $V(\Gamma)$.

Proof. The first statement follows easily from Lemma 4.2.3 (3) since we then have $M \cong M^{\Gamma_L} = \mathrm{soc}(G^{\Gamma_L}) = N^{\Gamma_L} \cong N$, and similarly $L \cong M$ and $L \cong N$. By Theorem 1.3.3, $\mathrm{soc}(G^{\Gamma_L})$ is either regular and elementary abelian, or is nonregular, nonabelian and simple. Suppose that $\mathrm{soc}(G^{\Gamma_L})$ is nonregular, nonabelian and simple, and let $T := \mathrm{soc}(G^{\Gamma_L})$. Since $M^{\Gamma_L} = N^{\Gamma_L} = T$ as observed above, it follows that $(MN)^{\Gamma_L} = T$ and $MN \cong T \times T$. So the kernel K of the action of MN on $V(\Gamma_L)$ is a normal subgroup of MN with $K \cong T$. The only such normal subgroups of MN are M and N. Each is impossible since M^{Γ_L} and N^{Γ_L} are both nontrivial. Therefore T is elementary abelian, and hence so are L, M and N. This proves (1).

Let $c := |T| = |M| = |N|$. By Lemma 4.2.3 (3), the groups M^{Γ_N}, M^{Γ_L} and N^{Γ_M} are minimal normal subgroups of G^{Γ_N}, G^{Γ_L} and G^{Γ_M}, respectively, and are abelian and regular by Theorem 1.3.3. Thus $|V(\Gamma_N)| = \left|M^{\Gamma_N}\right| = |M| = c$, and similarly $|V(\Gamma_M)| = |V(\Gamma_L)| = c$. It follows from Hypothesis 4.2.2 that $\Gamma_L \cong \Gamma_M \cong \Gamma_N \cong K_c$, which proves (2).

Now let $\alpha \in V(\Gamma)$. Since M^{Γ_N} is regular, we have $(M \times N)_{\alpha^N} = N$, and likewise $(M \times N)_{\alpha^M} = M$. Hence $(M \times N)_\alpha \leq (M \times N)_{\alpha^M} \cap (M \times N)_{\alpha^N} = M \cap N = 1$, and so $M \times N$ is semiregular. Moreover, $M \times N$ is transitive by Lemma 4.2.3 (2), so $M \times N$ is regular. Therefore $|V(\Gamma)| = |M \times N| = c^2$, and (3) holds.

Finally, observe that the group $M \times N$ is self-centralising since it is both transitive and elementary abelian. Any minimal normal subgroup of G is then contained in $M \times N$, so $M \times N = \mathrm{soc}(G)$. Therefore (4) holds. □

Proposition 4.2.5. *Let Γ be a graph and let $G \leq \mathrm{Aut}\,(\Gamma)$, such that Γ and G satisfy Hypothesis 4.2.2. Then there exists an integer d and prime p such that $G \leq \mathrm{AGL}(V)$ and $\Gamma \cong \mathrm{Cay}(V, S)$, where $V = U \oplus U$, $U = \mathbb{F}_p^d$, and S is a G_0-orbit in $V^\#$ with $S = -S$. Furthermore:*

- *(1) $G \cong T_V \rtimes G_0$, where $G_0 = \{(h, h) \mid h \in H\} \leq \mathrm{GL}(V)$ for some $H \leq \mathrm{GL}(U)$ which is transitive on $U^\#$.*
- *(2) If Γ is not connected then $\Gamma \cong c.K_c$ where $c = p^d$, and the component containing $\mathbf{0}_V$ is $\mathrm{Cay}(W, W^\#)$ where W is a G_0-invariant diagonal subspace distinct from $\{(u, u) \mid u \in U\}$.*

Proof. Let $K := \mathrm{soc}(G)$. By Proposition 4.2.4 (4) the group K^Γ is regular, so by Theorem 2.2.4 we have $\Gamma \cong \mathrm{Cay}(K, S)$ for some Cayley subset S of V — that is, (using additive notation) $S \subseteq K^\#$ with $S = -S$. By Theorem 1.1.8 we have $G \leq K \rtimes \mathrm{Aut}\,(K)$, and since Γ is G-arc-transitive, S is a G_0-orbit. Furthermore, by Proposition 4.2.4 (1) and (4), we have $K \cong T \times T$ for some elementary abelian group T, so K can be identified with $V = \mathbb{F}_p^d \oplus \mathbb{F}_p^d$ for some prime p and integer d with $p^d = |T|$. Under this identification $\mathrm{Aut}\,(K)$ corresponds to $\mathrm{GL}(V)$, and if we further identify V with T_V, the group G then corresponds to a subgroup of $\mathrm{AGL}(V)$. In particular, $G \cong T_V \rtimes G_0$ where $G_0 \leq \mathrm{GL}(V)$.

To complete the proof of (1) it remains to show that G_0 has the given form. Let $U = \mathbb{F}_p^d$. Observe that under the identification above the groups $T_{U \oplus \{\mathbf{0}_U\}}$ and $T_{\{\mathbf{0}_U\} \oplus U}$ correspond to the subgroups M and N in Proposition 4.2.4 (4), and hence are minimal normal in G. Write $M = T_{U \oplus \{\mathbf{0}_U\}}$ and $N = T_{\{\mathbf{0}_U\} \oplus U}$, and note that $K = M \times N$ by Proposition 4.2.4 (4). Since $k \geq 3$ there exists another minimal normal subgroup L of G which is distinct from M and N. By Lemma 3.2.2 the corresponding subspace V_L is G_0-invariant and diagonal; without loss of generality assume that $V_L = \{(u, u) \mid u \in U\}$. Then also by Lemma 3.2.2 we have $G_0 = \{(h, h) \mid h \in H\}$ for some $H \leq \mathrm{GL}(U)$ which acts irreducibly on $U^\#$. Since $G^{\Gamma_L} \cong L.G_0^{\Gamma_L}$ and is arc-transitive, it follows that $G_0^{\Gamma_L}$ is transitive on $V_L^\#$. Hence H is transitive on $U^\#$, and (1) holds.

Suppose now that Γ is not connected. Then $\langle S\rangle \neq V$. Thus by Lemma 3.2.3 and the previous paragraph, $\langle S\rangle^{\#} = S$ and $\langle S\rangle$ is a G_0-invariant diagonal subspace distinct from V_L. (Indeed, S is not $U \oplus \{\mathbf{0}_U\}$, $\{\mathbf{0}_U\} \oplus U$ or V_L since Γ_M, Γ_N and Γ_L are assumed to be complete.) If we write $W = \langle S\rangle$ then $\Gamma \cong \mathrm{Cay}(V, W^{\#})$. Clearly the connected component containing $\mathbf{0}_V$ is $\mathrm{Cay}(W, W^{\#})$, which is a complete graph of order $|W| = |U| = p^d$. Since $|V(\Gamma)| = p^{2d}$ and Γ is G-arc-transitive, it has p^d connected components which are all isomorphic to $\mathrm{Cay}(W, W^{\#})$. Therefore $\Gamma \cong c.K_c$ where $c = p^d$. This proves (2). $\square$

Corollary 4.2.6. *Let Γ be a graph and let $G \leq \mathrm{Aut}(\Gamma)$, such that Γ and G satisfy Hypothesis 4.2.2, and let H and $c = p^d$ be as in Proposition 4.2.5. Then $\left|C_{\mathrm{GL}(U)}(H)\right| = c^{1/\ell} - 1$ and $k = c^{1/\ell} + \delta$ for some integer $\ell \geq 1$, where*

$$\delta = \begin{cases} 1 & \text{if } \Gamma \text{ is connected,} \\ 0 & \text{if } \Gamma \text{ is not connected.} \end{cases}$$

Proof. Since H acts irreducibly on $U^{\#}$, it follows from Schur's Lemma (see, for instance, [**27**, Lemma IX.1.10]) that $\left|C_{\mathrm{GL}(U)}(H)\right| = p^m - 1$ for some divisor m of d, so $\left|C_{\mathrm{GL}(U)}(H)\right| = c^{1/\ell} - 1$ where $\ell = d/m$. Recall from Lemma 3.2.2 that the minimal normal subgroups of G are the subgroups $N \leq T_V$ where V_N is $U \oplus \{\mathbf{0}_U\}$, $\{\mathbf{0}_U\} \oplus U$, or a diagonal subspace $\{(u, u^{\varphi}) \mid u \in U\}$, $\varphi \in C_{\mathrm{GL}(U)}(H)$. By Lemma 4.2.3 (1) each nontrivial normal quotient of Γ is a quotient graph relative to a vertex-intransitive minimal normal subgroup N; conversely, it is clear from Lemma 3.2.2 that all minimal normal subgroups of G are vertex-intransitive, and distinct minimal normal subgroups yield distinct nontrivial normal quotients. So there is a one-to-one correspondence between the set of minimal normal subgroups of G and the set of nontrivial G-normal quotients of Γ, and Γ has exactly $\left|C_{\mathrm{GL}(U)}(H)\right| + 2 = c^{1/\ell} + 1$ distinct nontrivial G-normal quotients. Therefore $k \leq c^{1/\ell} + 1$.

If Γ is connected then so is Γ_N for all minimal normal subgroups N of G, so by Definition 2.4.8 the graphs Γ_N are all complete and $k = c^{1/\ell} + 1$ in this case. Suppose that Γ is not connected. Then by Proposition 4.2.5 we have $\Gamma \cong c.K_c$, and in particular $\Gamma \cong \mathrm{Cay}(V, S)$, where $T_{\langle S\rangle}$ is minimal normal in G. The connected components of Γ are the cosets of $\langle S\rangle$ in V. If $N = T_{\langle S\rangle}$ then $\Gamma_N \cong \overline{K_c}$; for any other minimal normal subgroup $N \neq T_{\langle S\rangle}$ the subspace V_N intersects each coset of $\langle S\rangle$ nontrivially, so $\Gamma_N \cong K_c$. Therefore $k = c^{1/\ell}$ for disconnected Γ, as asserted. $\square$

Lemma 4.2.7. *Let $\Gamma = \mathrm{Cay}(V, S)$ and $G = T_V \rtimes G_0$, where*

(1) $V = U \oplus U$ with $U = \mathbb{F}_q^n$ for some prime power q and integer n,

(2) $G_0 = \{(h, h) \mid h \in H\} \leq \mathrm{GL}(V)$ for some $H \leq \mathrm{GL}(U)$ which is transitive on $U^{\#}$, and

(3) S is a G_0-orbit in $V^{\#}$ with $S = -S$ and $\langle S\rangle = V$.

Then Γ *is a connected graph satisfying Hypothesis* 4.2.2 *with* $k = |C_{\mathrm{GL}(U)}(H)| + 2$*, and each nontrivial* G*-normal quotient of* Γ *is a complete graph of order* q^n*.*

Proof. It follows from condition (3) that Γ is undirected, connected, and G-arc-transitive. The group H is irreducible since it is transitive on $U^{\#}$, so $U \oplus \{\mathbf{0}_U\}$ and $\{\mathbf{0}_U\} \oplus U$ are minimal G_0-invariant subspaces, and $T_{U\oplus\{\mathbf{0}_U\}}$ and $T_{\{\mathbf{0}_U\}\oplus U}$ are minimal normal subgroups. By Lemma 3.2.2 the other minimal normal subgroups of G are precisely the subgroups T_W with $W = \{(u, u^{\varphi}) \mid u \in U\}$, for all $\varphi \in C_{\mathrm{GL}(U)}(H)$. As was observed in the proof of Corollary 4.2.6 above, Lemmas 3.2.2 and 4.2.3 (1) imply that the set of minimal normal subgroups of G is in one-to-one correspondence with the set of nontrivial G-normal quotients of Γ. Since Γ is connected all nontrivial normal quotients are complete graphs, so $k = |C_{\mathrm{GL}(U)}(H)| + 2$.

Let N be a minimal normal subgroup of G. The group G^{Γ_N} is transitive on $V(\Gamma_N)$ since G is transitive on $V(\Gamma)$ by assumption. We claim that the stabiliser $\left(G^{\Gamma_N}\right)_N$ of N in the action of G on $V(\Gamma_N)$ is transitive on $V(\Gamma_N)\setminus\{N\}$. Indeed, the subspace V_N is G_0-invariant by Lemma 3.2.2, so $(G_0)^{\Gamma_N} \le \left(G^{\Gamma_N}\right)_N$. Moreover, if M is minimal normal in G with $M \ne N$, the elements of V_M constitute a complete set of coset representatives for V_N in V. It follows from Lemma 3.2.2 and the transitivity of H that G_0 is transitive on $V_M^{\#}$, which implies that $(G_0)^{\Gamma_N}$ is transitive on $V(\Gamma_N) \setminus \{N\}$. Therefore $\left(G^{\Gamma_N}\right)_N$ is transitive on $V(\Gamma_N) \setminus \{N\}$ as claimed, and hence G^{Γ_N} acts 2-transitively on $V(\Gamma_N)$. Since Γ_N is connected for all minimal normal subgroups N it then follows that all nontrivial normal quotients Γ_N are complete. Therefore Γ is G-quotient-complete with $k = |C_{\mathrm{GL}(U)}(H)| + 2$. □

Proof of Theorem 2. The first part follows immediately from Proposition 4.2.5 (1) with $c = p^d$, so it remains only to show that either $k = c$ and $\Gamma \cong c.K_c$, or $k \le \sqrt{c} + 1$.

Recall from Proposition 4.2.5 that $\Gamma \cong \mathrm{Cay}(V, S)$ where $V = \mathbb{F}_p^d \oplus \mathbb{F}_p^d$ and $S \subseteq V^{\#}$ is a G_0-orbit with $S = -S$. It follows from Corollary 4.2.6 that there is an integer $\ell \ge 1$ with $k = c^{1/\ell} + 1$ if Γ is connected and $k = c^{1/\ell}$ otherwise. If $\ell \ge 2$ then $k \le \sqrt{c} + 1$, so we may assume that $\ell = 1$ and hence $k = c$ or $k = c + 1$ according as Γ is connected or not. Suppose that $k = c + 1$. Then Γ is connected, and all nontrivial G-normal quotients of Γ are complete. So k is equal to the number of minimal normal subgroups of G, which by Lemma 3.2.2 is less than or equal to the number of G_0-invariant subspaces of $V^{\#}$, which in turn is less than or equal to the number of G_0-orbits in $V^{\#}$. Since $|V| = c^2$ and H is transitive on $U^{\#}$, there are at most $c + 1$ G_0-orbits in $V^{\#}$ and each orbit has length at least $c - 1$. Thus G_0 has exactly $c + 1$ orbits in $V^{\#}$, each of length $c - 1$, and hence k is equal to the number of G_0-orbits in $V^{\#}$. This implies that each G_0-orbit generates $U \oplus \{\mathbf{0}_U\}$, $\{\mathbf{0}_U\} \oplus U$, or a G_0-invariant diagonal subspace. So $\langle S \rangle$ must be one of these subspaces and thus Γ is not connected, a contradiction. Therefore $k = c$ and Γ is not connected, and by Proposition 4.2.5 (2) we have $\Gamma \cong c.K_c$, which completes the proof. □

4.3. Connected quotient-complete symmetric graphs

In this section we determine most of the connected graphs which satisfy Hypothesis 4.2.2. In particular, we identify which of the graphs with form as given in Proposition 4.2.5 and Lemma 4.2.7 are connected, provided that $H \not\leq \Gamma\mathrm{L}(1,q)$ (see Theorem 3.5.1).

It follows from Proposition 4.2.5 and Lemma 4.2.7 that a connected graph Γ and group $G \leq \mathrm{Aut}\,(\Gamma)$ satisfy Hypothesis 4.2.2 if and only if Γ and G are as described in Lemma 4.2.7 (1) – (3). So to get the desired connected graphs Γ we only need to determine the G_0-orbits $S \subseteq V^{\#}$ such that $S = -S$ and $\langle S \rangle = V$.

Notation. Throughout this section U, V, G, G_0 and H are as in Lemma 4.2.7 (1) and (2). Set

$$V_\infty := \{\mathbf{0}_U\} \oplus U,$$

and for each $\lambda \in \mathbb{F}_q$,

$$V_\lambda := \{(u, \lambda u) \mid u \in U\}. \tag{4.3.1}$$

Thus, in particular, $V_0 = U \oplus \{\mathbf{0}_U\}$.

In cases (2) – (4) of Theorem 3.5.1, there exists a homomorphism $\sigma : H \to \mathrm{Aut}\,(\mathbb{F}_q)$, and it will be shown that $\left|C_{\mathrm{GL}(U)}(H)\right| = |\mathrm{Fix}(\sigma(H))| - 1$. So if $c = q^n$, Corollary 4.2.6 gives

$$k = c^{1/\ell} + \delta = \left|C_{\mathrm{GL}(U)}(H)\right| + 1 + \delta = |\mathrm{Fix}(\sigma(H))| + \delta \leq q + 1.$$

4.3.1. $\mathrm{SL}(n,q) \trianglelefteq H \leq \Gamma\mathrm{L}(n,q)$**,** $n \geq 3$**.** Recall that if $n \geq 3$ then $\mathrm{SL}(n,q)$ is transitive on the set

$$V_{ind} := \{(u, w) \mid u, w \in U \text{ linearly independent}\}, \tag{4.3.2}$$

whereas $\mathrm{SL}(2,q)$ is not. *Moreover* $\mathrm{SL}(2,q) = \mathrm{Sp}(2,q)$*, and this case is considered in Subsection* 4.3.2 *along with the other symplectic groups.* Thus from now on we assume that $n \geq 3$.

Recall from Section 3.2 that $\Gamma\mathrm{L}(n,q) = \mathrm{GL}(n,q) \rtimes \mathrm{Aut}\,(\mathbb{F}_q)$, so the group H consists of elements $h = \rho(h)\sigma(h)$ where $\rho(h) \in \mathrm{GL}(n,q)$ and $\sigma(h) \in \mathrm{Aut}\,(\mathbb{F}_q)$. Note that $\mathrm{SL}(n,q) \leq \rho(H) \leq \mathrm{GL}(n,q)$ and $\sigma(H) \leq \mathrm{Aut}\,(\mathbb{F}_q)$. So $G \geq K := \{(h,h) \mid h \in \mathrm{SL}(n,q)\}$, which has orbits V_{ind}, $V_\infty^{\#}$, and $V_\lambda^{\#}$ for all $\lambda \in \mathbb{F}_q$. Hence the G_0-orbits in $V^{\#}$ are V_{ind}, $V_\infty^{\#}$, and $\bigcup_{\lambda' \in A(\lambda)} V_{\lambda'}^{\#}$, where

$$A(\lambda) := \lambda^{\sigma(H)}. \tag{4.3.3}$$

It follows from Lemma 3.2.3 that the only G_0-orbits S with $\langle S \rangle = V$ are V_{ind} and $\bigcup_{\lambda' \in A(\lambda)} V_{\lambda'}^{\#}$ for all $\lambda \notin \mathrm{Fix}(\sigma(H))$, and there is a one-to-one correspondence between the set of all remaining orbits and the set of minimal normal subgroups of G. We thus have the following:

Proposition 4.3.1. *Let Γ be a graph and $G = T_V \rtimes G_0$, where V, T_V and G_0 are as in Lemma* 4.2.7 *(1) and (2) with $n \geq 3$ and $\mathrm{SL}(n,q) \trianglelefteq H \leq \Gamma\mathrm{L}(n,q)$. Then Γ is connected, G-symmetric and G-quotient-complete if and only if $\Gamma \cong \mathrm{Cay}(V,S)$ where S is one of the following:*

(1) V_{ind};

(2) $\bigcup_{\lambda' \in A(\lambda)} V^{\#}_{\lambda'}$ for some $\lambda \notin \mathrm{Fix}(\sigma(H))$.

Furthermore, such a graph Γ has exactly $k = |\mathrm{Fix}(\sigma(H))|+1$ nontrivial complete G-normal quotients.

Proof. This follows immediately from Proposition 4.2.5, Lemma 4.2.7, and the discussion above. □

Observe that for all Γ in Proposition 4.3.1, we have $k \leq q+1 \leq q^{n/3}+1$, which is less than the upper bound $\sqrt{q^n}+1$ of Theorem 2.

4.3.2. $\mathrm{Sp}(n,q) \trianglelefteq H \leq \Gamma\mathrm{L}(n,q)$**,** n **even.** Let f be the corresponding symplectic form on U. Recall that $g \in \Gamma\mathrm{L}(U)$ normalises $\mathrm{Sp}(n,q)$ if and only if there exist $\gamma(g) \in \mathbb{F}_q^{\#}$ and $\sigma(g) \in \mathrm{Aut}\,(\mathbb{F}_q)$, both independent of u and w, such that

$$f(u^g, w^g) = \gamma(g) f(u,w)^{\sigma(g)} \quad \forall\ u,w \in U.$$

Moreover, $\sigma(g)$ is the same as that defined in (3.2.1). For each $\lambda \in \mathbb{F}_q$ define

$$C(\lambda) := \left\{ \gamma(h)\lambda^{\sigma(h)} \mid h \in H \right\}. \tag{4.3.4}$$

We shall abuse notation slightly and define

$$S_\lambda := \{(u,w) \in V_{ind} \mid f(u,w) = \lambda\}, \tag{4.3.5}$$

where $A(\lambda)$ is as in (4.3.3) for each λ and V_{ind} is as in (4.3.2). Note that the sets S_λ in this case are different from the S_λ defined in (3.3.1). Clearly $\bigcup_{\lambda \in \mathbb{F}_q} S_\lambda = V_{ind}$, and it is known that S_0 is nonempty if and only if $n \geq 4$.

Lemma 4.3.2. *The G_0-orbits in $V^{\#}$ are $V^{\#}_\infty$, $\bigcup_{\lambda' \in A(\lambda)} V^{\#}_{\lambda'}$, and $\bigcup_{\lambda' \in C(\lambda)} S_{\lambda'}$ for all $\lambda \in \mathbb{F}_q$.*

Proof. Let $K = \{(h,h) \mid h \in \mathrm{Sp}(n,q)\}$ and $(u,w) \in V^{\#}$. If $\{u,w\}$ is linearly dependent in U then $(u,w)^K$ is either $V^{\#}_\infty$ or $V^{\#}_\lambda$ for some $\lambda \in \mathbb{F}_q$. Suppose that $\{u,w\}$ is linearly independent and let $\alpha \in \mathbb{F}_q$ satisfy $\alpha = f(u,w)$. Then clearly $(u,w)^K \subseteq S_\alpha$, and it remains to show that $S_\alpha \subseteq (u,w)^K$. Let $(u',w') \in S_\alpha$. Then there is a linear map $g : \langle u,w \rangle \to \langle u',w' \rangle$ such that $ug = u'$ and $wg = w'$, and g is an isometry from $\langle u,w \rangle$ to $\langle u',w' \rangle$. Thus by Witt's Lemma g extends to an isometry g' on U. That is, $(u',w') = (ug',wg')$ where $g' \in \mathrm{Sp}(n,q) \leq H$, so $(u',w') \in (u,w)^K$. Hence $S_\alpha \subseteq (u,w)^K$, and thus S_α is a K-orbit.

It follows immediately that $V_\infty^\#$, $\bigcup_{\lambda'\in A(\lambda)} V_{\lambda'}^\#$, and $\bigcup_{\lambda'\in C(\lambda)} S_{\lambda'}$ for all $\lambda \in \mathbb{F}_q$ are the G_0-orbits in $V^\#$. □

Proposition 4.3.3. *Let Γ be a graph and $G = T_V \rtimes G_0$, where V, T_V and G_0 are as in Lemma* 4.2.7 *(1) and (2), with n even and $\mathrm{Sp}(n,q) \trianglelefteq H \le \Gamma\mathrm{L}(n,q)$. Then Γ is connected, G-symmetric and G-quotient-complete if and only if $\Gamma \cong \mathrm{Cay}(V,S)$, where S is one of the following:*

(1) $\bigcup_{\lambda'\in A(\lambda)} V_{\lambda'}^\#$ for some $\lambda \notin \mathrm{Fix}(\sigma(H))$;
(2) $\bigcup_{\lambda'\in C(\lambda)} S_{\lambda'}$ for any $\lambda \in \mathbb{F}_q$.

Furthermore, such a graph Γ has exactly $k = |\mathrm{Fix}(\sigma(H))|+1$ nontrivial complete G-normal quotients. In particular, $k = \sqrt{q^n}+1$ if and only if $n = 2$ and $\sigma(H) = 1$.

Proof. This follows immediately from Proposition 4.2.5, Lemma 4.2.7, and the discussion above. □

4.3.3. $H \trianglerighteq G_2(q)$, $n = 6$ and q even. Recall from Section 3.4 that $G_2(q) \le \mathrm{Sp}(6,q)$. Let $\mathcal{P}$, $\mathcal{L}$, $\mathcal{L}'$ and $\mathcal{N}$ be as defined in Section 3.4, and let S_λ be as in (4.3.5) (with $n = 6$ and q even) for all $\lambda \in \mathbb{F}_q$. Define

$$S_{\mathcal{L}} := \{(u,w) \mid u,w \in U; \langle u,w\rangle \in \mathcal{L}\} \tag{4.3.6}$$

and

$$S_{\mathcal{L}'} := \{(u,w) \mid u,w \in U; \langle u,w\rangle \in \mathcal{L}'\}, \tag{4.3.7}$$

and for $\lambda \in \mathbb{F}_q$ let $A(\lambda)$ be as in (4.3.3) and $C(\lambda)$ be as in (4.3.4). Recall that $G_2(q) \le \mathrm{Sp}(6,q)$, and is transitive on $\mathcal{L}$, $\mathcal{L}'$ and $\mathcal{N}$ by Lemma 3.4.1 (1), so it follows that $S_{\mathcal{L}}$, $S_{\mathcal{L}'}$ and S_λ for any $\lambda \in \mathbb{F}_q^\#$ are K-invariant for $K := \{(h,h) \mid h \in G_2(q)\}$. In fact we show that:

Lemma 4.3.4. *The K-orbits in $V^\#$ are $V_\infty^\#$, $V_0^\#$, $V_\lambda^\#$ and S_λ for each $\lambda \in \mathbb{F}_q^\#$, $S_{\mathcal{L}}$, and $S_{\mathcal{L}'}$. Hence the G_0-orbits in $V^\#$ are $V_\infty^\#$, $V_0^\#$, $S_{\mathcal{L}}$, $S_{\mathcal{L}'}$, $\bigcup_{\lambda'\in A(\lambda)} V_{\lambda'}^\#$ and $\bigcup_{\lambda'\in C(\lambda)} S_{\lambda'}$ for all $\lambda \in \mathbb{F}_q^\#$.*

To prove Lemma 4.3.4 we need to determine the group induced on a two-dimensional subspace W of U by the setwise stabiliser in $G_2(q)$ of W. We denote this group by $G_2(q)_{\{W\}}^W$.

Lemma 4.3.5. *If W is a two-dimensional subspace of U then $G_2(q)_{\{W\}}^W \ge \mathrm{SL}(2,q)$. Moreover, if W is nondegenerate then $G_2(q)_{\{W\}}^W = \mathrm{SL}(2,q)$.*

Proof. The first statement is a direct consequence of Lemma 3.4.1, and knowledge of $|\mathcal{L}|$, $|\mathcal{L}'|$ and $|\mathcal{N}|$. The second statement follows from the fact that for nondegenerate W we have $G_2(q)_{\{W\}}^W \le \mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$ (since $G_2(q) \le \mathrm{Sp}(6,q)$). □

Lemma 4.3.6. *If W is a totally isotropic two-dimensional subspace of U then $G_2(q)^W_{\{W\}} = \mathrm{GL}(2,q)$.*

Proof. Let $\langle x_1,\dots,x_8\rangle$ be a basis for the octonion algebra with multiplication as given in Table 3.4.1, and let $E(\lambda)$, $F(\lambda)$, T, r and s be the elements of $G_2(q)$ as defined in Section 3.4.1. Recall that $\langle \overline{x_1},\overline{x_2}\rangle \in \mathcal{L}$ and $\langle \overline{x_2},\overline{x_3}\rangle \in \mathcal{L}'$. To simplify notation we identify each coset $\overline{x_i}$ of $\langle x_4+x_5\rangle$ with its representative x_i. As we observed earlier, the stabiliser of $\langle x_1,x_2\rangle$ contains the subgroup T, the map s, and all elements $F(\lambda)$. Relative to the ordered basis $\{x_1,x_2\}$ (and acting on row vectors), the maps s, $F(\lambda)$, and the elements of T acting on $\langle x_1,x_2\rangle$ induce the matrices

$$\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&\lambda\\0&1\end{pmatrix},\text{ and }\begin{pmatrix}\lambda'&0\\0&\mu\end{pmatrix},$$

respectively, for all $\lambda\in\mathbb{F}_q$ and $\lambda',\mu\in\mathbb{F}_q^{\#}$. Hence $\langle T,s,F(\lambda)\mid\lambda\in\mathbb{F}_q\rangle$ induces the group $\mathrm{GL}(2,q)$ on $\langle x_1,x_2\rangle$. Similarly, the stabiliser of $\langle x_2,x_3\rangle$ contains T, r, and all elements $E(\lambda)$, which respectively induce the matrices

$$\begin{pmatrix}\mu&0\\0&\lambda'\mu^{-1}\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\text{ and }\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}$$

for all $\lambda',\mu\in\mathbb{F}_q^{\#}$ and all $\lambda\in\mathbb{F}_q^{\#}$, on $\langle x_2,x_3\rangle$ relative to the ordered basis $\{x_2,x_3\}$. So $\langle T,r,E(\lambda)\mid\lambda\in\mathbb{F}_q\rangle$ also induces $\mathrm{GL}(2,q)$ on $\langle x_2,x_3\rangle$. □

Proof of Lemma 4.3.4. Let $(u,w)\in V^{\#}$. If $\{u,w\}$ is linearly dependent then $(u,w)^K$ is $V^{\#}_\infty$ or $V^{\#}_\lambda$ for some $\lambda\in\mathbb{F}_q$. Suppose that $\{u,w\}$ is linearly independent. If $\langle u,w\rangle$ is totally isotropic then $G_2(q)^{\langle u,w\rangle}_{\{\langle u,w\rangle\}}=\mathrm{GL}(2,q)$ by Lemma 4.3.6, so $G_2(q)_{\{\langle u,w\rangle\}}$ is transitive on the set of ordered bases of $\langle u,w\rangle$. Since $G_2(q)$ is transitive on $\mathcal{L}$ and $\mathcal{L}'$ it follows that K is transitive on $S_{\mathcal{L}}$ and $S_{\mathcal{L}'}$. If $\langle u,w\rangle$ is nondegenerate then $G_2(q)^{\langle u,w\rangle}_{\{\langle u,w\rangle\}}=\mathrm{SL}(2,q)=\mathrm{Sp}(2,q)$, so that the orbitals of $G_2(q)_{\{\langle u,w\rangle\}}$ in $\langle u,w\rangle$ are the sets

$$\{(u',w')\in S_\lambda\mid u',w'\in\langle u,w\rangle\}$$

for each $\lambda\in\mathbb{F}_q^{\#}$. Again, since $G_2(q)$ is transitive on the set of all nondegenerate two-dimensional subspaces, we have $(u,w)^K=S_\lambda$ where λ is the value of the symplectic form at (u,w). Hence the K-orbits in $V^{\#}$ are $V^{\#}_\infty$, $V^{\#}_0$, $V^{\#}_\lambda$ and S_λ for each $\lambda\in\mathbb{F}_q^{\#}$, $S_{\mathcal{L}}$, and $S_{\mathcal{L}'}$. It follows that the G_0-orbits are $V^{\#}_\infty$, $V^{\#}_0$, $S_{\mathcal{L}}$, $S_{\mathcal{L}'}$, $\bigcup_{\lambda'\in A(\lambda)}V^{\#}_{\lambda'}$ and $\bigcup_{\lambda'\in C(\lambda)}S_{\lambda'}$ for all $\lambda\in\mathbb{F}_q^{\#}$. □

Again by Lemma 3.2.3, the orbits $V^{\#}_\infty$ and $V^{\#}_\lambda$ (for all $\lambda\in\mathrm{Fix}(\sigma(H))$) correspond to disconnected graphs.

Proposition 4.3.7. *Let Γ be a graph and $G=T_V\rtimes G_0$, where V, T_V, and G_0 are as in Lemma 4.2.7 (1) and (2), with $n=6$, q even, and $G_2(q)\trianglelefteq H$. Then Γ is connected,*

G-symmetric and G-quotient-complete if and only if $\Gamma \cong \mathrm{Cay}(V, S)$*, where S is one of the following:*

(1) $S_{\mathcal{L}}$;

(2) $S_{\mathcal{L}'}$;

(3) $\bigcup_{\lambda' \in C(\lambda)} S_{\lambda'}$ *for any* $\lambda \in \mathbb{F}_q^{\#}$;

(4) $\bigcup_{\lambda' \in A(\lambda)} V_{\lambda'}^{\#}$ *for some* $\lambda \notin \mathrm{Fix}(\sigma(H))$.

Furthermore, such a graph Γ has exactly $k = |\mathrm{Fix}(\sigma(H))|+1$ *nontrivial complete G-normal quotients.*

Proof. This follows immediately from Proposition 4.2.5 and Lemmas 4.2.7 and 4.3.4. □

4.3.4. Exceptional cases. Assume that H is as given in Table 3.5.1, with $n = d$ and $q = p$. Since $H \leq \mathrm{GL}(n, q)$ for each case, the sets $V_\infty^{\#}$ and $V_\lambda^{\#}$ for all $\lambda \in \mathbb{F}_q$ are G_0-orbits. These orbits correspond to disconnected graphs by Lemma 3.2.3, while all other orbits, which are subsets of V_{ind}, give rise to connected graphs Γ. The orbits in V_{ind} were all obtained using Magma [**1**].

For the case $n = 2$ (i.e., H as in lines 1, 2 and 3 of Table 3.5.1 or lines 1-17 of Table 4.1.2), we prove in Lemma 4.3.8 that all connected graphs arising from each H have the same valency and belong to one isomorphism class.

Lemma 4.3.8. *Let* $G_0 = \{(h, h) \mid h \in H\}$ *where* $H \leq \mathrm{GL}(2, q)$ *is one of the groups in lines* 1, 2 *and* 3 *of Table* 3.5.1, $U = \mathbb{F}_q^2$, *and* $V = U \oplus U$. *Then the connected graphs* $\mathrm{Cay}(V, S)$ *correspond to G_0-orbits* $S \subseteq V_{ind}$, *and belong to one isomorphism class. Moreover, all of these graphs have valency* $|H|$.

To prove Lemma 4.3.8 we need the following. Recall that the space $V = U \oplus U$ can be viewed as a tensor product $U \otimes U$ via the linear transformation $f : V \to U \otimes U$, where $(u, \mathbf{0}_U) \mapsto e_1 \otimes u$ and $(\mathbf{0}_U, u) \mapsto e_2 \otimes u$ for all $u \in U$ (with $e_1 = (1, 0)$ and $e_2 = (0, 1)$, the standard basis vectors in U). Each $(x, y) \in V$ then corresponds to $e_1 \otimes x + e_2 \otimes y \in U \otimes U$. Likewise the group $G_0 = \mathrm{diag}(H \times H)$ can be viewed as the tensor product $\langle I_2 \rangle \otimes H$, where I_2 is the 2×2 identity matrix over $\mathbb{F}_q$ and each $(h, h) \in G_0$ corresponds to $I_2 \otimes h \in \langle I_2 \rangle \otimes H$. Observe that for each $(x, y) \in V$ and $h \in H$, the element $(x, y)^{(h,h)} = \left(x^h, y^h\right)$ in $U \otimes U$ corresponds to

$$e_1 \otimes x^h + e_2 \otimes y^h = (e_1 \otimes x + e_2 \otimes y)^{I_2 \otimes h}$$

in $U \otimes U$, so the original action of $\mathrm{diag}(H \times H)$ on $U \oplus U$ is equivalent to the natural action of $\langle I_2 \rangle \otimes H$ on $U \otimes U$. Furthermore, note that $\mathrm{GL}(2, q) \otimes \langle I_2 \rangle \leq N_{\mathrm{GL}(V)}(G_0)$.

Proof of Lemma 4.3.8. It was shown in the first paragraph of this section that the graph $\mathrm{Cay}(V, S)$ is connected if and only if $S \subseteq V_{ind}$. To prove that the connected graphs belong to one isomorphism class we show that $N_{\mathrm{GL}(V)}(G_0)$ is transitive on V_{ind}.

Let $(u,w),(x,y) \in V_{ind}$. Then $\{u,w\}$ and $\{x,y\}$ are ordered bases of U; let $A = (a_{ij})$ be the change-of-basis matrix from $\{u,w\}$ to $\{x,y\}$. (That is, $x = a_{11}u + a_{21}w$ and $y = a_{12}u + a_{22}w$.) Then in $U \otimes U$ we have

$$\begin{aligned}(e_1 \otimes u + e_2 \otimes w)^{A \otimes I_2} &= e_1^A \otimes u + e_2^A \otimes w \\ &= (a_{11}e_1 + a_{12}e_2) \otimes u + (a_{21}e_1 + a_{22}e_2) \otimes w \\ &= e_1 \otimes (a_{11}u + a_{21}w) + e_2 \otimes (a_{21}u + a_{22}w) \\ &= e_1 \otimes x + e_2 \otimes y\end{aligned}$$

Recall from the remarks preceding the proof that $A \otimes I_2 \in N_{\mathrm{GL}(V)}(G_0)$, so the group $N_{\mathrm{GL}(V)}(G_0)$ is transitive on V_{ind}. It follows that the graphs $\mathrm{Cay}(V,S)$ are all isomorphic for all G_0-orbits $S \subseteq V_{ind}$.

Now let $(u,w) \in V_{ind}$ and $(h,h) \in \mathrm{Stab}_{G_0}((u,w))$. Then $u^h = u$ and $w^h = w$. Since $\{u,w\}$ is a basis of U then h must be the identity in $\mathrm{GL}(U)$. Therefore (h,h) is the identity in $\mathrm{GL}(V)$, and hence G_0 acts semiregularly on V_{ind}. Thus $|S| = |G_0| = |H|$ for all G_0-orbits S in V_{ind}. □

The connected graphs arising from transitive groups $H \le N_{\Gamma\mathrm{L}(2,9)}(\mathrm{SL}(2,5))$ are presented in lines 18-33 of Table 4.1.2. We have $A(3) = N_{\mathrm{GL}(2,9)}(\mathrm{SL}(2,5)) \cong Z \circ \mathrm{SL}(2,5)$, where $Z = Z(\mathrm{GL}(2,9)) \cong \mathbb{Z}_8$, and $N_{\Gamma\mathrm{L}(2,9)}(\mathrm{SL}(2,5)) \cong A(3) \rtimes \mathrm{Aut}\,(\mathbb{F}_9)$. The graphs $\Gamma(31)$ correspond to $\mathrm{Cay}(V,S)$ with $S = V_\lambda^\# \cup V_{\lambda^3}^\#$ and $\lambda \in \mathbb{F}_9 \setminus \mathbb{F}_3$. The group $A(5)$ has two maximal subgroups which are transitive and not contained in $\mathrm{GL}(2,9)$, namely $A(4) = (Z_0 \circ \mathrm{SL}(2,5)) \rtimes \mathrm{Aut}\,(\mathbb{F}_9)$ and $A(1) = (Z \circ K) \rtimes \mathrm{Aut}\,(\mathbb{F}_9)$, where $\mathbb{Z}_4 \cong Z_0 \le Z$ and $K = A(1) \cap \mathrm{SL}(2,5) \cong \mathbb{Z}_{10} \rtimes \mathbb{Z}_2$. The group $A(2)$ is isomorphic to the subgroup $\mathrm{SL}(2,5) \rtimes \mathrm{Aut}\,(\mathbb{F}_9)$.

The group $B(1)$ in Table 4.1.2 is conjugate to $A(2)$, and thus gives the same graphs as $A(2)$; we do not list these graphs in the table. The group $B(3)$ has order 320 and is isomorphic to $B(4) \cap B(5)$. The groups $B(1)$, $B(4)$ and $B(5)$ are maximal in the group $N_{\mathrm{GL}(4,3)}(D_8 \circ Q_8)$.

For the rest of Table 4.1.2, isomorphisms (and non-isomorphisms) are determined using MAGMA [**1**]. Except where indicated, each line of the table represents a distinct isomorphism class of graphs. For each H the isomorphisms are induced by elements of $N_{\mathrm{GL}(V)}(G_0)$, except for those in line 33: in this case $N_{\mathrm{GL}(V)}(G_0)$ divides the four graphs of valency 960 into two classes of sizes 3 and 1; it is determined by MAGMA that these merge into one isomorphism class. For lines 53 – 72 the isomorphisms are induced by elements of $\langle g \otimes h \mid g \in \mathrm{GL}(2,3), h \in H \rangle \le N_{\mathrm{GL}(V)}(G_0)$.

The results in Section 4.3 complete the proof of Theorem 4.1.1.

PROOF OF THEOREM 4.1.1. This follows from Proposition 4.2.5, Lemma 4.2.7, and the results in this section (Propositions 4.3.1, 4.3.3 and 4.3.7 and the above). □

4.4. Quotient-complete symmetric graphs with diameter 2

In this section we identify which of the graphs in Section 4.3 have diameter 2. Those for the exceptional cases (namely, the graphs in Table 4.1.2) were found using Magma [**1**] and are indicated by a "†" in the first column of Table 4.1.2. From now on we consider the graphs in Table 4.1.1. Recall that $\mathrm{Cay}(V,S)$ has diameter 2 if and only if $S \neq V^{\#}$ and $V \subseteq S \cup (S+S)$ (equivalently, $V \setminus S \subseteq S+S$) where $S+S := \{x+y \mid x,y \in S\}$. Since the S that appear in Table 4.1.1 all satisfy $S \neq V^{\#}$ and $S=-S$, we only need to verify that $V^{\#} \setminus S \subseteq S+S$.

As in Section 4.3 we assume throughout that U, V, G, G_0 and H are as in Lemma 4.2.7 (1) and (2). Also let V_λ be as in (4.3.1) and S_λ be as in (4.3.5) for each $\lambda \in \mathbb{F}_q^{\#}$, V_{ind} be as in (4.3.2), $S_{\mathcal{L}}$ be as in (4.3.6) and $S_{\mathcal{L}'}$ be as in (4.3.7).

Lemma 4.4.1. *Let $S = V_\lambda^{\#} \cup V_\mu^{\#}$ where $\lambda \neq \mu$. Then $V^{\#} \setminus S \subseteq S+S$.*

Proof. Let $(u,w) \in V^{\#} \setminus S$. Since $\mu \neq \lambda$ the matrix $\begin{pmatrix} 1 & \lambda \\ 1 & \mu \end{pmatrix}$ is invertible, and thus there exist $x,y \in U$ (not both $\mathbf{0}_U$) which satisfy the equation

$$(u \quad w) = (x \quad y) \begin{pmatrix} 1 & \lambda \\ 1 & \mu \end{pmatrix}.$$

That is,

$$(u,w) = (x+y, \lambda x + \mu y) = (x, \lambda x) + (y, \mu y) \in S+S.$$

Therefore $V^{\#} \setminus S \subseteq S+S$. □

Clearly $|A(\lambda)| \geq 2$ if and only if $\lambda \notin \mathrm{Fix}(\sigma(H))$, so it follows from Lemma 4.4.1 that the graphs in lines 2, 5 and 9 of Table 4.1.1 have diameter 2.

Lemma 4.4.2. *Suppose that $n \geq 2$, and let $S = V_{ind}$. Then $V^{\#} \setminus S \subseteq S+S$.*

Proof. Let $(u,w) \in V^{\#} \setminus S = \bigcup_{\lambda \in \mathbb{F}_q \cup \{\infty\}} V_\lambda^{\#}$.

Case 1: Suppose that $(u,w) = (u, \mathbf{0}_U) \in V_0^{\#}$. Take $x \in U^{\#}$ such that $\{x,u\}$ is linearly independent in U. Then $\{u-x, -u\}$ is also linearly independent, and thus $(x,u), (u-x, -u) \in S$. Hence $(u,w) = (x,u) + (u-x,-u) \in S+S$. The case $(u,w) \in V_\infty^{\#}$ is proved similarly.

Case 2: Suppose that $(u,w) \in V_\lambda^{\#}$ for some $\lambda \in \mathbb{F}_q^{\#}$, so that $u \neq \mathbf{0}_U$ and $w = \lambda u$. Take $x \in U$ such that $\{u,x\}$ is linearly independent. Then $\{u-x, x\}$ and $\{x, \lambda u - x\}$ are also linearly independent, and $(u-x,x), (x, \lambda u - x) \in S$. Hence $(u,w) \in S+S$, which completes the proof. □

Lemma 4.4.3. *Suppose that* $\dim(U)$ *is even, and let $\lambda \in \mathbb{F}_q^{\#}$. Then $V^{\#} \setminus S_\lambda \subseteq S_\lambda + S_\lambda$.*

Proof. Let $(u,w) \in V^{\#} \setminus S_\lambda$.

Case 1: Suppose that $(u,w) = (u, \mathbf{0}_U) \in V_0^{\#}$. Since the symplectic form f on U is nondegenerate there exists $x \in U$ such that $f(x,u) = \lambda$. Then $f(u-x, -u) = f(x,u) = \lambda$, and $(u,w) = (u-x,-u) + (x,u) \in S_\lambda + S_\lambda$. The case where $(u,w) \in V_\infty^{\#}$ is similar.

Case 2: Suppose that $(u,w) = (u, \alpha u) \in V_\alpha^{\#}$ for some $\alpha \in \mathbb{F}_q^{\#}$. Again by the nondegeneracy of f we can find $x \in U$ such that $f(x,u) = 1$. Set $y = \alpha x + \lambda u$. Then $f(x,y) = f(x, \lambda u) = \lambda$ and

$$\begin{aligned} f(u-x, w-y) &= f(u-x, (\alpha-\lambda)u - \alpha x) \\ &= f(u, -\alpha x) + f(-x, (\alpha-\lambda)u) \\ &= \alpha - (\alpha - \lambda) \\ &= \lambda. \end{aligned}$$

So $(x,y), (u-x, w-y) \in S_\lambda$ and $(u,w) = (u-x, w-y) + (x,y) \in S_\lambda + S_\lambda$.

Case 3: Suppose that $(u,w) \in S_\mu$ for some $\mu \in \mathbb{F}_q^{\#}$, $\mu \neq \lambda$. Set $x := u - w$ and $y := \lambda\mu^{-1}u$. Then

$$f(x,y) = f(-w, \lambda\mu^{-1}u) = \lambda\mu^{-1}\mu = \lambda$$

and

$$f(u-x, w-y) = f(w, w - \lambda\mu^{-1}u) = \lambda.$$

So $(x,y), (u-x, w-y) \in S_\lambda$ and $(u,w) \in S_\lambda + S_\lambda$.

Case 4: Suppose that $n \geq 4$ and $(u,w) \in S_0$. (If $n = 2$ then S_0 is empty, so Cases 1 to 3 suffice to prove that $V^{\#} \setminus S_\lambda \subseteq S_\lambda + S_\lambda$.) Since $n \geq 4$ the vector space U can be written as the orthogonal direct sum of two or more hyperbolic planes $L_1, \ldots, L_r$ (so $2r = n$). We choose the L_i's such that $u \in L_1$. Since $f(u,w) = 0$ we can write $w = \gamma u + x_2 + \cdots + x_r$, where $\gamma \in \mathbb{F}_q$ and $x_i \in L_i$ for all i, with $x_i \neq \mathbf{0}_U$ for at least one i (since u and w are linearly independent). Without loss of generality suppose that $x_2 \neq \mathbf{0}_U$, and let $y_2 \in L_2$ such that $f(x_2, y_2) = \lambda$. Note that $f(u, y_2) = f(x_2, w) = 0$, so that $f(u - x_2, w - y_2) = f(x_2, y_2) = \lambda$. Hence $(x_2, y_2), (u - x_2, w - y_2) \in S_\lambda$ and $(u,w) \in S_\lambda + S_\lambda$. □

Lemma 4.4.4. *Suppose that $n \geq 4$ and is even. Then $V^{\#} \setminus S_0 \subseteq S_0 + S_0$.*

PROOF. Let $(u,w) \in V^{\#} \setminus S_0$.

Case 1: Suppose that $(u,w) \in V_0^{\#}$. We can decompose U into an orthogonal direct sum of $r \geq 2$ hyperbolic planes $L_1, \ldots, L_r$ with $u \in L_1$. Let $x \in L_2^{\#}$, so that $f(x,u) = 0$ and $\{x,u\}$ is linearly independent; that is, $(x,u) \in S_0$. Then also $(u-x, -u) \in S_0$ (indeed, $u - x$ and $-u$ are linearly independent, and $f(u-x,-u) = f(x,u) = 0$). Hence $(x,u), (u-x,-u) \in S_0$ and $(u,w) = (u, \mathbf{0}_U) = (u-x,-u) + (x,u) \in S_0 + S_0$. The case where $(u,w) \in V_\infty^{\#}$ is similar.

Case 2: Suppose that $(u,w) = (u, \lambda u) \in V_\lambda^{\#}$ for some $\lambda \in \mathbb{F}_q^{\#}$. As in Case 1 we can write U as the orthogonal direct sum of $r \geq 2$ hyperbolic planes $L_1, \ldots, L_r$, with $u \in L_1$. Take $y \in L_2^{\#}$ and set $x = y + u$. Then $f(x,y) = f(u,y) = f(x,u) = 0$ and

$f(u-x, w-y) = f(u-x, \lambda u - y) = 0$. Furthermore $\{x, y\}, \{u-x, w-y\}$ are linearly independent, so $(x, y), (u-x, w-y) \in S_0$. Therefore $(u, w) = (u-x, w-y)+(x, y) \in S_0+S_0$.

Case 3: Suppose that $(u, w) \in S_\lambda$ for some $\lambda \in \mathbb{F}_q^\#$. Since $n \geq 4$ there exists $y \in U^\#$ such that $f(u, y) = f(w, y) = 0$. Set $x = y + u$. Then $f(x, y) = 0$ and $f(u - x, w - y) = f(-y, w) = 0$, and moreover $\{x, y\}$ and $\{u-x, w-y\} = \{-y, w-y\}$ are linearly independent. So $(x, y), (u-x, w-y) \in S_0$, and $(u, w) \in S_0 + S_0$. □

Lemma 4.4.5. *Suppose that q is even and $n = 6$. Then $V^\# \setminus S_{\mathcal{L}} \subseteq S_{\mathcal{L}} + S_{\mathcal{L}}$.*

PROOF. Let $(u, w) \in V^\# \setminus S_{\mathcal{L}}$.

Case 1: Suppose that $(u, w) \in V_\lambda^\#$ for some $\lambda \in \mathbb{F}_q \cup \{\infty\}$. If $\lambda \in \mathbb{F}_q^\#$, let $\ell \in \mathcal{L}$ be such that $u \in \ell$ and take $x \in \ell \setminus \langle u \rangle$. Then clearly $u + x \notin \langle x \rangle$, so $\langle x, \lambda(u+x) \rangle = \langle x, u+x \rangle = \ell$ and $(x, \lambda(u+x)), (\lambda x, u+x) \in S_{\mathcal{L}}$. Hence $(u, w) = (u, \lambda u) = (x, \lambda(u+x)) + (u+x, \lambda x) \in S_{\mathcal{L}} + S_{\mathcal{L}}$. If $\lambda = 0$ define ℓ and x similarly as the above. Then $u + x \notin \langle u \rangle$ so that $\langle x, u \rangle = \langle u + x, u \rangle = \ell$, and again $(u, w) = (u, \mathbf{0}_U) = (x, u) + (u + x, u) \in S_{\mathcal{L}} + S_{\mathcal{L}}$. The case where $\lambda = \infty$ is proved similarly, with $\ell \in \mathcal{L}$ chosen such that $w \in \ell$.

Case 2: Suppose that $(u, w) \in S_{\mathcal{L}'}$. Then by Lemma 3.4.2 the points $\langle u \rangle$ and $\langle w \rangle$ of the generalised hexagon $\mathcal{H}(q)$ are at distance 2 from each other in the point graph of $\mathcal{H}(q)$. Let $\langle x \rangle$ be a point of $\mathcal{H}(q)$ which is collinear to both $\langle u \rangle$ and $\langle w \rangle$. Then clearly $\langle u + x, x \rangle = \langle u, x \rangle \in \mathcal{L}$ and $\langle w + x, x \rangle = \langle w, x \rangle \in \mathcal{L}$ (see Figure 1). Hence $(u, w) = (u + x, x) + (x, w + x) \in S_{\mathcal{L}} + S_{\mathcal{L}}$.

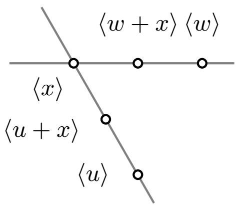

FIGURE 1. Diagram for Lemma 4.4.5, Case 2

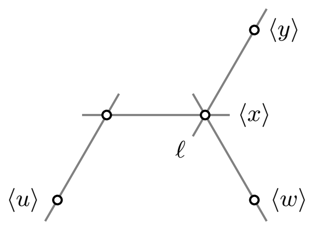

FIGURE 2. Diagram for Lemma 4.4.5, Case 3

Case 3: Suppose that $(u, w) \in S_\lambda$ for some $\lambda \in \mathbb{F}_q^\#$. By Lemma 3.4.2 the points $\langle u \rangle$ and $\langle w \rangle$ are at distance 3 from each other in the point graph of $\mathcal{H}(q)$. Let $\langle x \rangle$ be a point of $\mathcal{H}(q)$ which is collinear with $\langle w \rangle$ and is at distance 2 from $\langle u \rangle$ (see Figure 2). By the axioms of $\mathcal{H}(q)$, and in particular the fact that at least 3 lines of $\mathcal{H}(q)$ pass through $\langle x \rangle$, there exists $\ell \in \mathcal{L}$ through $\langle x \rangle$ such that all points in $\ell \setminus \langle x \rangle$ belong in $\Delta_3(\langle u \rangle) \cap \Delta_2(\langle w \rangle)$ (i.e., at distance 3 from $\langle u \rangle$ and distance 2 from $\langle w \rangle$). Let $y \in \ell \setminus \langle x \rangle$ be such that $y \neq \mathbf{0}_U$ and $f(u, y) = f(u, w)$. Then $\langle w, x, y \rangle$ is a maximal totally isotropic subspace, and it follows from Theorem 3.4.3 that it is the union of all lines in $\mathcal{L}$ that pass through $\langle x \rangle$. Now $y + w \in \langle w, x, y \rangle$, so $\langle y + w \rangle$ is collinear with $\langle x \rangle$ in $\mathcal{H}(q)$. Since $f(u, y + w) = f(u, y) + f(u, w) = 0$, Lemma 3.4.2 implies that either $\langle y + w \rangle \in \Delta_1(\langle u \rangle)$ or $\langle y + w \rangle \in \Delta_2(\langle u \rangle)$. We consider each of these cases in turn.

Case 3.1: Suppose that $\langle y+w\rangle \in \Delta_1(\langle u\rangle)$ (see Figure 3). Since it is also collinear with $\langle x\rangle$, the 3-dimensional subspace $\langle u, x, y+w\rangle$ is totally isotropic. It follows from Theorem 3.4.3 that $\langle u, x, y+w\rangle$ consists of all lines through $\langle y+w\rangle$. In particular, $\langle x+u\rangle$ is collinear with $\langle y+w\rangle$, and so $(u, w) = (x+u, y+w) + (x, y) \in S_{\mathcal{L}} + S_{\mathcal{L}}$, as required.

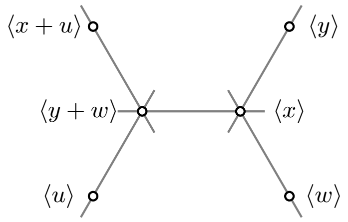

FIGURE 3. Diagram for Lemma 4.4.5, Case 3.1

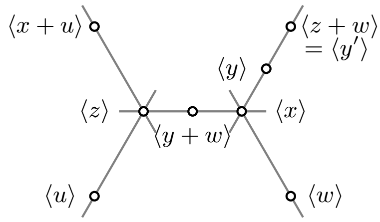

FIGURE 4. Diagram for Lemma 4.4.5, Case 3.2

Case 3.2: Suppose that $\langle y+w\rangle \in \Delta_2(\langle u\rangle)$. Let $\langle z\rangle$ be the point collinear with both $\langle u\rangle$ and $\langle x\rangle$ (see Figure 4). By Theorem 3.4.3 (1), the point $\langle x+u\rangle$ is collinear with $\langle z\rangle$. Claim that $z \in \langle x, y+w\rangle$. Suppose otherwise, and let $\langle z'\rangle$ be the point collinear with $\langle u\rangle$ and $\langle y+w\rangle$. Then $\langle z\rangle \neq \langle z'\rangle$, so that $\langle u\rangle$, $\langle z\rangle$, $\langle x\rangle$, $\langle y+w\rangle$, and $\langle z'\rangle$ form a 5-cycle in $\mathcal{H}(q)$. But this is impossible by the axioms of $\mathcal{H}(q)$. Therefore $\langle z\rangle = \langle z'\rangle$, and hence $z \in \langle x, y+w\rangle$, which proves the claim. Take $y' = z+w$, which is collinear with $\langle x\rangle$ by Theorem 3.4.3 (1). Then $\langle x, y'\rangle, \langle x+u, y'+w\rangle \in \mathcal{L}$, and therefore $(u, w) = (x+u, y'+w) + (x, y') \in S_{\mathcal{L}} + S_{\mathcal{L}}$. $\square$

Lemma 4.4.6. *Suppose that q is even and* $\dim(U) = 6$. *Then* $V^{\#} \setminus S_{\mathcal{L}'} \subseteq S_{\mathcal{L}'} + S_{\mathcal{L}'}$.

PROOF. Let $(u, w) \in V^{\#} \setminus S_{\mathcal{L}'}$.

Case 1: Suppose that $(u, w) \in V^{\#}_{\lambda}$ for some $\lambda \in \mathbb{F}_q \cup \{\infty\}$. An argument similar to that in Case 1 of the proof of Lemma 4.4.5, but taking $\ell \in \mathcal{L}'$, shows that $(u, w) \in S_{\mathcal{L}'} + S_{\mathcal{L}'}$.

Case 2: Suppose that $(u, w) \in S_{\mathcal{L}}$. Take $\ell \in \mathcal{L}$ such that ℓ contains $\langle u+w\rangle$ and $\ell \neq \langle u, w\rangle$ (see Figure 5). Let $\langle x\rangle$ be a point in ℓ distinct from $\langle u+w\rangle$. Then $\langle u, x\rangle, \langle w, x\rangle \in \mathcal{L}'$ by Lemma 3.4.2, and likewise $\langle u+x, x\rangle, \langle w+x, x\rangle \in \mathcal{L}'$. Thus $(u, w) = (u+x, x) + (x, w+x) \in S_{\mathcal{L}'} + S_{\mathcal{L}'}$.

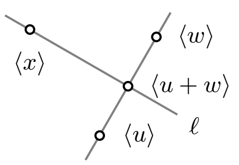

FIGURE 5. Diagram for Lemma 4.4.6, Case 2

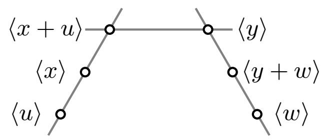

FIGURE 6. Diagram for Lemma 4.4.6, Case 3

Case 3: Suppose that $(u, w) \in S_\lambda$ for some $\lambda \in \mathbb{F}_q^{\#}$. Then $\langle u\rangle$ and $\langle w\rangle$ have distance 3 in $\mathcal{H}(q)$ by Lemma 3.4.2. Take points $\langle x\rangle$ and $\langle y\rangle$ such that $\langle x\rangle \neq \langle u\rangle$ and $\langle x\rangle \in \Delta_1(\langle u\rangle) \cap \Delta_3(\langle w\rangle)$, and $\langle y\rangle \in \Delta_1(\langle w\rangle) \cap \Delta_2(\langle u\rangle) \cap \Delta_2(\langle x\rangle)$ (see Figure 6). Then $\langle x\rangle \in \Delta_2(\langle y\rangle)$. Choose x such that $f(x, w) = f(u, w)$. Then $f(x+u, w) = 0$, so by Lemma 3.4.2 either

$\langle x+u\rangle \in \Delta_1(\langle w\rangle)$ or $\langle x+u\rangle \in \Delta_2(\langle w\rangle)$. Since $\langle x+u\rangle$ lies on the line $\langle x,u\rangle$, it follows that $\langle x+u\rangle \in \Delta_2(\langle w\rangle)$. Finally, since $y+w \in \langle y,w\rangle$, we have $\langle y+w\rangle \in \Delta_2(\langle x+u\rangle)$. So $\langle x,y\rangle, \langle x+u, y+w\rangle \in \mathcal{L}'$ by Lemma 3.4.2, and $(u,w) = (x+u,y+w)+(x,y) \in S_{\mathcal{L}'}+S_{\mathcal{L}'}$. □

The diameter 2 graphs in Table 4.1.1 are indicated by a "†" in the first column, and this follows from Lemmas 4.4.1 to 4.4.6.

4.5. Quotient-complete symmetric graphs arising from $H \leq \Gamma\mathrm{L}(1,q)$

Let U, V, G, G_0 and H be as in Lemma 4.2.7 (1) and (2), with $q = p^d$ (p prime), $n = 1$, and $H \leq \Gamma\mathrm{L}(1,q)$. Let ω be a fixed primitive element of $\mathbb{F}_q$ and let $\widehat{\omega}$ denote scalar multiplication by ω. Also, let τ be the Frobenius automorphism of $\mathbb{F}_q$, that is, $\tau : \lambda \mapsto \lambda^p$ for all $\lambda \in \mathbb{F}_q$. Then $\mathrm{GL}(1,q) = \langle\widehat{\omega}\rangle$ and $\Gamma\mathrm{L}(1,q) = \langle\widehat{\omega}, \tau\rangle$.

The following result, originally by D.A. Foulser, gives a standard generating set for H, as well as necessary and sufficient conditions (with respect to this generating set) for H to be transitive on $U^{\#}$.

Lemma 4.5.1. [**33**, Lemmas 4.4 and 4.7] *Let $H \leq \Gamma\mathrm{L}(1,q) = \langle\widehat{\omega}, \tau\rangle$, where $q = p^d$ (p prime), $\widehat{\omega}$ is scalar multiplication by a fixed primitive element $\omega \in \mathbb{F}_q$, and τ is the Frobenius automorphism of $\mathbb{F}_q$. Then there exist unique integers a, b and c such that $H = \left\langle \widehat{\omega}^a, \widehat{\omega}^b\tau^c \right\rangle$ and the following hold: $a > 0$ and a divides $q-1$; $c > 0$ and c divides d; $0 \leq b < a$ and $b(q-1)/(p^c-1) \equiv 0 \pmod d$. Moreover, H is transitive on $U^{\#} = \mathbb{F}_q^{\#}$ if and only if one of the following holds:*

1. *(1) $a = 1$ (so $b = 0$), or*
2. *(2) $b > 0$, a divides $b(p^{ac}-1)/(p^c-1)$, and a does not divide $b(p^{a'c}-1)/(p^c-1)$ whenever $1 < a' < a$.*

We do not treat this case completely; rather, we consider the subcases for which either $H \cap \mathrm{GL}(1,q) = \mathrm{GL}(1,q)$, or $H = \langle\widehat{\omega}^a, \widehat{\omega}\tau^c\rangle$ where $p^c \equiv 1 \pmod a$.

4.5.1. $H = \langle\widehat{\omega}, \tau^c\rangle$ where $d \equiv 0 \pmod c$. Let τ and $\widehat{\omega}$ be as in Lemma 4.5.1, and suppose that H is of the type described in Lemma 4.5.1 (1). Then $H = \langle\widehat{\omega}, \tau^c\rangle$ for some divisor c of d. The G_0-orbits in $V^{\#}$ are the sets $V_\infty^{\#}$ and $\bigcup_{\lambda' \in D(\lambda)} V_{\lambda'}^{\#}$ for all $\lambda \in \mathbb{F}_q$, where

$$D(\lambda) := \{\lambda^\sigma \mid \sigma \in \langle\tau^c\rangle\} = \{\lambda^{p^{ci}} \mid 0 \leq i < d/c - 1\}. \tag{4.5.1}$$

Then $|D(\lambda)| = 1$ if and only if $\lambda \in \mathrm{Fix}(\langle\tau^c\rangle)$, where $|\mathrm{Fix}(\langle\tau^c\rangle)| = p^c$, and there exist connected graphs if and only if $d \geq 2$.

Proposition 4.5.2. *Let Γ be graph and $G = T_V \rtimes G_0$, where V, T_V and G_0 are as in Lemma 4.2.7 (1) and (2), with $n = 1$, $q = p^d$ (p prime), and $d \geq 2$. Also, suppose that $H = \langle\widehat{\omega}, \tau^c\rangle$, where $\widehat{\omega}$ and τ are as in Lemma 4.5.1 and c divides d. Then Γ is connected, G-symmetric and G-quotient-complete if and only if $\Gamma \cong \mathrm{Cay}(V,S)$ where $S = \bigcup_{\lambda' \in D(\lambda)} V_{\lambda'}^{\#}$*

for some $\lambda \notin \mathrm{Fix}(\langle\tau^c\rangle)$. Furthermore, such a graph Γ has diameter 2 and has exactly p^c+1 nontrivial complete G-normal quotients.

Proof. This follows immediately from Proposition 4.2.5, Lemma 4.2.7, Lemma 4.4.1, and the preceding remarks. $\square$

4.5.2. $H = \langle\widehat{\omega}^a, \widehat{\omega}\tau^c\rangle$**, where** $d \equiv 0 \pmod c$, $q \equiv p^c \equiv 1 \pmod a$**, and** $(q-1)/(p^c-1) \equiv 0 \pmod d$**.** Again we let $\widehat{\omega}$ and τ be as in Lemma 4.5.1. Suppose that $H = \langle\widehat{\omega}^a, \widehat{\omega}\tau^c\rangle$ for some divisor a of $q-1$ and divisor c of d, such that $p^c \equiv 1 \pmod a$ and $(q-1)/(p^c-1) \equiv 0 \pmod d$. Then H is a transitive subgroup of $\Gamma\mathrm{L}(1,q)$ of the type described in Lemma 4.5.1 (2). (Indeed, observe that $(p^{ac}-1)/(p^c-1) = p^{c(a-1)} + p^{c(a-2)} + \ldots + 1 \equiv 0 \pmod a$ and $(p^{a'c}-1)/(p^c-1) \equiv a' \pmod a \not\equiv 0 \pmod a$ for all $1 < a' < a$.) The G_0-orbits in $V^\#$ are $V^\#_\infty$ and $(1,\lambda)^{G_0}$ for each $\lambda \in U$.

Let $r := p^c$. For any positive integer j,

$$(\widehat{\omega}\tau^c)^j : \lambda \mapsto \lambda^{r^j}\omega^{r(r^j-1)/(r-1)} \text{ for all } \lambda \in U,$$

where U is identified with $\mathbb{F}_q$. Now for any $(1,\lambda) \in V$,

$$(1,\lambda)^{G_0} = \left\{ \left(\omega^{ai}, \lambda\omega^{ai}\right)^{(\widehat{\omega}\tau^c)^j} \;\middle|\; \text{all } i \text{ and all } j \right\},$$

where for each i and j we have $\left(\omega^{ai}, \lambda\omega^{ai}\right)^{(\widehat{\omega}\tau^c)^j} = \left(\omega^\ell, \lambda^{r^j}\omega^\ell\right)$ and $\ell = ai + r(r^j-1)/(r-1) \equiv j \pmod a$. Hence

$$(1,\lambda)^{G_0} = \Big\{ \left(\omega^{ai}, \lambda\omega^{ai}\right), \left(\omega^{ai+1}, \lambda^r\omega^{ai+1}\right), \ldots, \left(\omega^{ai+m}, \lambda^{r^j}\omega^{ai+m}\right), \ldots \;\Big|\; \text{all } i \text{ and all } j;\ 0 \le m < a \text{ and } m \equiv j \pmod a \Big\}.$$

Clearly $(1,\lambda)^{G_0} = V^\#_\lambda$ if and only if $\lambda \in \mathrm{Fix}(\langle\tau^c\rangle)$.

Proposition 4.5.3. *Let Γ be graph and $G = T_V \rtimes G_0$, where V, T_V and G_0 are as in Lemma 4.2.7 (1) and (2), with $n = 1$, $q = p^d$ (p prime), and $d \ge 2$. Also, suppose that $H = \langle\widehat{\omega}^a, \widehat{\omega}\tau^c\rangle$, where $\widehat{\omega}$ and τ are as in Lemma 4.5.1, a divides $q-1$, c divides d, $p^c \equiv 1 \pmod a$, and $(q-1)/(p^c-1) \equiv 0 \pmod d$. Then Γ is connected, G-symmetric and G-quotient-complete if and only if $\Gamma \cong \mathrm{Cay}(V,S)$ where $S = (1,\lambda)^{G_0}$ for some $\lambda \notin \mathrm{Fix}(\langle\tau^c\rangle)$. Furthermore, such a graph Γ has exactly p^c+1 nontrivial complete G-normal quotients.*

Proof. This follows immediately from Proposition 4.2.5, Lemma 4.2.7, and the preceding remarks. $\square$

In general,

$$\left|(1,\lambda)^{G_0}\right| = \mathrm{lcm}\,(a, |D(\lambda)|)(q-1)/a$$

with $D(\lambda)$ as in (4.5.1), since $\lambda^{r^j}\omega^{ai+m} = \lambda\omega^{ai}$ if and only if j is divisible by both a and $|D(\lambda)|$. Moreover, $(1,\lambda)^{G_0} \subseteq \bigcup_{\lambda' \in D(\lambda)} V^\#_{\lambda'}$ where $\left|\bigcup_{\lambda' \in D(\lambda)} V^\#_{\lambda'}\right| = |D(\lambda)|(q-1)$, and by comparing cardinalities we get that $(1,\lambda)^{G_0} = \bigcup_{\lambda' \in D(\lambda)} V^\#_{\lambda'}$ if and only if $|D(\lambda)|$ is coprime to a. In this case the resulting graphs $\mathrm{Cay}(V, (1,\lambda)^{G_0})$ have diameter 2 and are the same as the graphs in Proposition 4.5.2. There may be other diameter 2 graphs distinct from the type described in Proposition 4.5.2, arising from the other G_0-orbits, as can be seen in the following example.

Example 4.5.4. Suppose that $q = 3^4$ and let $H = \langle \widehat{\omega}^2, \widehat{\omega}\tau \rangle$. Then the G_0-orbits in $V^{\#}$ are the sets $V^{\#}_{\infty}$ and $(1,\lambda)^{G_0}$ for each $\lambda \in U$, where

$$(1,\lambda)^{G_0} = \left\{ \left(\omega^{2i}, \lambda\omega^{2i}\right), \left(\omega^{2i+1}, \lambda^3\omega^{2i+1}\right), \left(\omega^{2i}, \lambda^9\omega^{2i}\right), \left(\omega^{2i+1}, \lambda^{27}\omega^{2i+1}\right) \mid \text{all } i \right\}.$$

Observe that $(1,\lambda)^{G_0} = (1,\mu)^{G_0}$ if and only if $\mu = \lambda^9$, so there are 46 G_0-orbits in all. Also, since $d = 4$ and $c = 1$, $|D(\lambda)| \in \{1,2,4\}$ for all $\lambda \in \mathbb{F}_q$ (since by its definition $|D(\lambda)|$ must divide d/c). So by the preceding remarks $(1,\lambda)^{G_0} = \bigcup_{\lambda' \in D(\lambda)} V^{\#}_{\lambda'}$ if and only if $\lambda \in \mathrm{Fix}(\langle\tau\rangle)$, which yield disconnected graphs by Lemma 3.2.3. Hence there are no connected graphs of the form described in Proposition 4.5.2. Moreover, there are 10 orbits which have length 80 — namely, $V^{\#}_{\infty}$ and $(1,\lambda)^{G_0}$ where $\lambda \in \{0, 1, \omega^{10}, \omega^{20}, \dots, \omega^{70}\}$ — and 36 of length 160. Of the graphs which arise, 24 have diameter 2, and all of these have valency 160. It was verified using MAGMA that the diameter 2 graphs belong to one isomorphism class. □

CHAPTER 5

Symmetric vertex-quasiprimitive graphs: affine case

5.1. Overview and main results

We now turn our attention to symmetric graphs that satisfy Case (2) of Theorem 1 with $N = 1$; that is, we look at symmetric graphs that admit a vertex-quasiprimitive subgroup of automorphisms. Recall from Theorem 1.3.8 that there are eight types of quasiprimitive permutation groups; in this chapter we consider graphs with quasiprimitive automorphism group of type HA. Graphs that correspond to the other quasiprimitive types are discussed in Chapter 6.

Lemma 5.1.1 describes the structure of symmetric graphs Γ, together with $G \leq \mathrm{Aut}(\Gamma)$, such that G acts as an affine-type quasiprimitive permutation group on $V(\Gamma)$. This result follows from basic properties of affine quasiprimitive permutation groups and Cayley graphs (see Sections 1.3.4 and 2.2).

Lemma 5.1.1. [**39**] *Let Γ be a graph and let $G \leq \mathrm{Aut}(\Gamma)$, where G acts quasiprimitively on $V(\Gamma)$ and is of affine type. Then $G \cong V \rtimes G_0 \leq \mathrm{AGL}(d,p)$ and $\Gamma \cong \mathrm{Cay}(V,S)$ for some vector space $V = \mathbb{F}_p^d$ over a prime field $\mathbb{F}_p$, where V is identified with its translation group and $G_0 \leq \mathrm{GL}(d,p)$ is irreducible. Moreover, Γ is G-symmetric with diameter 2 if and only if S is a G_0-orbit of nonzero vectors satisfying $-S = S$ and $S \cup (S+S) = V$.*

Remark. Recall from the remarks after Lemma 2.2.5 that if $\mathrm{diam}(\mathrm{Cay}(V,S)) = 2$ then $|V| \leq |S|^2 + 1$, where $|S| \leq |G_0|$. Hence if $|V| > |G_0|^2 + 1$, then for any G_0-orbit S in V the graph $\mathrm{Cay}(V,S)$ has diameter greater than 2.

We are interested in the case where the irreducible subgroup G_0 is maximal in $\mathrm{GL}(d,p)$ with respect to being intransitive on $V^{\#}$. By Aschbacher's classification of the subgroups of the finite classical groups (see Section 3.6), the irreducible subgroups of $\mathrm{GL}(d,p)$ which do not contain $\mathrm{SL}(d,p)$ are organised into eight classes $\mathcal{C}_i$, $2 \leq i \leq 9$. The maximal subgroups in these classes are all intransitive on $V^{\#}$, except for those in the class $\mathcal{C}_3$ — which are of the form $\Gamma\mathrm{L}(n,q)$, where $q^n = p^d$ and d/n is prime — as well as the $\mathcal{C}_8$-subgroup $\mathrm{GSp}(d,p)$. The irreducible maximal subgroups of $\Gamma\mathrm{L}(n,q)$ and $\mathrm{GSp}(d,p)$ which do not contain $\mathrm{SL}(n,q)$ and $\mathrm{Sp}(d,p)$, respectively, are again organised into classes $\mathcal{C}_2$ to $\mathcal{C}_9$. In $\Gamma\mathrm{L}(n,q)$, the maximal $\mathcal{C}_i$-subgroups which are transitive on $V^{\#}$ are those in the class $\mathcal{C}_3$, which have the form $\Gamma\mathrm{L}(m,q^{n/m})$ with n/m prime, and the $\mathcal{C}_8$-subgroup $\Gamma\mathrm{Sp}(n,q)$.

In $\mathrm{GSp}(d,p)$, all maximal $\mathcal{C}_i$-subgroups for $i \neq 3$ are intransitive on $V^\#$; a maximal $\mathcal{C}_3$-subgroup either contains $\mathrm{Sp}(n,q)$, in which case it is contained in $\Gamma\mathrm{Sp}(n,q)$, or has the form $\mathrm{GU}(d/2,p^2)$, in which case it is contained in $\Gamma\mathrm{U}(d/2,p^2)$, which in turn is intransitive on $V^\#$ and is a maximal $\mathcal{C}_8$-subgroup of $\Gamma\mathrm{L}(d/2,p^2)$. Thus the maximal $\mathcal{C}_3$-subgroups of $\mathrm{GSp}(d,p)$ can be dealt with by considering maximal intransitive subgroups of $\Gamma\mathrm{L}(n,q)$ and $\Gamma\mathrm{Sp}(n,q)$ of type $\mathcal{C}_i$, $i \neq 3$, for all n and q.

In view of the above, we assume for the rest of this chapter that the following hypothesis holds:

Hypothesis 5.1.2. Let $V = \mathbb{F}_p^d$ with p prime and $d \geq 2$, and let $q = p^{d/n}$ for some divisor n of d (possibly n composite or $n = d$). The space V is viewed as $\mathbb{F}_q^n$, τ denotes the Frobenius automorphism of $\mathbb{F}_q$, $\mathcal{B}$ is a fixed $\mathbb{F}_q$-basis of V, and τ acts on V as in (3.2.2) with respect to $\mathcal{B}$. Define $G := V \rtimes G_0 \leq \mathrm{AGL}(d,p)$ and $L := G_0 \cap \mathrm{GL}(n,q)$, where G_0 is a maximal $\mathcal{C}_i$-subgroup of H for $2 \leq i \leq 9$, $i \neq 3$, and one of the following holds:

(1) $H = \Gamma\mathrm{L}(n,q) = \mathrm{GL}(n,q) \rtimes \langle\tau\rangle$ and $G_0 \not\geq \mathrm{Sp}(n,q)$, or
(2) $H = \Gamma\mathrm{Sp}(n,q) = \mathrm{GSp}(n,q) \rtimes \langle\tau\rangle$, the group of semisimilarities of a symplectic form on V.

All irreducible subgroups of $\mathrm{GL}(d,p)$ which are maximal with respect to being intransitive on $V^\#$ thus occur as subcases of the groups considered in Hypothesis 5.1.2. (Indeed, G_0 is maximal intransitive if $n = d$ or if d/n is prime.) Our goal is to identify the diameter 2 Cayley graphs $\mathrm{Cay}(V,S)$, if any, that arise from the G_0-orbits S in $V^\#$. We thus have two main concerns: first, to determine the G_0-orbits S in $V^\#$, and second, to identify which of these orbits satisfy $S = -S$ and $S \cup (S+S) = V$. In the cases where we are not able to do one or the other of these, we obtain bounds on certain parameters to reduce the number of unresolved cases.

For the rest of this chapter we prove Theorem 4, which is done by considering separately each of the Aschbacher classes $\mathcal{C}_2$, $\mathcal{C}_4$, $\mathcal{C}_5$, $\mathcal{C}_6$, $\mathcal{C}_7$ and $\mathcal{C}_8$.

5.2. Class $\mathcal{C}_8$

In this case the space V has a form ϕ, which is symplectic, unitary, or nondegenerate quadratic if $H = \Gamma\mathrm{L}(n,q)$, and is nondegenerate quadratic if $H = \Gamma\mathrm{Sp}(n,q)$ with q even. The group G_0 is the semisimilarity group $\Gamma\mathrm{I}(n,q)$ of (V,ϕ) where I is as in Table 3.3.1. Since the symplectic group is transitive on $V^\#$, we only consider the unitary and orthogonal cases here.

Recall from Theorem 3.3.3 that the orbits of the isometry group of V are the sets S_λ defined in (3.3.1), where $\lambda \in \mathrm{Im}\,\overline{\phi}$ with $\overline{\phi}$ as defined in (3.3.2). Since $-I_n \in \mathrm{I}(n,q)$ for all I in Table 3.3.1, it follows that $-S_\lambda = S_\lambda$ for all possible λ. So to prove that $\mathrm{Cay}(V,S)$, for some G_0-orbit S, has diameter 2, we only need to show that $V \setminus S \subseteq S + S$. In most cases this is done by showing that for any $v \in V \setminus S$ there exists a $w \in S$ such that $v - w \in S$.

As in Section 3.3, let $\mathbb{F}_q^{\square} := \left\{\alpha^2 \mid \alpha \in \mathbb{F}_q^{\#}\right\}$ and $\mathbb{F}_q^{\boxtimes} := \mathbb{F}_q^{\#} \setminus \mathbb{F}_q^{\square}$. (So $\mathbb{F}_q^{\boxtimes} \neq \varnothing$ only if q is odd.) For $\theta \in \{\square, \boxtimes, \#\}$ let

$$S_\theta := \bigcup_{\lambda \in \mathbb{F}_q^\theta} S_\lambda. \tag{5.2.1}$$

If q is a square (as in the unitary case), let $q_0 := \sqrt{q}$ and let $\mathbb{F}_{q_0}$ denote the subfield of $\mathbb{F}_q$ of index 2. Also let $Tr : \mathbb{F}_q \to \mathbb{F}_{q_0}$ denote the trace map, that is, $Tr(\alpha) = \alpha + \alpha^{q_0}$ for all $\alpha \in \mathbb{F}_q$.

Remark. As was pointed out in Section 3.3, we use the notation $\mathrm{U}(n, q)$ to denote the unitary group on $\mathbb{F}_q^n$, instead of the standard $\mathrm{U}(n, q_0)$. Also $\mathrm{GI}(n, q)$ denotes the similarity group of $(\mathbb{F}_q^n, \phi)$.

Proposition 5.2.1. *Let $V = \mathbb{F}_q^n$, ϕ be a unitary or nondegenerate quadratic form on V, and $G_0 = \mathrm{GI}(n, q)$ with* I *as in Table* 3.3.1*. Let S_0 be as in* (3.3.1) *and $S_\square$, $S_\boxtimes$ and $S_\#$ be as in* (5.2.1)*.*

(1) If ϕ is unitary, then the G_0-orbits in $V^\#$ are S_0 and $S_\#$.

(2) If ϕ is nondegenerate quadratic, then the G_0-orbits in $V^\#$ are as follows:

- *(i) $S_\#$ if $n = 1$;*
- *(ii) S_0 and $S_\#$ if n is even;*
- *(iii) S_0, $S_\square$ and $S_\boxtimes$ if n is odd and $n \geq 3$.*

Proof. It follows from Theorem 3.3.3 that S_0 is a G_0-orbit for all cases (that is, provided that $S_0 \neq \varnothing$), so we only need to determine the G_0-orbits in $S_\#$.

Suppose first that $\phi = f$ is unitary. Let $v \in S_\#$; clearly, $v^{G_0} \subseteq S_\#$. For any $u \in S_\#$ set $\alpha := f(u, u)f(v, v)^{-1}$. Then $\alpha \in \mathbb{F}_{q_0}$, so $\alpha = \beta^{q_0+1}$ for some $\beta \in \mathbb{F}_q$. Hence $f(u, u) = \beta^{q_0+1} f(v, v) = f(\beta v, \beta v)$, so by Theorem 3.3.3 we have $u = (\beta v)^g$ for some $g \in \mathrm{U}(n, q)$. Then $u = v^{\beta g}$, where $\beta g \in \mathrm{GU}(n, q)$. Therefore $v^{G_0} = S_\#$, as required.

Suppose now that $\phi = Q$ is a nondegenerate quadratic form. Observe that $\langle v\rangle^\# \subseteq v^{G_0}$ for any $v \in V$ since G_0 contains all nonzero scalar matrices. Therefore $V^\# = v^{G_0}$ if $n = 1$, which proves (i).

From now on assume that $n \geq 2$. It follows from Theorem 3.3.3 that the set S_0 is a G_0-orbit. Let $v \in S_\square$. Then for any $w \in S_\square$ we have $Q(w) = Q(\alpha v)$ for some $\alpha \in \mathbb{F}_q^\#$, so $w \in (\alpha v)^{\mathrm{I}(n,q)}$ by Theorem 3.3.3, and it follows that $w \in v^{G_0}$. So $S_\square \subseteq v^{G_0}$, and by a similar argument $S_\boxtimes$ is also contained in one G_0-orbit. If q is even then $\mathbb{F}_q^\boxtimes = \varnothing$, so $S_\square = S_\#$ is a G_0-orbit, which proves one case of (ii) (recall that if Q is nondegenerate and q is even, then n is even). Suppose that q is odd. Then either $S_\square \cup S_\boxtimes = S_\#$ is a G_0-orbit, or $S_\square$ and $S_\boxtimes$ are distinct G_0-orbits. Let $u \in S_\square$ and $w \in S_\boxtimes$. Then $U := \langle u\rangle$ and $W := \langle w\rangle$ are non-isometric spaces, and thus $D(Q|_U) \neq D(Q|_W)$. It follows from Theorem 3.3.6 (1) that also $D(Q|_{U^\perp}) \neq D(Q|_{W^\perp})$, so $U^\perp$ and $W^\perp$ are non-isometric. We have two cases.

Case 1: Suppose that n is even. Then $U^\perp$ and $W^\perp$ have odd dimension and are thus similar. Let $h : U^\perp \to W^\perp$ be a similarity, and let $\lambda \in \mathbb{F}_q^\#$ satisfy $Q(u_0^h) = \lambda Q(u_0)$ for all $u_0 \in U^\perp$. From Theorem 3.3.6 (2) applied to $U^\perp$, we deduce that $\lambda^{d-1} \in \mathbb{F}_q^\boxtimes$, and hence $\lambda \in \mathbb{F}_q^\boxtimes$. So there exists $w_0 \in W$ such that $Q(w_0) = \lambda Q(u)$, and the linear map $g : U \to W$, where $u \mapsto w_0$, is a similarity with $Q(x^g) = \lambda Q(x)$ for all $x \in U$. Writing $V = U \perp U^\perp$, let $\rho \in \mathrm{GL}(V)$ be defined by $x + y \mapsto x^g + y^h$ for all $x \in U$ and $y \in U^\perp$. Then $\rho \in M$ with $u^\rho \in W$, which shows that $S_\square \cup S_\boxtimes$ is a G_0-orbit. This completes the proof of (ii).

Case 2: Suppose that n is odd. Then $\dim\left(U^\perp\right) = \dim\left(W^\perp\right)$ is even, and there is no similarity of V which sends $U^\perp$ to $W^\perp$. It follows that there is no $g \in M$ with $u^g = w$. Therefore $S_\square$ and $S_\boxtimes$ are distinct G_0-orbits, which proves (iii). □

Recall that if Q is a nondegenerate quadratic form of minus type and $n = 2$, then V is anisotropic. In this case $S_0 = \varnothing$, so by Proposition 5.2.1 (2.ii), G_0 is transitive on $V^\#$.

Lemma 5.2.2. *Let $V = \mathbb{F}_q^n$ and ϕ be a unitary or nondegenerate quadratic form on V. Let S_0 and $S_\#$ be as in* (3.3.1) *and* (5.2.1)*, respectively. Then $S_\# \subseteq S_0 + S_0$ if ϕ is unitary and $n \geq 2$, or if ϕ is nondegenerate quadratic and $n \geq 3$.*

Proof. Let $v \in S_\#$. Then by Corollary 3.3.5 there exists $u \in \langle v\rangle^\perp$ with $\overline{\phi}(u) = -\overline{\phi}(v)$. If ϕ is unitary set $w := \beta(u+v)$, where $\beta := \alpha\overline{\phi}(v)^{-1}$ and $\alpha \in \mathbb{F}_q$ such that $Tr(\alpha) = \overline{\phi}(v)$. If ϕ is quadratic and q is odd set $w := \frac{1}{2}(u+v)$. Then in both cases we have $w, v-w \in S_0$, so $v \in S_0 + S_0$ and therefore $S_\# \subseteq S_0 + S_0$. If ϕ is quadratic and q is even then n must also be even, so in particular $n \geq 4$. Let f_ϕ be the associated bilinear form of ϕ and let $u \in V$ with $f_\phi(u, v) = \phi(v)$, so that $W := \langle u, v\rangle$ is non-degenerate with $\dim\left(W^\perp\right) \geq 2$. Note that $\phi = \overline{\phi}$, hence $\operatorname{Im}\phi|_{W^\perp} = \mathbb{F}_q$ by Lemma 3.3.4. In particular there exists $x \in W^\perp$ with $\phi(x) = \phi(u + v)$. Setting $w := u + v + x$, we again get $w, v - w \in S_0$, and therefore $S_\# \subseteq S_0 + S_0$. This completes the proof. □

Lemma 5.2.3. *Let $V = \mathbb{F}_q^n$, ϕ be a unitary or nondegenerate quadratic form on V, $\overline{\phi}$ as in* (3.3.2) *and S_λ as in* (3.3.1)*. Then $S_0 \subseteq S_\mu + S_\mu$ for any $\mu \in (\operatorname{Im}\overline{\phi})^\#$, if ϕ is unitary and $n \geq 2$, or if ϕ is quadratic and $n \geq 4$.*

Proof. Let $v \in S_0$. Suppose first that either ϕ is unitary and $n \geq 3$, or ϕ is nondegenerate quadratic with $n \geq 4$. Then by Corollary 3.3.5, for any $\mu \in (\operatorname{Im}\overline{\phi})^\#$ there exists $w \in S_\mu \cap \langle v\rangle^\perp$. It is easy to verify that $\phi(v - w) = \phi(w)$, so $v - w \in S_\mu$ and $v \in S_\mu + S_\mu$. Therefore $S_0 \subseteq S_\mu + S_\mu$.

If $\phi = f$ is unitary and $n = 2$ then $\langle v\rangle^\perp = \langle v\rangle$ for any $v \in S_0$. We claim that there exists $u \in S_0$ such that $f(u, v) = 1$. Indeed, take $x \in V \setminus \langle v\rangle$. Then $f(v, x) \neq 0$. If $x \in S_0$ define $u' := x$; if $x \notin S_0$ let $u' := \alpha v + f(x, x)^{-1}x$ where $\alpha \in \mathbb{F}_q$ with $Tr(\alpha) = -f(x, x)$. Then in both cases $u' \in S_0$ and $f(u', v) \neq 0$, and we take u to be the suitable scalar multiple of u'. This proves the claim. Let $w := \beta u + \gamma v$, where $\beta, \gamma \in \mathbb{F}_q$ with $Tr(\beta) = 0$ and $Tr(\beta^{q_0}\gamma) = \mu$. Then $w, v - w \in S_\mu$, and thus $v \in S_\mu + S_\mu$. Therefore $S_0 \subseteq S_\mu + S_\mu$. □

The diameter 2 Cayley graphs arising from $\Gamma\mathrm{U}(V)$ can now be easily deduced from the three results above.

Proposition 5.2.4. *Let* Γ *be a graph and* $G \leq \mathrm{Aut}\,(\Gamma)$ *such that* G *satisfies Hypothesis* 5.1.2 *with* $G_0 = \Gamma\mathrm{U}(n, q)$. *Then* Γ *is* G*-symmetric with diameter* 2 *if and only if* $n \geq 2$ *and* $\Gamma \cong \mathrm{Cay}(V, S)$, *where* $V = \mathbb{F}_q^n$ *and* $S \in \{S_0, S_\#\}$.

Proof. By Lemma 5.1.1 and Proposition 5.2.1 we only need to prove that $\mathrm{Cay}(V, S)$ has diameter 2 if and only if $n \geq 2$. If $n = 1$ then V is anisotropic, so $\mathrm{GU}(n, q)$ is transitive on $V^\#$ by Proposition 5.2.1 (1) and $\mathrm{Cay}(V, S)$ is a complete graph. If $n \geq 2$ then $V^\# \setminus S_0 = S_\#$ and $V^\# \setminus S_\# = S_0$ by Proposition 5.2.1 (1). Hence the result follows from Lemma 5.2.2 if $S = S_0$, and from Lemma 5.2.3 if $S = S_\#$. □

Proposition 5.2.6 gives the diameter 2 Cayley graphs that arise from the general orthogonal groups. Its proof uses the following technical lemma.

Lemma 5.2.5. *Suppose that* $q \geq 5$ *and is odd.*

(1) For any $\alpha \in \mathbb{F}_q^\#$, *there exist* $\beta \in \mathbb{F}_q^\square$ *and* $\gamma \in \mathbb{F}_q^\boxtimes$ *such that* $\alpha = \beta + \gamma$.
(2) For any $\alpha \in \mathbb{F}_q^\#$, *there exist* $\beta, \gamma \in \mathbb{F}_q^\# \setminus \alpha\mathbb{F}_q^\square$ *such that* $\alpha = \beta - \gamma$.

Proof. Since $q \geq 5$, there exist $\beta_0 \in \mathbb{F}_q^\square$ and $\gamma_0 \in \mathbb{F}_q^\boxtimes$ with $\beta_0 + \gamma_0 \neq 0$. For any $\alpha \in \mathbb{F}_q^\#$ we have $\alpha = \delta\beta_0 + \delta\gamma_0$, where $\delta := \alpha(\beta_0 + \gamma_0)^{-1}$. Clearly $\delta\beta_0 \notin \delta\gamma_0\mathbb{F}_q^\square$, and we can take $\{\beta, \gamma\} = \{\delta\beta_0, \delta\gamma_0\}$. This proves (1).

It follows from (1) that for any $\beta' \in \mathbb{F}_q^\boxtimes$, there exist $\gamma' \in \mathbb{F}_q^\boxtimes$ and $\delta' \in \mathbb{F}_q^\square$ such that $\beta' = \gamma' + \delta'$; multiplying both sides by $(\delta')^{-1}$, we get that for some $\beta_0, \gamma_0 \in \mathbb{F}_q^\boxtimes$ we have $\beta_0 = \gamma_0 + 1$. For any $\alpha \in \mathbb{F}_q^\#$ set $\gamma := \gamma_0^{-1}\alpha$. Then $\alpha = \alpha\beta_0 - \alpha\gamma_0$, with $\alpha\beta_0, \alpha\gamma_0 \notin \alpha\mathbb{F}_q^\square$, so we can take $\beta = \alpha\beta_0$ and $\gamma = \alpha\gamma_0$. Thus we have proved (2). □

Proposition 5.2.6. *Let* Γ *be a graph and* $G \leq \mathrm{Aut}\,(\Gamma)$ *such that* G *satisfies Hypothesis* 5.1.2 *with* $G_0 = \Gamma\mathrm{O}(n, q)$ *or* $G_0 = \Gamma\mathrm{O}^\epsilon(n, q)$ *(*$\epsilon = \pm$*). Then* Γ *is* G*-symmetric with diameter* 2 *if and only if* $\Gamma \cong \mathrm{Cay}(V, S)$ *with* $V = \mathbb{F}_q^n$ *and the conditions listed in Table* 5.2.1 *hold.*

Proof. By Lemma 5.1.1 and Proposition 5.2.1 it remains to prove that $\mathrm{Cay}(V, S)$ has diameter 2 if and only if the conditions in Table 5.2.1 hold. Suppose first that $n = 2$. Then by Proposition 5.2.1 (2) the G_0-orbits in $V^\#$ are S_0 and $S_\#$. If ϕ is of minus type then V is anisotropic, so $S_\# = V^\#$ and there is no graph of diameter 2. If ϕ is of plus type then V has a basis $\{x, y\}$ which is a hyperbolic pair, and we have $S_0 = \langle x\rangle^\# \cup \langle y\rangle^\#$ and $S_\# = \left\{\alpha x + \beta y \mid \alpha, \beta \in \mathbb{F}_q^\#\right\}$. Then $V^\# \setminus S_0 = S_\# \subseteq S_0 + S_0$, so $\mathrm{diam}(\mathrm{Cay}(V, S_0)) = 2$. If

	n	q	ϕ	S
1	2	2	plus-type	S_0
2	2	$q>2$	plus-type	$S_0, S_\#$
3	$n>2$, even	all q	plus-/minus-type	$S_0, S_\#$
4	3	3		S_0
5	3	$q>3$		$S_0, S_\Box, S_\boxtimes$
6	$n>3$, odd	all q		$S_0, S_\Box, S_\boxtimes$

TABLE 5.2.1

$q=2$ then $S_\# = \{x+y\}$, so $\mathrm{Cay}(V, S_\#)$ is disconnected and we get the first line of Table 5.2.1. If $q>2$, then $e=(\alpha x+y)+((1-\alpha)x-y) \in S_\# + S_\#$ where $\alpha \in \mathbb{F}_q^\# \setminus \{1\}$, and similarly $f \in S_\# + S_\#$. Thus $V \setminus S_\# = S_0 \subseteq S_\# + S_\#$ and $\mathrm{diam}(\mathrm{Cay}(V, S_\#)) = 2$, which yields one case of line 2 of Table 5.2.1. Now suppose that $n>2$ with n even. Then the G_0-orbits in $V^\#$ are again S_0 and $S_\#$, and it follows from Lemmas 5.2.2 and 5.2.3 that $\mathrm{Cay}(V, S_0)$ and $\mathrm{Cay}(V, S_\#)$ both have diameter 2. This gives lines 2 and 3 of Table 5.2.1.

From now on assume that n is odd. Then the G_0-orbits in $V^\#$ are S_0, $S_\Box$ and $S_\boxtimes$. It again follows from Lemma 5.2.2 that $\mathrm{diam}(\mathrm{Cay}(V, S_0)) = 2$. For $\mathrm{Cay}(V, S_\theta)$, $\theta \in \{\Box, \boxtimes\}$, we consider three cases.

Case 1: Suppose that $n=3$ and $q=3$. Then $\mathbb{F}_3^\Box = \{1\}$ and $\mathbb{F}_3^\boxtimes = \{2\}$. Let $v \in S_0$. If also $v \in S_\theta + S_\theta$, then $w, v-w \in S_\theta$ for some $w \in V$, so that $\phi(w) = \phi(v-w)$ and $B(v,w)=0$. So $w \in \langle v\rangle^\perp$, and thus $\mathrm{Im}\,\phi|_{\langle v\rangle^\perp} = \{\phi(w), 0\}$ by Corollary 3.3.5 (3). Since there exists $u \in S_0$ with $\mathrm{Im}\,\phi|_{\langle u\rangle^\perp} \neq \{\phi(w), 0\}$, we conclude that $S_0 \nsubseteq S_\theta + S_\theta$. Hence $\mathrm{diam}(\mathrm{Cay}(V, S_\theta)) \neq 2$, which proves line 4 of Table 5.2.1.

Case 2: Suppose that $n=3$ and $q>3$, and let $v \in V^\# \setminus S$. If $v \in S_0$, take $u \in V$ such that $\{u, v\}$ is a hyperbolic pair. Then $\mathrm{Im}\,\phi|_{\langle u,v\rangle} = \mathbb{F}_q$ by Lemma 3.3.4, and hence there exists $w' \in S_\theta \cap \langle u, v\rangle$. It follows from Lemma 5.2.5 (1) that we can find $\beta \in \mathbb{F}_q^\# \setminus \mathbb{F}_q^\theta$ such that $\phi(w') - \beta \in \mathbb{F}_q^\theta$; set $w := \beta u + (\phi(w')\beta^{-1})v$. Then $w, v-w \in \mathbb{F}_q^\theta$ and $v \in S_\theta + S_\theta$. So $S_0 \subseteq S_\theta + S_\theta$. If $v \in S_{\theta'} := S_\# \setminus S_\theta$, then $\mathrm{Im}\,\phi|_{\langle v\rangle^\perp} = \mathbb{F}_q$ by Lemma 3.3.4. By Lemma 5.2.5 (2) there are elements $\gamma, \delta \in \mathbb{F}_q^\theta$ such that $\phi(v) = \delta - \gamma$, and hence $\phi(v) + \gamma \in \mathbb{F}_q^\theta$. Take $w \in \langle v\rangle^\perp$ such that $\phi(w) = \gamma$; then $w, v-w \in S_\theta$ and $S_{\theta'} \subseteq S_\theta + S_\theta$. Therefore $\mathrm{diam}(\mathrm{Cay}(V, S_\theta)) = 2$ for $\theta \in \{\Box, \boxtimes\}$, which proves line 5 of Table 5.2.1.

Case 3: Suppose that $n>3$. Then $S_0 \subseteq S_\theta + S_\theta$ by Lemma 5.2.3. If $v \in S_{\theta'} := S_\# \setminus S_\theta$ then $\mathrm{Im}\,\phi|_{\langle v\rangle^\perp} = \mathbb{F}_q$ by Corollary 3.3.5 (1). If $q=3$ take $u \in \langle v\rangle^\perp$ with $\phi(u) = \phi(v)$, and set $w := -(u+v)$. Then $w, v-w \in \mathbb{F}_q^\theta$ and $S_{\theta'} \subseteq S_\theta + S_\theta$, so $\mathrm{diam}(\mathrm{Cay}(V, S_\theta)) = 2$. If $q>3$ then by Lemma 5.2.5 (2) there is a $\gamma \in \mathbb{F}_q^\theta$ such that $\phi(v) + \gamma \in \mathbb{F}_q^\theta$. Take $w \in \langle v\rangle^\perp$ with $\phi(w) = \gamma$. Then $w, v-w \in \mathbb{F}_q^\theta$, so again $S_{\theta'} \subseteq S_\theta + S_\theta$ and $\mathrm{diam}(\mathrm{Cay}(V, S_\theta)) = 2$. This proves line 6 of Table 5.2.1. $\Box$

5.3. Class $\mathcal{C}_2$

In this case $V = \oplus_{i=1}^t U_i$, where $U_i = \mathbb{F}_q^m$ for each i, $mt = n$, $m \geq 2$ and $t \geq 2$. Assume that $\mathcal{B} = \bigcup_{i=1}^t \mathcal{B}_i$, where each $\mathcal{B}_i$ is a basis for U_i. We write the elements of V as t-tuples over $\mathbb{F}_q^m$; under this identification the τ-action is equivalent to the natural componentwise action.

Assume first that $H = \Gamma\mathrm{L}(n,q)$. Then by Theorem 3.6.2 we have

$$G_0 = (\mathrm{GL}(m,q) \wr \mathrm{Sym}\,(t)) \rtimes \langle \tau \rangle, \tag{5.3.1}$$

and so

$$L = G_0 \cap \mathrm{GL}(n,q) = \mathrm{GL}(m,q) \wr \mathrm{Sym}\,(t)\,. \tag{5.3.2}$$

Lemma 5.3.1. *Let G_0 be as in* (5.3.1). *Then the G_0-orbits in $V^{\#}$ are the sets X_s for each $s \in \{1, \ldots, t\}$, where*

$$X_s := \{(u_1, \ldots, u_t) \in V^{\#} \mid \textit{exactly } s \textit{ coordinates nonzero}\}. \tag{5.3.3}$$

Proof. Let $v = (u_1, \ldots, u_t) \in X_s$. Then clearly $v^{G_0} \subseteq X_s$. For any $w \in X_s$, say, $w = (x_1, \ldots, x_t)$, take $\pi \in \mathrm{Sym}\,(t)$ such that $u_{i'} = \mathbf{0}$ if and only if $x_i = \mathbf{0}$, where $i' := i^{\pi^{-1}}$. Then there are elements $g_1, \ldots, g_t \in \mathrm{GL}(m,q)$ such that $u_{i'}^{g_{i'}} = x_i$ for all i. Hence $v^{(g_1,\ldots,g_t)\pi} = w$, so $X_s \subseteq v^L \subseteq v^{G_0}$. Therefore X_s is a G_0-orbit for each s, and $X_1, \ldots, X_t$ are all the G_0-orbits in $V^{\#}$. □

Proposition 5.3.2. *Let Γ be a graph and $G \leq \mathrm{Aut}\,(\Gamma)$ such that G satisfies Hypothesis* 5.1.2 *with G_0 as in* (5.3.1). *Then Γ is G-symmetric with diameter* 2 *if and only if $\Gamma \cong \mathrm{Cay}(V, X_s)$, where X_s is as in* (5.3.3), *such that $q^m > 2$ and $s \geq t/2$.*

Proof. In view of Lemmas 5.1.1 and 5.3.1, we only need to show that $V = X_s \cup (X_s + X_s)$ under the given conditions.

Suppose first that $q^m = 2$. Then $V = \oplus_{i=1}^t \mathbb{F}_2$. Fix $s \in \{1, \ldots, t\}$ and let $u, w \in X_s$. Then $u + w \in X_r$, where r is the number of positions in which u and w differ, so r is even. That is, $X_{r_0} \nsubseteq X_s + X_s$ whenever r_0 is odd, and if there exists an odd $r_0 \in \{1, \ldots, t\}$ with $r_0 \neq s$ then $\mathrm{diam}(\Gamma) > 2$ by Lemma 5.1.1. In particular we have $\mathrm{diam}(\Gamma) > 2$ for all $t \geq 3$, and if $t = 2$ then $\mathrm{diam}(\Gamma) = 2$ if and only if $S = X_1$. In the last case, however, we have $G_0 = C_2 \times C_2$ and G is not quasiprimitive.

Now suppose that $q^m > 2$. If $s < t/2$ then $X_t \nsubseteq X_s + X_s$, so $\mathrm{diam}(\Gamma) > 2$. Assume from now on that $s \geq t/2$, and take $u = (u_1, \ldots, u_t) \in X_s$. For each $r < s$, take $w = (w_1, \ldots, w_t) \in X_s$ with $w_i = -u_i$ in $t - r$ positions and $w_i \neq -u_i$ in the rest, and for each $r > s$ take $w \in X_s$ with $u_i \neq w_i = \mathbf{0}$ for $1 \leq i \leq r - s$, $w_i \neq u_i = \mathbf{0}$ for $r - s + 1 \leq i \leq s$, and $u_i \neq -w_i$ (both nonzero) for $s + 1 \leq i \leq r$. Then $u + w \in X_r$ in each case, so $X_r \subseteq X_s + X_s$ for all $r \neq s$. Therefore $\mathrm{diam}(\Gamma) = 2$. □

We now consider the case where $H = \Gamma\mathrm{Sp}(n,q)$ with $n \geq 4$. Recall from Section 3.6.1 that we have two subcases:

($\mathcal{C}_2$.1) The dimension m is even and U_i is a symplectic space for each i, and the subspaces U_i are pairwise orthogonal. Then by Theorem 3.6.3,

$$\begin{aligned} G_0 = \{(g_1,\dots,g_t)\pi\sigma \mid \pi \in \mathrm{Sym}\,(t)\,,\, \sigma \in \langle\tau\rangle,\, g_i \in \mathrm{GSp}(m,q),\\ \lambda(g_i) = \lambda(g_1)\} \\ \cong (\mathrm{Sp}(m,q)^t.[q-1].\mathrm{Sym}\,(t)) \rtimes \langle\tau\rangle, \end{aligned} \tag{5.3.4}$$

where $\lambda : \mathrm{GSp}(n,q) \to \mathbb{F}_q^{\#}$ is as defined in (3.3.3), so that

$$L = G_0 \cap \mathrm{GL}(n,q) \cong \mathrm{Sp}(m,q)^t.[q-1].\mathrm{Sym}\,(t)\,.$$

($\mathcal{C}_2$.2) The dimension $m = n/2$ so that $t = 2$, and both subspaces U_i are totally singular with dimension $n/2$. Also q is odd if $n = 4$. By Theorem 3.6.3 we have

$$\begin{aligned} G_0 &= \left\{\left(g, g^{-\top}\right)\pi\sigma \,\middle|\, \pi \in \mathrm{Sym}\,(t)\,,\, \sigma \in \langle\tau\rangle,\, g \in \mathrm{GL}(m,q)\right\} \\ &\cong (\mathrm{GL}(m,q).[2]) \rtimes \langle\tau\rangle, \end{aligned} \tag{5.3.5}$$

where $g^{\top}$ denotes the transpose of g, and $g^{-\top} = (g^{\top})^{-1}$. Then

$$L = G_0 \cap \mathrm{GL}(n,q) \cong \mathrm{GL}(m,q).[2]. \tag{5.3.6}$$

Lemma 5.3.3. *For each $s \in \{1,\dots,t\}$ let X_s be as in* (5.3.3). *The G_0-orbits in $V^{\#}$ are*

(1) the sets X_s for each $s \in \{1,\dots,t\}$ if case ($\mathcal{C}_2$.1) holds and G_0 is as in (5.3.4)*;*

(2) the sets X_1 and $\bigcup_{\sigma\in\langle\tau\rangle} W_{\beta^\sigma}$ for all $\beta \in \mathbb{F}_q$, if case ($\mathcal{C}_2$.2) holds and G_0 is as in (5.3.5)*, where*

$$W_\beta := (w_1, x_\beta)^L, \tag{5.3.7}$$

L is as in (5.3.6) *and $w_1 := (1,0,\dots,0) \in \mathbb{F}_q^m$, and $x_\beta \in (\mathbb{F}_q^m)^{\#}$ with first component β.*

Proof. The proof of part (1) is similar to that of Lemma 5.3.1, and uses the transitivity of $\mathrm{Sp}(m,q)$ on $U_i^{\#}$, so we only need to prove part (2). Assume that case ($\mathcal{C}_2$.2) holds. Then $L = K.\mathrm{Sym}\,(2)$, where $K := \left\{\left(g, g^{-\top}\right) \,\middle|\, g \in \mathrm{GL}(m,q)\right\}$. It is easy to see that $U_1 \oplus \{\mathbf{0}\}$ and $\{\mathbf{0}\} \oplus U_2$ are K-orbits, so $X_1 = (U_1 \otimes \{\mathbf{0}\}) \cup (\{\mathbf{0}\} \oplus U_2)$ is a G_0-orbit. Let $(u,v) \in X_2$, and for any $\beta \in \mathbb{F}_q$ define

$$w_\beta := \begin{cases} (\beta,0,\dots,0) & \text{if } \beta \neq 0, \\ (0,1,0,\dots,0) & \text{if } \beta = 0. \end{cases} \tag{5.3.8}$$

Since $w_1 \in u^{\mathrm{GL}(m,q)}$ we can assume that $u = w_1$. Suppose that $v = (\beta, v_2, \dots, v_m)$.

Claim 1: $(w_1, y) \in (w_1, v)^K$ *if and only if* $y = (\beta, y_2, \dots, y_m)$ *for some* $y_2, \dots, y_m \in \mathbb{F}_q$. Indeed, $(w_1, y) \in (w_1, v)^K$ if and only if $y = v^{h^{-\top}}$ for some $h \in \mathrm{Stab}_{\mathrm{GL}(m,q)}(w_1)$. Now $w_1^h = w_1$ if and only if the matrix of $h^{-\top}$ has the form

$$\left(\begin{array}{c|c} 1 & C \\ \hline 0 & \\ \vdots & D \\ 0 & \end{array}\right)$$

where C is a $1 \times (m-1)$ matrix over $\mathbb{F}_q$ and $D \in \mathrm{GL}(m-1, q)$. Clearly, the orbit of v under the subgroup $\{h^{-\top} \mid h \in \mathrm{Stab}_{\mathrm{GL}(m,q)}(w_1)\}$ is the set of all nonzero vectors in $\mathbb{F}_q^m$ with first component β. Therefore Claim 1 holds.

Claim 2: $(w_1, v)^L = (w_1, v)^K$. By Claim 1 we can assume that $v = w_\beta$. If $\beta \neq 0$ let

$$g := \left(\begin{array}{c|ccc} \beta & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & I_{m-1} & \\ 0 & & & \end{array}\right).$$

If $\beta = 0$ let $g := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ if $m = 2$, and

$$g := \left(\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline & & \\ \multicolumn{2}{c|}{0} & I_{m-2} \\ & & \end{array}\right)$$

if $m > 2$. Then $g \in \mathrm{GL}(m, q)$ for all cases, and $w_1^g = w_1^{g^\top} = v$. Hence $(w_1^g, v^{g^{-\top}}) = (v, w_1)$, so that $(v, w_1) \in (w_1, v)^K$. Therefore $(w_1, v)^L = (w_1, v)^K \cup (v, w_1)^K = (w_1, v)^K$, which proves Claim 2.

It follows from Claims 1 and 2 that each set W_β is an L-orbit (and moreover $W_\beta = W_{\beta'}$ if and only if $\beta = \beta'$). It follows from the definition of the τ-action on $V^\#$ that $(w_1, v)^{G_0} = \bigcup_{\sigma \in \langle \tau \rangle} W_{\beta^\sigma}$. This completes the proof of part (2). □

Proposition 5.3.4. *Let* Γ *be a graph and* $G \leq \mathrm{Aut}(\Gamma)$ *such that* G *satisfies Hypothesis* 5.1.2 *with* $H = \Gamma\mathrm{Sp}(n, q)$ *and* $i = 2$*. Then* Γ *is* G*-symmetric with diameter* 2 *if and only if* $\Gamma \cong \mathrm{Cay}(V, S)$*, where*

(1) if case $(\mathcal{C}_2.1)$ *holds, then* $q^m > 2$*,* G_0 *is as in* (5.3.4)*,* $S = X_s$*, and* $s \geq t/2$*;*

(2) if case $(\mathcal{C}_2.2)$ *holds with* $q = 2$*, then* G_0 *is as in* (5.3.5) *and* $S = W_\beta$ *for any* $\beta \in \mathbb{F}_q$*;*

(3) if case $(\mathcal{C}_2.2)$ *holds with* $q^m > 2$*, then* G_0 *is as in* (5.3.5)*, and* $S = X_1$ *or* $S = \bigcup_{\sigma \in \langle \tau \rangle} W_{\beta^\sigma}$ *for some* $\beta \in \mathbb{F}_q$*;*

with X_s *as in* (5.3.3) *and* W_β *as* (5.3.7).

PROOF. The graph of (1) is precisely that of Proposition 5.3.2, and the fact that it is G-symmetric follows from Lemma 5.1.1. So assume that case ($\mathcal{C}_2$.2) holds. By Lemma 5.1.1 we only need to show that $V = S \cup (S+S)$ unless $S = X_1$ and $q = 2$. It follows from Proposition 5.3.2 that $\mathrm{Cay}(V, X_1)$ has diameter 2 (with G quasiprimitive) if and only if $q^m > 2$. Thus we may assume that $S = \bigcup_{\sigma \in \langle \tau \rangle} W_{\beta^\sigma}$ for some $\beta \in \mathbb{F}_q$. It remains to prove that $V = S \cup (S+S)$.

Let w_β be as in (5.3.8) and $\gamma \in \mathbb{F}_q$, with $\gamma \neq \beta$. Define

$$g_0 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } h_0 := \begin{pmatrix} 0 & -1 \\ -1 & \gamma_0 \end{pmatrix},$$

where $\gamma_0 := 1 - \beta^{-1}\gamma$ if $\beta \neq 0$ and $\gamma_0 := 0$ if $\beta = 0$. If $m = 2$ let $g := g_0$ and $h := h_0$; if $m \geq 3$ define g and h by

$$g := \begin{pmatrix} g_0 & 0 \\ 0 & I_{m-2} \end{pmatrix}$$

and

$$h := \left(\begin{array}{c|ccc} \multirow{2}{*}{h_0} & 0 & \cdots & 0 \\ & 1 & \cdots & 1 \\ \hline 0 & & I_{m-2} & \end{array}\right).$$

Then $g, h \in \mathrm{GL}(m, q)$ for all $m \geq 2$, and $w_1^g + w_1^h = w_1$. Recall that q is odd if $m = 2$, so we can take $x \in (\mathbb{F}_q^m)^\#$ where

$$x := \begin{cases} w_\beta & \text{if } \beta \neq 0; \\ (0, -\gamma/2) & \text{if } \beta = 0 \text{ and } m = 2; \\ (0, 0, 1, 0, \ldots, 0) & \text{if } \beta = 0 \text{ and } m \geq 3. \end{cases}$$

Then for all cases $y := x^{g^{-\top}} + x^{h^{-\top}}$ has first component γ. Hence, applying Lemma 5.3.3, we have $W_\gamma = (w_1, y)^{G_0} \subseteq W_\beta + W_\beta$ for any $\gamma \neq \beta$. Since also $\{\mathbf{0}\} \cup X_1 \subseteq W_\beta + W_\beta$, it follows that $V = W_\beta \cup (W_\beta + W_\beta)$. Therefore $V = S \cup (S+S)$, which completes the proof of parts (2) and (3). □

5.4. Class $\mathcal{C}_4$

In this case $V = U \otimes W = \mathbb{F}_q^k \otimes \mathbb{F}_q^m$ with $k, m \geq 2$, and $\mathcal{B}$ is a tensor product basis of V (see Section 3.1), say,

$$\mathcal{B} = \{u_i \otimes w_j \mid 1 \leq i \leq k,\ 1 \leq j \leq m\},$$

where $\mathcal{B}_U := \{u_1, \ldots, u_k\}$ and $\mathcal{B}_W := \{w_1, \ldots, w_m\}$ are fixed bases of U and W, respectively. We choose τ to fix each of the vectors $u_i \otimes w_j$. Then for any simple vector $u \otimes w \in V$, we have $(u \otimes w)^\tau = u^\tau \otimes w^\tau$, and for any $v = \sum_{i=1}^r (a_i \otimes b_i) \in V$,

$$v^\tau = \sum_{i=1}^r a_i^\tau \otimes b_i^\tau.$$

Recall that $k \neq m$ in the description given in Section 3.6.1; however, all of the results in this section also hold for $k = m$, so we do not assume that k and m are distinct. In this way the results yield useful information for the $\mathcal{C}_7$ case.

Recall from Section 3.1 that the tensor weight $\mathrm{wt}\,(v)$ of $v \in V^{\#}$, in the decomposition $V = \mathbb{F}_q^k \otimes \mathbb{F}_q^m$, is the least number s such that v can be written as the sum of s simple vectors in $\mathbb{F}_q^k \otimes \mathbb{F}_q^m$. It follows from Lemma 3.1.1 that $\mathrm{wt}\,(v) \leq \min\{k, m\}$ for any $v \in V^{\#}$, and that for each $s \in \{1, \ldots, \min\{k, m\}\}$ there is a vector $v \in V^{\#}$ with weight s.

Lemma 5.4.1. *For any $v \in V^{\#}$ we have $\mathrm{wt}\,(v^\sigma) = \mathrm{wt}\,(v)$ for each $\sigma \in \langle \tau \rangle$.*

Proof. Let $v = \sum_{i=1}^{\mathrm{wt}(v)} a_i \otimes b_i \in V^{\#}$. It follows from the above that

$$v^\sigma = \sum_{i=1}^{\mathrm{wt}(v)} a_i^\sigma \otimes b_i^\sigma$$

for any $\sigma \in \langle \tau \rangle$, so $\mathrm{wt}\,(v^\sigma) \leq \mathrm{wt}\,(v)$. Likewise $\mathrm{wt}\left(v^{\sigma^{-1}}\right) \leq \mathrm{wt}\,(v)$, so $\mathrm{wt}\,(v) \leq \mathrm{wt}\,(v^\sigma)$. Therefore $\mathrm{wt}\,(v^\sigma) = \mathrm{wt}\,(v)$. □

Assume that $H = \Gamma\mathrm{L}(n, q)$. By Theorem 3.6.2,

$$G_0 = (\mathrm{GL}(k, q) \otimes \mathrm{GL}(m, q)) \rtimes \langle \tau \rangle \tag{5.4.1}$$

and

$$L = G_0 \cap \mathrm{GL}(n, q) = \mathrm{GL}(k, q) \otimes \mathrm{GL}(m, q). \tag{5.4.2}$$

Lemma 5.4.2. *Let G_0 be as in* (5.4.1)*. Then the G_0-orbits in $V^{\#}$ are the sets Y_s for each $s \in \{1, \ldots, \min\{k, m\}\}$, where*

$$Y_s := \{v \in V^{\#} \mid \mathrm{wt}\,(v) = s\}. \tag{5.4.3}$$

Proof. Let $v \in Y_s$, say, $v = \sum_{i=1}^{s} a_i \otimes b_i$. It follows from Lemmas 3.1.1 and 5.4.1 that $v^{G_0} \subseteq Y_s$. Let $v' = \sum_{i=1}^{s} a'_i \otimes b'_i \in Y_s$. It follows from Lemma 3.1.1 that we can find $g \in \mathrm{GL}(k, q)$ and $h \in \mathrm{GL}(m, q)$ for which $a_i^g = a'_i$ and $b_i^g = b'_i$ for all i. So $v^{g \otimes h} = v'$, and thus $Y_s \subseteq v^L \subseteq v^{G_0}$. Therefore Y_s is an orbit of G_0 for all $s \in \{1, \ldots, \min\{k, m\}\}$, and the sets Y_s are all the G_0-orbits in $V^{\#}$. □

Proposition 5.4.3. *Let Γ be a graph and $G \leq \mathrm{Aut}\,(\Gamma)$ such that G satisfies Hypothesis 5.1.2 with G_0 as in* (5.4.1)*, where k and m may be equal. Then Γ is G-symmetric with diameter 2 if and only if $\Gamma \cong \mathrm{Cay}(V, Y_s)$, where $s \geq \frac{1}{2}\min\{k, m\}$ and Y_s is as in* (5.4.3).

Proof. As in the proof of Proposition 5.3.2 we only need to show that $V \setminus Y_s \subseteq Y_s + Y_s$ under the given conditions. Set $\mu := \min\{k, m\}$. If $s < \mu/2$ then it follows from Lemma 3.1.1 that $Y_\mu \nsubseteq Y_s + Y_s$, so $\mathrm{diam}(\Gamma) > 2$ in this case. Assume from now on that $s \geq \mu/2$. Let $v = \sum_{i=1}^{s} u_i \otimes w_i \in Y_s$, and $r \in \{1, \ldots, \mu\}$ with $r \neq s$. If $r < s$ take $z = \sum_{i=1}^{s} x_i \otimes w_i$, where $x_i = u_{i+1} - u_i$ for $1 \leq i \leq r - 1$, $x_r = u_1 - u_r$, and $x_i = -u_i$ for $r + 1 \leq i \leq s$. Then

$z \in Y_s$ and $v + z \in Y_r$ by Lemma 3.1.1, so $Y_r \subseteq Y_s + Y_s$. If $r > s$, extend $\{u_1, \ldots, u_s\}$ and $\{w_1, \ldots, w_s\}$ to linearly independent sets $\{u_1, \ldots, u_r\} \subset \mathbb{F}_q^k$ and $\{w_1, \ldots, w_r\} \subseteq \mathbb{F}_q^m$. Take $z = \sum_{i=r-s+1}^{r} x_i \otimes w_i$ with the vectors x_i chosen as follows: if $r = 2s$, then $x_i = u_i$ for $s+1 \leq i \leq r$; if $r = 2s-1$ then $x_s = u_r - u_s$, $x_i = u_i$ for $s+1 \leq i \leq r-1$, and $x_r = u_s$; and if $r \notin \{2s, 2s-1\}$, then $x_i = u_{i+1} - u_i$ for $r-s+1 \leq i \leq s-1$, $x_s = u_{r-s+1} - u_s$ and $x_i = u_i$ for $s+1 \leq i \leq r$. Again by Lemma 3.1.1 we have $z \in Y_s$ and $v + z \in Y_r$, so $Y_r \subseteq Y_s + Y_s$. Therefore $Y_r \subseteq Y_s + Y_s$ for all $r \neq s$, and thus $\mathrm{diam}(\Gamma) = 2$. $\square$

Now assume that $H = \Gamma\mathrm{Sp}(n, q)$. In this case k is even, $m \geq 3$, q is odd, and $\phi = \phi_U \otimes \phi_W$ (see Subsection 3.3.2), where ϕ_U is a symplectic form on U and ϕ_W is a nondegenerate symmetric bilinear form on W. By Theorem 3.6.3

$$G_0 = (\mathrm{GSp}(k, q) \otimes \mathrm{GO}^{\epsilon}(m, q)) \rtimes \langle \tau \rangle, \tag{5.4.4}$$

and

$$L = \mathrm{GSp}(k, q) \otimes \mathrm{GO}^{\epsilon}(m, q).$$

Recall from Proposition 5.2.1 that the $\mathrm{GO}^{\epsilon}(m, q)$-orbits in $W^{\#}$ are S_0 and $S_{\#}$ if m is even, and S_0, $S_{\square}$ and $S_{\boxtimes}$ if m is odd, with S_0 as defined in (3.3.1) and $S_{\#}$, $S_{\square}$ and $S_{\boxtimes}$ as in (5.2.1). For each $s \in \{1, \ldots, \min\{k, m\}\}$ let Y_s be as in (5.4.3).

If $v = \sum_{i=1}^{s} a_i \otimes b_i \in Y_s$, it is easy to see that

$$v^{G_0} = \left\{ \sum_{i=1}^{s} a_i' \otimes b_i' \;\middle|\; a_i \in U^{\#},\ b_i' \in b_i^{\mathrm{GO}^{\epsilon}(m,q)} \right\}.$$

If $s = 1$ then the set Y_1 of simple vectors splits into the G_0-orbits Y_1^{θ}, where $\theta \in \{0, \#\}$ if m is even and $\theta \in \{0, \square, \boxtimes\}$ if m is odd, and

$$Y_1^{\theta} := \left\{ a \otimes b \mid a \in U^{\#},\ b \in S_{\theta} \right\}.$$

If $s > 1$ suppose that exactly r of the vectors b_i belong in $S_{\#}$ for some r, $0 \leq r \leq s$; if m is odd suppose further that exactly $r_{\square}$ belong in $S_{\square}$ and $r_{\boxtimes}$ in $S_{\boxtimes}$. If m is even then $v^{G_0} \subset Y_s^r$, where

$$Y_s^r := \left\{ \sum_{i=1}^{s} a_i' \otimes b_i' \in Y_s \;\middle|\; \text{exactly } r \text{ of the vectors } b_i' \text{ are in } S_{\#} \right\},$$

and if m is even then $v^{G_0} \subset Y_s^{r_{\square}, r_{\boxtimes}}$, where

$$Y_s^{r_{\square}, r_{\boxtimes}} := \left\{ \sum_{i=1}^{s} a_i' \otimes b_i' \in Y_s \;\middle|\; \text{exactly } r_{\theta} \text{ of the vectors } b_i' \text{ are in } S_{\theta} \right\}.$$

Note that the sets Y_s^r and $Y_s^{r_{\square}, r_{\boxtimes}}$ above are, in general, not G_0-orbits. For instance, if $s = 2$, the weight-2 vectors $a_1 \otimes b_1 + a_2 \otimes b_2, a_1' \otimes b_1' + a_2' \otimes b_2' \in Y_2^0$ (or $Y_2^{0,0}$ if m is even), such that $b_1 \perp b_2$ and $b_1' \not\perp b_2'$, belong to different G_0-orbits.

Proposition 5.4.4. *Let* Γ *be a graph and* $G \leq \mathrm{Aut}(\Gamma)$ *such that* G *satisfies Hypothesis* 5.1.2 *with* G_0 *as in* (5.4.4)*, where* k *and* m *may be equal. If* Γ *is* G*-symmetric with* *diameter* 2*, then* $\Gamma \cong \mathrm{Cay}(V, S)$ *where* $S = v^{G_0}$ *for some* $v \in Y_s$*, where* Y_s *is as in* (5.4.3) *and* $s \geq \frac{1}{2}\min\{k, m\}$*.*

PROOF. This follows immediately from the discussion above and Proposition 5.4.3. □

5.5. Class $\mathcal{C}_5$

In this case $n \geq 2$, d/n is composite with a prime divisor r, and V has a fixed ordered basis

$$\mathcal{B} := (v_1, \dots, v_n).$$

Let $q_0 := q^{1/r}$ and let $\mathbb{F}_{q_0}$ denote the subfield of $\mathbb{F}_q$ of index r. Let V_0 be the $\mathbb{F}_{q_0}$-span of $\mathcal{B}$. Then V_0 is a vector space over $\mathbb{F}_{q_0}$ that is contained in V, but V_0 is not an $\mathbb{F}_q$-subspace of V.

Regard the field $\mathbb{F}_q$ as a vector space of dimension r over $\mathbb{F}_{q_0}$, and for any $a \in \{1, \dots, r\}$, define

$$\mathbb{K}(a) := \begin{cases} \mathbb{F}_q & \text{if } a = r, \\ \mathbb{F}_{q_0} & \text{otherwise.} \end{cases} \tag{5.5.1}$$

The significance of $\mathbb{K}(a)$ is given by Lemma 5.5.1.

Lemma 5.5.1. *Let* $\mathbb{F}_{q_0}$ *be a proper nontrivial subfield of* $\mathbb{F}_q$ *with prime index* r*, and let* D *be a nontrivial* $\mathbb{F}_{q_0}$*-subspace of* $\mathbb{F}_q$ *with* $\dim_{\mathbb{F}_{q_0}}(D) = a$*. Then*

$$\{\lambda \in \mathbb{F}_q \mid \lambda D = D\} = \mathbb{K}(a),$$

where $\mathbb{K}(a)$ *is as defined in* (5.5.1)*.*

PROOF. Let $K := \{\lambda \in \mathbb{F}_q \mid \lambda D = D\}$. Clearly, $\mathbb{F}_{q_0} \subseteq K$ since D is a vector space over $\mathbb{F}_{q_0}$. It is easy to see that $K^{\#}$ is a subgroup of the multiplicative group $\mathbb{F}_q^{\#}$. In general, for any distinct $\lambda, \mu \in K$, we have $(\lambda - \mu)D \subseteq \lambda D - \mu D \subseteq D + D = D$, and hence $(\lambda - \mu)D = D$ as D contains no zero divisors. So K is a group under addition in $\mathbb{F}_q$, and thus K is a subfield of $\mathbb{F}_q$. In particular, $\mathbb{F}_{q_0} \leq K \leq \mathbb{F}_q$, and since $\mathbb{F}_{q_0}$ has prime index in $\mathbb{F}_q$, the only possibilities for K are $\mathbb{F}_{q_0}$ and $\mathbb{F}_q$. We get $K = \mathbb{F}_q$ if and only if $\mathbb{F}_q \subseteq D$, that is, $D = \mathbb{F}_q$, in which case $a = r$. Therefore $K = \mathbb{K}(a)$, as asserted. □

For $a \in \{1, \dots, r\}$ define

$$\eta(a) := \frac{\begin{bmatrix} r \\ a \end{bmatrix}_{q_0}}{\left|\mathbb{F}_q^{\#} : \mathbb{K}(a)^{\#}\right|}, \tag{5.5.2}$$

where

$$\begin{bmatrix} r \\ a \end{bmatrix}_{q_0} := \prod_{i=0}^{a-1} \frac{q_0^r - q_0^i}{q_0^a - q_0^i},$$

the number of a-dimensional subspaces of $\mathbb{F}_{q_0}^r$. Lemma 5.5.2 gives some elementary observations about η, whose significance will be apparent in Corollary 5.5.6.

Lemma 5.5.2. *Let $a \in \{1, \dots, r\}$ and let $\mathcal{D}$ denote the set of $\mathbb{F}_{q_0}$-subspaces of $\mathbb{F}_q$ with dimension a. Let $\mathbb{K}(a)$ and $\eta(a)$ be as in* (5.5.1) *and* (5.5.2)*, respectively. Then for $D \in \mathcal{D}$, the sets $[D] = \{\lambda D \mid \lambda \in \mathbb{F}_q^\#\}$ partition $\mathcal{D}$. Moreover, $|[D]| = |\mathbb{F}_q^\# : \mathbb{K}(a)^\#|$, and the number of distinct parts $[D]$ in $\mathcal{D}$ is $\eta(a)$.*

Proof. It follows immediately from the definition of $[D]$ that $\{[D] \mid D \in \mathcal{D}\}$ is a partition of $\mathcal{D}$. For any $D \in \mathcal{D}$ and $\lambda, \mu \in \mathbb{F}_q^\#$, note that $\lambda D = \mu D$ if and only if $\lambda^{-1}\mu D = D$, and, equivalently, $\lambda^{-1}\mu \in \mathbb{K}(a)$ by Lemma 5.5.1. Therefore $|[D]| = |\mathbb{F}_q^\# : \mathbb{K}(a)^\#|$, thus proving the first assertion. Hence the number of classes $[D]$ in $\mathcal{D}$ is $|\mathcal{D}|/|\mathbb{F}_q^\# : \mathbb{K}(a)^\#|$, which completes the proof since

$$|\mathcal{D}| = \begin{bmatrix} r \\ a \end{bmatrix}_{q_0}.$$

□

To any $v = \sum_{i=1}^n \alpha_i v_i \in V$ we can associate the $\mathbb{F}_{q_0}$-subspace

$$D_v := \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{F}_{q_0}}. \tag{5.5.3}$$

Set

$$c(v) := \dim_{\mathbb{F}_{q_0}}(D_v), \tag{5.5.4}$$

and note that $c(v) \leq r$ (since D_v is an $\mathbb{F}_{q_0}$-subspace of $\mathbb{F}_q$) and $c(v) \leq n$ (since D_v is n-generated). For any $\lambda \in \mathbb{F}_q$ it is clear that $D_{\lambda v} = \lambda D_v$, so $c(\lambda v) = c(v)$. For any $\sigma \in \mathrm{Aut}\,(\mathbb{F}_q)$ we have $D_{v^\sigma} = \langle \alpha_1^\sigma, \dots, \alpha_n^\sigma \rangle_{\mathbb{F}_{q_0}}$; since $\sigma|_{\mathbb{F}_{q_0}} \in \mathrm{Aut}\,(\mathbb{F}_{q_0})$, it follows that $(D_v)^\sigma := \{\delta^\sigma \mid \delta \in D_v\} = D_{v^\sigma}$ and $|D_{v^\sigma}| = |(D_v)^\sigma| = |D_v|$. Hence, in particular, $c(v^\sigma) = c(v)$. As in Lemma 5.5.2, let

$$[D_v] := \{\lambda D_v \mid \lambda \in \mathbb{F}_q^\#\},$$

and observe that $D_u \in [D_{v^\sigma}]$ if and only if $D_u = \lambda D_{v^\sigma} = \left(\lambda^{\sigma^{-1}} D_v\right)^\sigma$ for some $\lambda \in \mathbb{F}_q^\#$. Hence $(D_u)^{\sigma^{-1}} = D_{u^{\sigma^{-1}}} = \lambda^{\sigma^{-1}} D_v$, so that $D_{u^{\sigma^{-1}}} \in [D_v]$. Thus $[D_{v^\sigma}] = [D_v]^\sigma$.

5.5.1. Case $H = \Gamma\mathrm{L}(n, q)$. By Theorem 3.6.2

$$G_0 = (\mathrm{GL}(n, q_0) \circ Z_{q-1}) \rtimes \langle \tau \rangle$$

and $L = \mathrm{GL}(n, q_0) \circ Z_{q-1}$.

The main result in this subsection, which relies on the value of the parameter $c(v)$, is the following:

Proposition 5.5.3. *Let Γ be a graph and $G \leq \mathrm{Aut}\,(\Gamma)$ such that G satisfies Hypothesis* 5.1.2 *with $H = \Gamma\mathrm{L}(n, q)$ and $i = 5$. Then Γ is connected and G-symmetric if and only if $\Gamma \cong \mathrm{Cay}(V, v^{G_0})$ for some $v \in V^\#$. Moreover, if D_v and $c(v)$ are as in* (5.5.3) *and* (5.5.4)*, respectively, then the following hold.*

(1) If $c(v) = r$ or $c(v) = r - 1$ then $\mathrm{diam}(\Gamma) = 2$.

(2) *If* $c(v) = 1$ *then* $\mathrm{diam}(\Gamma) = \min\{n, r\}$. *In particular* $\mathrm{diam}(\Gamma) = 2$ *if and only if* $n = 2$ *or* $r = 2$.

(3) *If* $2 \leq c(v) < \frac{1}{2}\min\{n, r\}$ *then* $\mathrm{diam}(\Gamma) > 2$.

(4) *Let* η *be as defined in* (5.5.2), s *be the largest divisor of* d/n *with* $s \leq \eta(c(v))$, *and*

$$k_1(q_0) := \begin{cases} 18s/17 & \text{if } q_0 = 2; \\ s - 5/4 & \text{if } q_0 > 2. \end{cases}$$

If $3 \leq n < r$ *and* $n/2 \leq c(v) < (r(n-2) + k_1(q_0))/(2n)$, *then* $\mathrm{diam}(\Gamma) > 2$.

The cases not covered by Proposition 5.5.3 are discussed briefly at the end of the section. The proof of Proposition 5.5.3 is given after Lemma 5.5.7, and relies on several intermediate results. We begin by describing the $\mathrm{GL}(n, q_0)$-orbits in terms of the subspaces D_v, which in turn leads to a description of the G_0-orbits in $V^{\#}$.

Lemma 5.5.4. *For any* $v \in V^{\#}$ *let* D_v *and* $c(v)$ *be as in* (5.5.3) *and* (5.5.4), *respectively, and let* $\mathcal{U}$ *denote the set of all* $\mathbb{F}_{q_0}$*-independent* $c(v)$*-tuples in* V_0. *Then for any fixed* $\mathbb{F}_{q_0}$*-basis* $\{\beta_1, \ldots, \beta_{c(v)}\}$ *of* D_v,

$$\begin{aligned} v^{\mathrm{GL}(n,q_0)} &= \left\{ \sum_{i=1}^{c(v)} \beta_i u_i \;\middle|\; (u_1, \ldots, u_{c(v)}) \in \mathcal{U} \right\} \\ &= \left\{ u \in V^{\#} \;\middle|\; D_u = D_v \right\}. \end{aligned}$$

Proof. Suppose that $v = \sum_{i=1}^{n} \alpha_i v_i$. Define

$$U := \left\{ u \in V^{\#} \;\middle|\; D_u = D_v \right\} \tag{5.5.5}$$

and

$$W := \left\{ \sum_{i=1}^{c(v)} \beta_i u_i \;\middle|\; (u_1, \ldots, u_{c(v)}) \in \mathcal{U} \right\}. \tag{5.5.6}$$

Claim 1: $v^{\mathrm{GL}(n,q_0)} \subseteq U$. Let $g \in \mathrm{GL}(n, q_0)$ with matrix $[g_{jk}]$ with respect to $\mathcal{B}$. Then $v^g = \sum_{k=1}^{n} \alpha'_k v_k$, where $\alpha'_k = \sum_{j=1}^{n} \alpha_j g_{jk} \in D_v$ for each k. Hence $D_{v^g} \leq D_v$. Since v and g are arbitrary, we also have $D_v \leq D_{v^g}$. So $D_{v^g} = D_v$, and therefore $v^{\mathrm{GL}(n,q_0)} \subseteq U$.

Claim 2: $U \subseteq W$. Let $u = \sum_{j=1}^{n} \alpha'_j v_j \in X$. Writing $\alpha'_j = \sum_{i=1}^{c(v)} \beta_i \gamma_{ij}$ for each j, where all $\gamma_{ij} \in \mathbb{F}_{q_0}$, we get $u = \sum_{i=1}^{c(v)} \beta_i u_i$, with $u_i = \sum_{j=1}^{n} \gamma_{ij} v_j \in V_0$ for all i. It remains to show that the set $\mathbf{u} := \{u_1, \ldots, u_{c(v)}\}$ is $\mathbb{F}_{q_0}$-independent. Indeed, let $\{u'_1, \ldots, u'_b\}$ be a maximal $\mathbb{F}_{q_0}$-independent subset of $\mathbf{u}$, and extend this to an ordered $\mathbb{F}_{q_0}$-basis $\mathcal{B}' := (u'_1, \ldots, u'_d)$ of V_0. Then $u = \sum_{k=1}^{b} \beta'_k u_k$ for some $\beta'_1, \ldots, \beta'_b \in \mathbb{F}_q$, and if $g \in \mathrm{GL}(n, q_0)$ is the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$, then $u^g = \sum_{k=1}^{b} \beta'_k v_k$. So $D_u = D_{u^g}$ by Claim 1, and thus $b \leq c(v) = \dim_{\mathbb{F}_{q_0}}(D_u) = \dim_{\mathbb{F}_{q_0}}(D_{u^g}) \leq b$. Hence $b = c(v)$ and $\mathbf{u}$ is $\mathbb{F}_{q_0}$-independent. Therefore $U \subseteq W$.

Claim 3: $W \subseteq v^{\mathrm{GL}(n,q_0)}$. It is easy to see that W is contained in one orbit of $\mathrm{GL}(n, q_0)$, and it follows from Claims 1 and 2 that $v \in W$. So $W \subseteq v^{\mathrm{GL}(n,q_0)}$, as claimed.

Thus we have $v^{\mathrm{GL}(n,q_0)} = U = W$ by Claims 1 – 3. □

Proposition 5.5.5. *For any $v \in V^{\#}$ let D_v and $c(v)$ be as in* (5.5.3) *and* (5.5.4), *respectively, and let $\mathcal{U}$ be the set of all $\mathbb{F}_{q_0}$-independent $c(v)$-tuples in V_0. Then for any fixed $\mathbb{F}_{q_0}$-basis $\{\beta_1, \dots, \beta_{c(v)}\}$ of D_v we have*

$$\begin{aligned} v^L &= \left\{ \lambda \sum_{i=1}^{c(v)} \beta_i u_i \;\middle|\; (u_1, \dots, u_{c(v)}) \in \mathcal{U},\, \lambda \in \mathbb{F}_q^{\#} \right\} \\ &= \left\{ u \in V^{\#} \;\middle|\; D_u = \lambda D_v,\, \lambda \in \mathbb{F}_q^{\#} \right\} \end{aligned}$$

and

$$\begin{aligned} v^{G_0} &= \left\{ \lambda \sum_{i=1}^{c(v)} \beta_i^{\sigma} u_i \;\middle|\; (u_1, \dots, u_{c(v)}) \in \mathcal{U},\, \lambda \in \mathbb{F}_q^{\#},\, \sigma \in \langle \tau \rangle \right\} \\ &= \left\{ u \in V^{\#} \;\middle|\; D_u = \lambda (D_v)^{\sigma},\, \lambda \in \mathbb{F}_q^{\#}, \sigma \in \langle \tau \rangle \right\}. \end{aligned}$$

Proof. Let $U' := \{u \in V^{\#} \mid D_u = \lambda D_v$ for some $\lambda \in \mathbb{F}_q^{\#}\}$. It follows from Lemma 5.5.4 that

$$v^L = \bigcup_{\lambda \in \mathbb{F}_q^{\#}} \lambda U \subseteq U',$$

with U as in (5.5.6). For any $w \in U'$ with, say, $D_w = \mu D_v$ for $\mu \in \mathbb{F}_q^{\#}$, it is easy to show that $\mu^{-1} w \in U$. Hence $w \in \mu U \subseteq v^L$, and therefore $v^L = U'$. It follows that

$$v^{G_0} = \bigcup_{\sigma \in \langle \tau \rangle} \{u^{\sigma} \mid u \in v^L\} \subseteq W',$$

where $W' := \{u \in V^{\#} \mid D_u = \lambda (D_v)^{\sigma},\, \lambda \in \mathbb{F}_q^{\#},\, \sigma \in \langle \tau \rangle\}$. For any $w \in W$ with $D_w = \mu (D_v)^{\rho}$ for $\mu \in \mathbb{F}_q^{\#}$ and $\rho \in \langle \tau \rangle$, we have $w \in (v^{\rho})^L \subseteq v^{G_0}$. Therefore $v^{G_0} = W'$, and the rest follows from Lemma 5.5.4. □

Corollary 5.5.6. *Let $v \in V^{\#}$, and let $\mathbb{K}$, η, D_v and $c(v)$ be as defined in* (5.5.1), (5.5.2), (5.5.3) *and* (5.5.4), *respectively.*

(1) For $a \in \{1, \dots, \min\{n, r\}\}$, the number of orbits v^L with $c(v) = a$ is $\eta(a)$.

(2) $\left|v^L\right| = \begin{bmatrix} n \\ c(v) \end{bmatrix}_{q_0} |\mathrm{GL}(c(v), q_0)| \left|\mathbb{F}_q^{\#} : \mathbb{K}(c(v))^{\#}\right|$

(3) $\left|v^{G_0}\right| = s \left|v^L\right|$ for some divisor s of d/n with $s \le \eta(c(v))$.

Proof. It follows from Proposition 5.5.5 that the map $v^L \mapsto [D_v] := \{\lambda D_v \mid \lambda \in \mathbb{F}_q^{\#}\}$ is a one-to-one correspondence between the set of L-orbits and the set of classes $[D]$ of $\mathbb{F}_{q_0}$-subspaces of $\mathbb{F}_q$. Therefore, by Lemma 5.5.2, there are exactly $\eta(a)$ orbits v^L with $c(v) = a$, which proves part (1). Also by Proposition 5.5.5, we have $|v^L| = |\mathcal{U}||[D_v]|$, where $\mathcal{U}$ is the set of $\mathbb{F}_{q_0}$-independent $c(v)$-tuples in V_0. So

$$|\mathcal{U}| = \begin{bmatrix} n \\ c(v) \end{bmatrix}_{q_0} |\mathrm{GL}(c(v), q_0)|,$$

and by Lemma 5.5.2, $|[D_v]| = |\mathbb{F}_q^\# : \mathbb{K}(c(v))^\#|$. This proves part (2). Applying part (5) of Theorem 1.1.2 we get $\left|v^{G_0}\right| = s\left|v^L\right|$ for some s dividing $|G_0 : L| = |\mathrm{Aut}\,(\mathbb{F}_q)\,| = d/n$. Also $s \leq \eta(c(v))$ since $c(v^\sigma) = c(v)$, which proves part (3). □

Lemma 5.5.7. *Let $\Gamma = \mathrm{Cay}(V, v^{G_0})$ for some $v \in V^\#$, and let $c(v)$ be as in* (5.5.4)*. Let $w \in V$.*

(1) If $w \in v^{G_0} + v^{G_0}$ then $c(w) \leq 2c(v)$.
(2) If $D_w < D_v$ then $w \in v^{G_0} + v^{G_0}$.

Proof. Let $\mathcal{U}$ and $\mathcal{W}$ denote the sets of $\mathbb{F}_{q_0}$-independent $c(v)$- and $c(w)$-tuples, respectively, in V.

Suppose first that $w = x + y$ for some $x, y \in v^{G_0}$. Then by Proposition 5.5.5 we can write x and y as $x = \sum_{i=1}^{c(v)} \lambda\beta_i^\rho x_i$ and $y = \sum_{i=1}^{c(v)} \mu\beta_i^\sigma y_i$ for some scalars $\lambda, \mu \in \mathbb{F}_q^\#$, maps $\rho, \sigma \in \mathrm{Aut}\,(\mathbb{F}_q)$, and $c(v)$-tuples $\left(x_1, \ldots, x_{c(v)}\right), \left(y_1, \ldots, y_{c(v)}\right) \in \mathcal{U}$. Hence

$$D_w = D_{x+y} \subseteq \langle \lambda\beta_1^\rho, \ldots, \lambda\beta_{c(v)}^\rho, \mu\beta_1^\sigma, \ldots, \mu\beta_{c(v)}^\sigma \rangle_{\mathbb{F}_{q_0}},$$

and therefore $c(w) = c(x + y) \leq 2c(v)$. This proves part (1).

To prove part (2), observe that Lemma 5.5.4 implies that we can write v and w as $v = \sum_{i=1}^{c(v)} \gamma_i u_i$ and $w = \sum_{i=1}^{c(w)} \delta_i z_i$ for some $\left(u_1, \ldots, u_{c(v)}\right) \in \mathcal{U}$ and $\left(z_1, \ldots, z_{c(w)}\right) \in \mathcal{W}$, and for some fixed $\mathbb{F}_{q_0}$-bases $\{\gamma_i, \ldots, \gamma_{c(v)}\}$ and $\{\delta_1, \ldots, \delta_{c(w)}\}$ of D_v and D_w, respectively. Since $D_w < D_v$ then $c(w) < c(v)$, and we can extend $\{\delta_1, \ldots, \delta_{c(w)}\}$ to an $\mathbb{F}_{q_0}$-basis $\{\delta_1, \ldots, \delta_{c(v)}\}$ of D_v, and $\left(z_1, \ldots, z_{c(w)}\right)$ to $\left(z_1, \ldots, z_{c(v)}\right) \in \mathcal{U}$. Set $x := \sum_{i=1}^{c(v)} \delta_i z_i$ and $y := \sum_{i=1}^{c(v)} \delta_i y_i$, where $y_i := z_{i+1} - z_i$ if $1 \leq i \leq c(w) - 1$, $y_{c(w)} := z_1 - z_{c(w)}$, and $y_i := -z_i$ if $c(w) + 1 \leq i \leq c(v)$. Then $\left(y_1, \ldots, y_{c(v)}\right) \in \mathcal{U}$ and $D_x = D_y = D_v$, so by Lemma 5.5.4 we have $x, y \in v^{\mathrm{GL}(n,q_0)} \subseteq v^{G_0}$. Therefore $x + y \in v^{G_0} + v^{G_0}$. Now $D_w = D_{x+y}$, so applying Lemma 5.5.4 again we get $w \in (x + y)^{\mathrm{GL}(n,q_0)} \subseteq v^{G_0} + v^{G_0}$. Thus (2) holds. □

Proof of Proposition 5.5.3. Suppose that $r - 1 \leq c(v) \leq r$. Observe that $\eta(r - 1) = \eta(r) = 1$, so for either value of $c(v)$ we have $v^L = \{u \in V \mid c(u) = c(v)\}$, which in turn implies that $v^{G_0} = v^L$. If $c(v) = r$ then $D_v = \mathbb{F}_q$, and clearly $D_w < D_v$ for any $w \in V^\# \backslash v^{G_0}$. So $w \in v^{G_0} + v^{G_0}$ by part (2) of Lemma 5.5.7, and thus $V^\# \backslash v^{G_0} \subseteq v^{G_0} + v^{G_0}$. Therefore $\mathrm{diam}(\Gamma) = 2$. Now suppose that $c(v) = r - 1$, and let $w \in V^\# \setminus v^{G_0}$. If $c(w) < r - 1$ then it follows from part (1) of Corollary 5.5.6 that $D_w < \lambda D_v = D_{\lambda v}$ for some $\lambda \in \mathbb{F}_q^\#$. Thus $w \in (\lambda v)^{G_0} + (\lambda v)^{G_0} = v^{G_0} + v^{G_0}$ by Lemma 5.5.4. If $c(w) = r$ let $x := \sum_{i=1}^{r-1} \alpha_i v_i$ and $y := \sum_{i=1}^{r-2} \beta_i v_i + \gamma v_r$, where $\{\alpha_1, \ldots, \alpha_{r-1}\}$ is an $\mathbb{F}_{q_0}$-basis of D_v, $\gamma \in \mathbb{F}_q^\# \setminus D_v$, and

$$\beta_i := \begin{cases} \alpha_{i+1} - \alpha_i & \text{if } 1 \leq i \leq r - 3; \\ \alpha_1 - \alpha_{r-2} & \text{if } i = r - 2. \end{cases}$$

Then $c(x) = c(y) = r - 1$ and $c(x + y) = r$, so $x, y \in v^{G_0}$ and $w \in (x + y)^{G_0} \subseteq v^{G_0} + v^{G_0}$. Therefore $V^\# \setminus v^{G_0} \subseteq v^{G_0} + v^{G_0}$, and again we have $\mathrm{diam}(\Gamma) = 2$. This completes the proof of part (1).

If $c(v) = 1$ then we get the special case $v^L = v^{G_0} = (\mathbb{F}_q V_0)^\#$. Let $\mathrm{dist}_\Gamma(\mathbf{0}_V, w)$ denote the distance in Γ between the vertices $\mathbf{0}_V$ and w; we claim that $\mathrm{dist}_\Gamma(\mathbf{0}_V, w) = c(w)$ for any $w \in V$. Let $\ell(w) := \mathrm{dist}_\Gamma(\mathbf{0}_V, w)$. Then $w \in Y$ by Proposition 5.5.5, where Y is as in (5.5.6), so w can be written as a sum of $c(w)$ elements of $(\mathbb{F}_q V_0)^\#$ and thus $\ell(w) \leq c(w)$. On the other hand $w = \sum_{i=1}^{\ell(w)} \lambda_i u_i$, where $\lambda_i \in \mathbb{F}_q^\#$ and $u_i \in V_0^\#$ for all i. Writing each u_i as $u_i = \sum_{j=1}^n \mu_{i,j} w_j$ where $\mu_{i,j} \in \mathbb{F}_{q_0}$ for all i, j, we get $w = \sum_{j=1}^n \lambda'_j w_j$ where $\lambda'_j = \sum_{j=1}^{\ell(w)} \lambda_i \mu_{i,j}$ for each j. Hence $D_w \leq \langle \lambda_1, \ldots, \lambda_{\ell(w)} \rangle_{\mathbb{F}_{q_0}}$, so that $c(w) \leq \ell(w)$. Therefore $\ell(w) = c(w)$, as claimed. It follows immediately that $\mathrm{diam}(\Gamma) = \min\{n, r\}$, and that $\mathrm{diam}(\Gamma) = 2$ if and only if $n = 2$ or $r = 2$. This proves (2).

Suppose that $\mathrm{diam}(\Gamma) = 2$. Then $c(w) \leq 2c(v)$ for any $w \in V^\#$ by part (1) of Lemma 5.5.7, and in particular $2c(v) \geq \min\{n, r\}$ since there clearly exists $u \in V^\#$ with $c(u) = \min\{n, r\}$. Hence $c(v) \leq \frac{1}{2}\min\{n, r\}$ implies that $\mathrm{diam}(\Gamma) > 2$, and part (3) holds.

Finally, let $a := c(v)$, $S := v^{G_0}$, and $\eta(a)$ as in (5.5.2). By Corollary 5.5.6 we have

$$|S| \leq \begin{bmatrix} n \\ a \end{bmatrix}_{q_0} |\mathrm{GL}(a, q_0)| \left|\mathbb{F}_q^\# : \mathbb{F}_{q_0}^\#\right| s,$$

where s is the largest divisor of d/n with $s \leq \eta(a)$. Hence

$$|S|^2 + 1 < q_0^{2an} \left|\mathbb{F}_q^\# : \mathbb{F}_{q_0}^\#\right|^2 s^2.$$

Observe that $s < q_0^{st}$ for all $s \geq 1$, where $t = \frac{9}{17}$ if $q_0 = 2$, and $t = \frac{1}{2}$ if $q_0 \geq 3$. Also, for $q_0 \geq 3$, we have $q_0 - 1 > q_0^{5/8}$, so that $\left|\mathbb{F}_q^\# : \mathbb{F}_{q_0}^\#\right| < q_0^{r-5/8}$. With these bounds we obtain

$$|S|^2 + 1 < q_0^{2(an+r)+k_1(q_0)},$$

where $k_1(q_0)$ is as defined in (4). It is easy to verify that if $a < (r(n-2) - k_1(q_0))/(2n)$ then $2(an + r) + k_1(q_0) < rn$, so $|S|^2 + 1 < |V|$, and thus $\mathrm{diam}(\Gamma) > 2$ by Lemma 5.1.1. This proves part (4). □

Remark. Some small cases covered by Proposition 5.5.3 are summarised in Table 5.5.1. The cases left unresolved by Proposition 5.5.3 are the following:

(1) $5 \leq r \leq n$, $r/2 \leq c(v) \leq r - 2$;
(2) $2 = n \leq r - 2$, $c(v) = 2$;
(3) $3 \leq n < r$, $\max\{n/2, (r(n-2) - k_1(q_0))/(2n)\} \leq c(v) \leq r - 2$.

Let $a := c(v) < r$, $S = v^{G_0}$, and s as in Proposition 5.5.3 (4). Then $s \geq 1$, $\left|\mathbb{F}_q^\# : \mathbb{F}_{q_0}^\#\right| > q_0^{r-2}$ and

$$\begin{bmatrix} n \\ a \end{bmatrix}_{q_0} |\mathrm{GL}(a, q_0)| > q_0^{2a(n-1)},$$

r	n	$c(v)$	Conclusion about $\Gamma = \mathrm{Cay}(V, v^{G_0})$
2	≥ 2	1	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (2)
		2	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (1)
3	2	1	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (2)
		2	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (1)
3	≥ 3	1	$\mathrm{diam}(\Gamma) = 3$ by Proposition 5.5.3 (2)
		2	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (1)
		3	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (2)
5	2	1	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (2)
5	3	1	$\mathrm{diam}(\Gamma) = 3$ by Proposition 5.5.3 (2)
5	4	1	$\mathrm{diam}(\Gamma) = 4$ by Proposition 5.5.3 (2)
		4	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (1)
5	≥ 5	1	$\mathrm{diam}(\Gamma) = 5$ by Proposition 5.5.3 (2)
		2	$\mathrm{diam}(\Gamma) > 2$ by Proposition 5.5.3 (3)
		4	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (1)
		5	$\mathrm{diam}(\Gamma) = 2$ by Proposition 5.5.3 (1)

TABLE 5.5.1

so

$$\begin{aligned} |G_0|^2 + 1 &\geq \left(\begin{bmatrix} n \\ a \end{bmatrix}_{q_0} |\mathrm{GL}(a, q_0)| \left| \mathbb{F}_q^{\#} : \mathbb{F}_{q_0}^{\#} \right| s \right)^2 + 1 \\ &> q_0^{2a(n-1)+2(r-2)}. \end{aligned}$$

It is easy to show that if condition (1) or (2) holds then $2(a(n-1)+r-2) > rn$, and thus $|G_0|^2 + 1 > |V|$. This, unfortunately, does not lead to any conclusion about $\mathrm{diam}(\Gamma)$.

5.5.2. Case $H = \Gamma\mathrm{Sp}(n, q)$. By Theorem 3.6.3,

$$G_0 = (\mathrm{GSp}(n, q_0) \circ Z_{q-1}) \rtimes \langle \tau \rangle$$

and $L = \mathrm{GSp}(n, q_0) \circ Z_{q-1}$. The main result in this section is parallel to part (4) of Proposition 5.5.3.

Proposition 5.5.8. *Let Γ be a graph and $G \leq \mathrm{Aut}(\Gamma)$ such that G satisfies Hypothesis 5.1.2 with $H = \Gamma\mathrm{Sp}(n, q)$ and $i = 5$. Then Γ is connected and G-symmetric if and only if $\Gamma \cong \mathrm{Cay}(V, v^{G_0})$ for some $v \in V^{\#}$. Moreover, if $s := d/n$ and $c(v)$ is as defined in (5.5.4), and if*

$$t := \begin{cases} 9/17 & \text{if } q_0 = 2, \\ 1/2 & \text{if } q_0 > 2 \end{cases}$$

then the following hold:

(1) If $c(v) < \frac{1}{2}\min\{n, r\}$ then $\mathrm{diam}(\Gamma) > 2$.
(2) If $3 \leq n \leq r$, $c(v) \geq n/2$ and $r > (n^2 + n + 2st)/(n-2)$, then $\mathrm{diam}(\Gamma) > 2$.

PROOF. In view of Lemma 5.1.1 and part (1) of Proposition 5.5.3, we only need to prove statement (2).

Let $S = v^{G_0}$. Observe that for any $\lambda \in \mathbb{F}_q^\#$ and $g \in \mathrm{GSp}(n, q_0)$, we have $\lambda v^g = v^{\lambda g} \in v^{\mathrm{GSp}(n,q_0)}$ if and only if $\lambda I_n \in Z_{q_0-1}$, the subgroup of scalar matrices in $\mathrm{GL}(n, q_0)$. Hence $v^L = \bigcup_{\lambda \in \mathbb{F}_q^\#} \lambda v^{\mathrm{GSp}(n,q_0)}$ can be written as a disjoint union $v^L = \bigcup_{\lambda \in T} \lambda v^{\mathrm{GSp}(n,q_0)}$, where T is a transversal of $\mathbb{F}_{q_0}^\#$ in $\mathbb{F}_q^\#$. Thus $|v^L| \leq |T||\mathrm{GSp}(n, q_0)| = (q_0^r - 1)|\mathrm{Sp}(n, q_0)|$ and $|S| \leq s|v^L|$, where $s = |G_0 : L| = |\mathrm{Aut}\,(\mathbb{F}_q)\,| = d/n$. Using the formula for the order of the symplectic group given in Table 3.3.2, we obtain the bound $|\mathrm{Sp}(n, q_0)| < q_0^{(n^2+n)/2}$. Also, as in the proof of Proposition 5.5.3 (4), we have $s < q_0^{st}$ for any s, where $t = \frac{9}{17}$ if $q_0 = 2$, and $t = \frac{1}{2}$ if $q_0 \geq 3$. Hence

$$|S|^2 + 1 < s^2(q_0^r - 1)^2 q_0^{n^2+n} < q_0^{n^2+n+2r+2st}.$$

If $r > (n^2+n+2st)/(n-2)$ then $rn > n^2+n+2r+2st$, so $|V| > |S|^2+1$ and $\mathrm{diam}(\Gamma) > 2$ by Lemma 5.1.1. Therefore part (2) holds. □

5.6. Class $\mathcal{C}_6$

In this case $\dim(V) = r^t$ where r is a prime different from p, q is the smallest power of p such that $q \equiv 1 \pmod{|Z(R)|}$ for some R in Table 3.6.1, and

$$G_0 = (Z_{q-1} \circ R).T \rtimes \langle \tau \rangle,$$

with T as in Table 3.6.1. By Theorems 3.6.2 and 3.6.3, if $H = \Gamma\mathrm{L}(n, q)$ then R is of type 1 or 2, and if $H = \Gamma\mathrm{Sp}(n, q)$ with q odd then R is of type 4.

Proposition 5.6.1. *Let V and G_0 be as above, and let $\Gamma := \mathrm{Cay}(V, S)$ for some G_0-orbit $S \subseteq V^\#$.*

(1) Suppose that r is odd, $q \equiv 1 \pmod r$, and R is of type 1. If $\mathrm{diam}(\Gamma) = 2$ then either $r^t = 3$, or $1 \leq t \leq 3$, $r \leq r_0(t)$, and $q < q_0(r, t)$, where $r_0(t)$ and $q_0(r, t)$ are given in Table 5.6.1.

(2) Suppose that $r = 2$, $t \geq 2$, $q \equiv 1 \pmod 4$, and R is of type 2. If $\mathrm{diam}(\Gamma) = 2$ then $2 \leq t \leq 6$ and $q < q_0(t)$, where $q_0(t)$ is given in Table 5.6.2.

(3) Suppose that $r = 2$, $t \geq 2$, q is odd, and R is of type 4. If $\mathrm{diam}(\Gamma) = 2$ then $2 \leq t \leq 7$ and $q < q_0(t)$, where $q_0(t)$ is given in Table 5.6.3.

(4) Suppose that $r = 2$, $t = 1$, q is odd, and R is of type 2 or 4. Then $\mathrm{diam}(\Gamma) = 2$ for any S.

Proof. If $q = p^\ell$ and R is of type 1 or 2, then $|G_0| = \ell(q-1)r^{2t}|\mathrm{Sp}(2t, r)|$. Recall from Section 3.3 that $|\mathrm{Sp}(2t, r)| = r^{t^2} \prod_{i=1}^t (r^{2i} - 1)$, so that

$$|G_0|^2 + 1 < \ell^2(q-1)^2 r^{2t^2+4t} \prod_{i=1}^t r^{4i} = \ell^2(q-1)^2 r^{4t^2+6t}.$$

Suppose first that r is odd and R is of type 1. We have $q \equiv 1 \pmod r$, so $q \geq 4$. Note that $\ell \leq p^{9\ell/17}$ for all $\ell \geq 1$ if $p \geq 3$, and for all $\ell \geq 2$ if $p = 2$, so $\ell \leq q^{9/17}$ for all $q \geq 4$.

t	1	2	3
$r_0(t)$	27	7	4
$q_0(3,t)$	-	170	12
$q_0(5,t)$	3823	8	-
$q_0(7,t)$	138	-	-
$q_0(11,t)$	21	-	-
$q_0(13,t)$	13	-	-
$q_0(17,t)$	8	-	-
$q_0(19,t)$	7	-	-
$q_0(23,t)$	5	-	-

TABLE 5.6.1. Bounds for r and q when R is Type 1

t	2	3	4	5	6
$q_0(t)$	32767	645	86	22	8

TABLE 5.6.2. Bounds for q when R is Type 2 and $t \geq 2$

t	2	3	4	5	6	7
$q_0(t)$	1919	149	38	13	6	4

TABLE 5.6.3. Bounds for q when R is Type 4 and $t \geq 2$

We then have

$$|G_0|^2 + 1 < q^{18/17} q^2 r^{4t^2+6t} = q^{52/17} r^{4t^2+6t}.$$

Fix q and let $\phi(r,t) := \ln(q^{52/17 r^{4t^2+6t}}) - \ln(q^{r^t})$. Using elementary calculus we can show that $\phi(r,t) < 0$ for all $r \geq 3$ whenever $t \geq 4$, whereas for each $t \in \{1,2,3\}$ there exists some $r_0(t)$ such that $\phi(r,t) < 0$ for all $r \geq r_0(t)$. The values of $r_0(t)$ are given in Table 5.6.1. Clearly, $\phi(r,t) < 0$ implies that $|G_0|^2 + 1 < |V|$, and consequently (by Lemma 5.1.1), $\mathrm{diam}(\Gamma) > 2$ for all Cayley graphs Γ arising from the G_0-orbits. So if $\mathrm{diam}(\Gamma) = 2$ for some Γ then it must be that $1 \leq t \leq 3$ and $r < r_0(t)$.

Now fix $t \in \{1,2,3\}$ and $r < r_0(t)$, and define $\pi(q) := \ln \mu^2 - \ln(|V| - 1)$, where $\mu := q^{9/17}(q-1)|\mathrm{Sp}(2t,r)|$. Note that π is a decreasing function of q and $\mu > |G_0|$. If $r^t = 3$ (i.e., $(r,t) = (3,1)$) then $\pi(q) > 0$ for all $q \geq 4$, which gives no information on the diameter of the Cayley graphs that arise. If $r^t > 3$ then for each pair (r,t) there is a value $q_0(r,t)$ such that $\pi(q) < 0$ for all $q \geq q_0(r,t)$; the values $q_0(r,t)$ are again in Table 5.6.1. Since $\pi(q) < 0$ again implies that $|G_0|^2 + 1 < |V|$, it follows that if $\mathrm{diam}(\Gamma) = 2$ for some Γ then $1 \leq t \leq 3$, $r < r_0(t)$, and $q < q_0(r,t)$. This proves part (1).

To prove (2), suppose that $r = 2$, $t \geq 2$, and R is of type 2. In this case $q \equiv 1 \pmod 4$ so $q \geq 5$ and $\ell \leq 2$. Hence $q^{1/2} > 2$ and $4(q-1) < q^{3/2}$ for all such q. We have

$|G_0| \leq (q-1)2^{2t+1}|\mathrm{Sp}(2t,r)|$, so

$$|G_0|^2 + 1 < (q-1)^2 2^{4t^2+6t+2} = 16(q-1)^2 2^{4t^2+6t-2} < q^{2t^2+3t+2}.$$

Define $\rho(t) := 2t^2 + 3t + 2 - 2^t$. Again, using elementary calculus, we can show that $\rho(t) < 0$ for all $t \geq 7$. So for these cases $|G_0|^2 + 1 < |V|$, and by Lemma 5.1.1 $\mathrm{diam}(\Gamma) > 2$ for all possible Γ. Fix $t \in \{2, \ldots, 6\}$ and let $\sigma(q) := \ln \nu^2 - \ln(|V| - 1)$, where $\nu := (q-1)2^{2t+1}|\mathrm{Sp}(2t,2)|$. Note that $\nu > |G_0|$. It can be shown that σ is a decreasing function of q, and that for each t there is a value $q_0(t)$, given in Table 5.6.2, such that $\sigma(q) < 0$ for all $q \geq q_0(t)$. Hence, for these t and q, we again get $|G_0|^2 + 1 < |V|$ so that $\mathrm{diam}(\Gamma) > 2$ for all Γ. Therefore if $\mathrm{diam}(\Gamma) = 2$ for some Γ we must have $2 \leq t \leq 6$ and $q < q_0(t)$. Thus part (2) holds.

For (3), suppose that $r = 2$, $t \geq 2$, and R is of type 4. Then q is odd, and since $|Z(R)| = 2$ then $\ell = 1$. We have $|G_0| \leq (q-1)2^{2t}|\mathrm{O}^-(2t,2)|$, where $|\mathrm{O}^-(2t,2)| = 2^{t(t-1)+1}(2^t+1)\prod_{i=1}^{t-1}(2^{2i}-1)$. Hence

$$|G_0|^2 + 1 < (q-1)^2 2^{4t} 2^{4t^2-2t+4} = 16(q-1)^2 2^{4t^2+2t}.$$

Since $q \geq 3$ we have $4(q-1) < q^2$ and $q^{2/3} > 2$, so

$$|G_0|^2 + 1 < q^{\frac{2}{3}(4t^2+2t+3)}.$$

Set $\rho(t) := \frac{2}{3}(4t^2 + 2t + 3) - 2^t$. As in the previous cases we can show that $\rho(t) < 0$ for all $t \geq 8$, so $|G_0|^2 + 1 < |V|$, and $\mathrm{diam}(\Gamma) > 2$ for all possible Γ, whenever $t \geq 8$. Fix $t \in \{2, \ldots, 7\}$ and define $\sigma(q) := \ln \nu^2 - \ln(|V| - 1)$, where $\nu := (q-1)2^{2t}|\mathrm{O}^-(2t,2)|$. Then $\nu > |G_0|$. For all t the function $\sigma(q)$ is decreasing, and for each t there is a value $q_0(t)$, given in Table 5.6.3, such that $\sigma(q) < 0$ for all $q \geq q_0(t)$. Hence for each t we have $\mathrm{diam}(\Gamma) > 2$ whenever $q \geq q_0(t)$. That is, if $\mathrm{diam}(\Gamma) = 2$ for some Γ then $2 \leq t \leq 7$ and $q < q_0(t)$. This proves part (3).

Finally, define the matrices $a, b, c \in \mathrm{GL}(V)$ by

$$a := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; b := \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \text{ and } c := \begin{pmatrix} \beta & \delta \\ \delta & -\beta \end{pmatrix},$$

where $\alpha, \beta, \gamma \in \mathbb{F}_q$ such that $\alpha^2 = -1$ and $\beta^2 + \gamma^2 = -1$. Then a representation of R in $\mathrm{GL}(2,q)$ is $\langle a, b, c \rangle$ if R is type 2, and $\langle a, c \rangle$ if R is type 4 (see [**31**, pp. 153-154]). Since R is irreducible on V in both cases, any R-orbit v^R in $V^\#$ contains a basis $\{v_1, v_2\}$ of V, and v^{G_0} contains $\langle v_1 \rangle^\# \cup \langle v_2 \rangle^\#$. Clearly $V^\# \subseteq \langle v_1 \rangle^\# + \langle v_2 \rangle^\#$. Therefore $V \subseteq v^{G_0} + v^{G_0}$, and thus $\mathrm{diam}(\Gamma) = 2$. This proves (4), and completes the proof of the proposition. □

5.7. Class $\mathcal{C}_7$

In this case $V = \otimes_{i=1}^t U_i$ with $U_i = \mathbb{F}_q^m$ for all i, $m \geq 2$, $t \geq 2$, and $d = m^t$. Assume that $\mathcal{B}$ is a tensor product basis of V (see Section 3.1), with

$$\mathcal{B} := \left\{ \otimes_{i=1}^t u_{i,j} \,\middle|\, 1 \leq j \leq m \right\}.$$

As in Section 5.4, it is not difficult to show that for any $v = \sum_{i=1}^{r}\left(\otimes_{j=1}^{t} v_{i,j}\right) \in V^{\#}$ we have

$$v^{\tau} = \sum_{i=1}^{r}\left(\otimes_{j=1}^{t} v_{i,j}^{\tau}\right),$$

where τ acts on each U_i with respect to the basis $\{u_{i,j} \mid 1 \leq j \leq m\}$.

Recall from Section 3.1 that the tensor weight $\mathrm{wt}\,(v)$ of $v \in V^{\#}$, in the decomposition $V = \otimes_{i=1}^{t} U_i$, is the least s such that v is the sum of s simple vectors in $\otimes_{i=1}^{t} U_i$.

Lemma 5.7.1. *For any $v \in V^{\#}$, $g \in \otimes_{i=1}^{t}\mathrm{GL}(m,q)$ and $\sigma \in \langle\tau\rangle$, we have $\mathrm{wt}\,(v^g) = \mathrm{wt}\,(v)$ and $\mathrm{wt}\,(v^{\sigma}) = \mathrm{wt}\,(v)$.*

Proof. Let $v = \sum_{i=1}^{\mathrm{wt}(v)}\left(\otimes_{j=1}^{t} v_{i,j}\right)$. It follows from the above that

$$v^{\sigma} = \sum_{i=1}^{\mathrm{wt}(v)}\left(\otimes_{j=1}^{t} v_{i,j}^{\sigma}\right)$$

for any $\sigma \in \langle\tau\rangle$, so $\mathrm{wt}\,(v^{\sigma}) \leq \mathrm{wt}\,(v)$. Since also $\mathrm{wt}\left(v^{\sigma^{-1}}\right) \leq \mathrm{wt}\,(v)$, we then have $\mathrm{wt}\,(v^{\sigma}) = \mathrm{wt}\,(v)$. The proof that $\mathrm{wt}\,(v^g) = \mathrm{wt}\,(v)$ is similar. □

5.7.1. Case $H = \Gamma\mathrm{L}(n,q)$. By Theorem 3.6.2

$$G_0 = (\mathrm{GL}(m,q) \wr_{\otimes} \mathrm{Sym}\,(t)) \rtimes \langle\tau\rangle. \tag{5.7.1}$$

If $t = 2$ then the results in Section 5.4 hold, with $m = n$, and we obtain the examples in Proposition 5.4.3.

Corollary 5.7.2. *Let $V = \otimes_{i=1}^{t}\mathbb{F}_q^m$ and let G_0 be as in (5.7.1) with $m \geq 2$ and $t = 2$. Then the G_0-orbits in $V^{\#}$ are the sets Y_s for each $s \in \{1, \ldots, m\}$, where Y_s is defined as in Lemma (5.4.2). Moreover, for any G_0-orbit $S \subseteq V^{\#}$, the graph $\mathrm{Cay}(V,S)$ has diameter 2 if and only if $S = Y_s$ for some $s \geq m/2$.*

Proof. This follows immediately from Lemma 5.4.2 and Proposition 5.4.3. □

If $t \geq 3$ it is not easy to describe the G_0-orbits in $V^{\#}$. We do know, from Lemma 5.7.1, that for any $v \in V^{\#}$, v^{G_0} consists of vectors having the same tensor weight as v. This in itself is not very helpful, since describing the G_0-orbits involves determining the weight of an arbitrary vector, which is not easy in general. Clearly, if $\mathrm{Cay}(V,S)$ has diameter 2, then S must consist of vectors whose weight is at least $\frac{1}{2}\omega$, where ω is the maximum weight that occurs in V. The exact value of ω is difficult to determine; all we have so far are the results in Section 3.1 (see Lemmas 3.1.6 and 3.1.7), which show that

$$m \leq \omega \leq m^{t-3}\left(m^2 - \left\lfloor \frac{m}{2} \right\rfloor\right).$$

Using Lemma 5.1.1, we get the following bounds which significantly reduce the cases that have to be considered.

Proposition 5.7.3. *Let Γ be a graph and let $G \leq \mathrm{Aut}(\Gamma)$, such that G satisfies Hypothesis* 5.1.2 *with G_0 as in* (5.7.1), *$m \geq 2$ and $t \geq 3$. Then Γ is connected and G-symmetric if and only if $\Gamma \cong \mathrm{Cay}(V, v^{G_0})$ for some $v \in V^{\#}$. Moreover, if* $\mathrm{diam}(\Gamma) = 2$ *then either:*

(1) $m = 2$ and $t \in \{3, 4, 5\}$; or

(2) $t = 3$ and $m \in \{3, 4, 5\}$.

Proof. Since $(\alpha g_1)\otimes g_2 \otimes \cdots \otimes g_t = g_1 \otimes \cdots \otimes (\alpha g_i) \otimes \cdots \otimes g_t$ for all $g_1, \ldots, g_t \in \mathrm{GL}(m, q)$ and $i \in \{1, \ldots, t\}$, it follows that

$$|G_0| \leq |\mathrm{GL}(m, q)|^t t! \ell/(q-1)^{t-1}$$

where $q = p^\ell$. Noting that $t < q^t$ for all $q \geq 2$ and $t \geq 3$, and $\ell < q^{1/2}$ for $q \geq 3$ ($\ell = 1$ if $q = 2$), we get $|G_0| \leq q^{m^2 t + (t^2 + f(t))/2}$, where

$$f(t) := \begin{cases} 1 & \text{if } q = 2; \\ t+2 & \text{otherwise.} \end{cases}$$

Hence

$$|G_0|^2 + 1 < q^{2m^2 t + t^2 + f(t) + 1}.$$

Let $\phi(m, t) := 2m^2 t + t^2 + f(t) + 1 - m^t$. Using elementary calculus it can be shown that $\phi(m, t) < 0$ whenever $t \geq 7$ and $m \geq 2$, and whenever $m \geq m_0$ for each value of t given in Table 5.7.1. So for these (m, t) we have $|G_0|^2 + 1 < |V|$, and thus $\mathrm{diam}(\Gamma) > 2$ for all

$\phi(m,t)$	m_0
$\phi(m,3)$	7
$\phi(m,4)$	4
$\phi(m,5)$	3
$\phi(m,6)$	3

Table 5.7.1. Values for m_0

Cayley graphs Γ arising from G_0-orbits in $V^{\#}$. For the remaining (m, t) fix m and t and let $\rho(q) := \ln \mu - \frac{1}{2} \ln (q^{m^t - 1})$, where $\mu = |\mathrm{GL}(m, q)|^t t! q/(q-1)^{t-1}$. Note that $\mu > |G_0|$ and $q^{m^t - 1} < |V| - 1$, so $\rho(q) < 0$ implies that $|G_0|^2 + 1 < |V|$. It can be shown that $\rho(q) < 0$ for $(m, t) \in \{(2, 6), (3, 4), (6, 3)\}$, so again $\mathrm{diam}(\Gamma) > 2$ for all Cayley grpahs Γ arising from the G_0-orbits in $V^{\#}$, for these pairs (m, t). These leaves us with (m, t) where $m = 2$ and $3 \leq t \leq 5$, or $t = 3$ and $3 \leq m \leq 5$. This completes the proof. □

5.7.2. Case $H = \Gamma\mathrm{Sp}(n, q)$. By Theorem 3.6.3, both q and t are odd and

$$G_0 = (\mathrm{GSp}(m, q) \wr_{\otimes} \mathrm{Sym}\,(t)) \rtimes \langle \tau \rangle. \tag{5.7.2}$$

Hence $q, t \geq 3$.

Proposition 5.7.4. *Let* Γ *be a graph and* $G \leq \mathrm{Aut}(\Gamma)$ *such that* G *satisfies Hypothesis* 5.1.2 *with* G_0 *as in* (5.7.2)*,* $m \geq 2$ *and* $t \geq 3$*. Then* Γ *is connected and* G*-symmetric if and only if* $\Gamma \cong \mathrm{Cay}(V, v^{G_0})$ *for some* $v \in V^{\#}$*. Moreover, if* $\mathrm{diam}(\Gamma) = 2$ *then either:*

(1) $m = 2$ *and* $t \in \{3, 4, 5\}$*; or*

(2) $t = 3$ *and* $m = 4$*.*

Proof. Recall that $|\mathrm{GSp}(m, q)| = (q-1)|\mathrm{Sp}(m, q)| < (q-1)q^{m^2+m}/2$. We have $t < q^{t/2}$ for all $q \geq 3$ and $t \geq 3$, which implies that if $q = p^\ell$ then $\ell < q^{1/2}$ for all $q \geq 3$, and $t! < q^{(t-1)(t+2)/4}$. It follows that

$$|G_0| \leq |\mathrm{GSp}(m, q)|^t t!\ell/(q-1)^{t-1} < (q-1)q^{(m^2t+mt+1)/2+(t-1)(t-2)/4}.$$

We then have

$$|G_0|^2 + 1 < q^{t^2/2+(m^2+m-3/2)t+5}.$$

Set $\phi(m, t) := t^2/2 + (m^2 + m - 3/2)t + 5 - m^t$. As in Proposition 5.7.3 we can show, using calculus, that $\phi(m, t) < 0$ whenever $t \geq 6$ and $m \geq 2$. Also, for each $t \in \{3, 4, 5\}$ there exists a value m_0, given in Table 5.7.2, such that $\phi(m, t) < 0$ for all $m \geq m_0$. Thus $|G_0|^2 + 1 < |V|$ (and $\mathrm{diam}(\Gamma) > 2$) for all m and t except possibly if $m = 2$ and $3 \leq t \leq 5$, or $t = 3$ and $m = 4$ (recall that m must be even). This completes the proof. □

$\phi(m,t)$	m_0
$\phi(m,3)$	5
$\phi(m,4)$	3
$\phi(m,5)$	3

Table 5.7.2. Values for m_0

CHAPTER 6

Other quasiprimitive types

In this chapter we consider briefly graphs Γ with vertex-quasiprimitive automorphism group G, where G has nonabelian socle and is maximal in $\mathrm{Sym}\,(V(\Gamma))$ such that G is not 2-transitive. It can be deduced from Theorem 1.3.8 that one of the following holds:

(1) $G = T^d.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(d))$, $d \geq 2$, for some nonabelian simple group T, acting on $V(\Gamma) = T^{d-1}$ with the diagonal action defined in (1.3.3) and (1.3.4);

(2) $G = \mathrm{Sym}\,(\Lambda) \wr \mathrm{Sym}\,(m)$, $|\Lambda| \geq 2$ and $m \geq 2$, acting on $V(\Gamma) = \Lambda^m$ with the product action defined in (1.3.1); or

(3) G is an almost simple group.

Assume throughout that Γ is connected and G-symmetric. Recall from Theorem 2.1.2 that Γ is then an orbital graph for G, and for any $\omega \in V(\Gamma)$, the set $\Gamma(\omega)$ of neighbours of ω is an orbit of G_ω. As usual, we are interested in the diameter 2 graphs. Our goal is to prove Theorems 5 and 6.

6.1. Diagonal type subgroups

If G is a maximal subgroup of diagonal type then $G = T^d.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(d))$ for some $d \geq 2$ and nonabelian simple group T, with the diagonal action (1.3.3) and (1.3.4) on $V(\Gamma) = T^{d-1}$. Fix

$$\omega := (1_T, \ldots, 1_T) \in T^{d-1}.$$

Recall that in the diagonal action the subgroup T^{d-1} acts regularly on itself, so $\Gamma \cong \mathrm{Cay}(T^{d-1}, S)$ by Theorem 2.2.4, where S is an orbit of $G_\omega = \mathrm{Aut}\,(T) \times \mathrm{Sym}\,(d)$ in $T^{d-1} \setminus \{\omega\}$ with $S^{-1} = S$.

6.1.1. The case $d = 2$. If $d = 2$ then $T^{d-1} = T$, and if, say, $S = t^{G_\omega}$, then by the definition of the diagonal action we get $S = t^{\mathrm{Aut}(T)} \cup (t^{-1})^{\mathrm{Aut}(T)}$. Thus $S = S^{-1}$ and is a union of conjugacy classes of T. We get diameter 2 if $S \cup S^2 = T$. Examples exist for those groups T that satisfy Thompson's Conjecture, which we state below.

Thompson's Conjecture. [**5**] *Every finite nonabelian simple group T contains a conjugacy class C such that $C^2 = T$.*

Thompson's conjecture has been verified for the alternating groups by C. Hsü in [**24**], for the sporadic simple groups by J. Neubüser et.al. in [**38**], and for most of the simple groups of Lie type by E. Ellers and N. Gordeev in [**18**]. The remaining open cases are summarised in [**29**]. Most of the proofs involve character-theoretic techniques rather than explicit descriptions of the conjugacy classes C. In the case of the alternating groups, several papers have investigated the problem of identifying the conjugacy classes C whose squares cover the whole group; the results in [**8**] are particularly useful.

R. Guralnick and G. Malle in [**23**] prove a weaker version of Thompson's Conjecture.

Theorem 6.1.1. [**23**, Theorem 1.4] *Let T be a finite nonabelian simple group. There exist conjugacy classes C_1 and C_2 in T such that $C_1C_2 = T^\#$. Moreover, aside from $T = \mathrm{PSL}(2,q)$ with $q = 7$ or $q = 17$, we can assume that each class C_i consists of elements of order prime to* 6.

Thus, if S contains a conjugacy class C that satisfies Thompson's Conjecture, or if S contains two conjugacy classes C_1 and C_2 with $C_1C_2 = T^\#$, then the graph $\mathrm{Cay}(T,S)$ has diameter 2. It remains to determine if there exist diameter 2 graphs $\mathrm{Cay}(T,S)$ apart from these.

Problem 1. Determine other possible S, apart from those that contain conjugacy classes satisfying Thompson's Conjecture or Theorem 6.1.1, for which $\mathrm{Cay}(T,S)$ has diameter 2.

6.1.2. The case $d \geq 3$. Suppose that $d > 2$. If $\mathrm{diam}(\Gamma) = 2$, then by the remarks after Lemma 2.2.5 we have $|T|^{d-1} \leq 1 + |S|^2$. Here $|S| \leq |G_\omega| = |T||\mathrm{Out}\,(T)\,|d!$, so $1 + |S|^2 < |T|^2|\mathrm{Out}\,(T)\,|^2 d^{2d}$. This yields

$$|T|^{d-3} < |\mathrm{Out}\,(T)\,|^2 d^{2d}.$$

The following is known.

Theorem 6.1.2. [**32**] *If T is a nonabelian simple group then*

$$|\mathrm{Out}\,(T)\,| < \log_2 |T|.$$

Substituting this bound into the inequality above yields the following.

Proposition 6.1.3. *Let Γ be a G-symmetric graph, where $G = T^d.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(d))$ for some $d \geq 4$ and nonabelian simple group T, and G is a quasiprimitive group on $V(\Gamma) = T^{d-1}$ of diagonal type. If $\mathrm{diam}(\Gamma) = 2$ then the order of T is bounded above by a function of d; more precisely,*

$$\frac{|T|^{d-3}}{\log_2 |T|} < d^{2d}.$$

PROOF. This follows immediately from the preceding discussion. □

Suppose that $d = 3$. Then $V(\Gamma) = T^2$ and $S = (t_1,t_2)^{G_\omega}$ for some $(t_1,t_2) \in T^2 \setminus \{\omega\}$. Hence $S = \bigcup (s_1,s_2)^{\mathrm{Aut}(T)}$, where (s_1,s_2) varies over the elements of

$$(t_1,t_2)^{\mathrm{Sym}(3)} = \left\{(t_1,t_2),(t_2,t_1),\left(t_1^{-1},t_3\right),\left(t_3,t_1^{-1}\right),\left(t_2^{-1},t_3^{-1}\right),\left(t_3^{-1},t_2^{-1}\right)\right\},$$

with $t_3 := t_1^{-1}t_2$. If $S = S^{-1}$ then $\left(t_1^{-1}, t_2^{-1}\right) = (s_1, s_2)^\sigma$ for some $(s_1, s_2) \in (t_1, t_2)^{\mathrm{Sym}(3)}$ and $\sigma \in \mathrm{Aut}\,(T)$. Proposition 6.1.4 gives a necessary condition for Γ to have diameter 2.

Proposition 6.1.4. *Let Γ be a G-symmetric graph, where $G = T^3.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(3))$ for some nonabelian simple group T, and G is a quasiprimitive group on $V(\Gamma) = T^2$ of diagonal type. If $\mathrm{diam}(\Gamma) = 2$ then $\Gamma \cong \mathrm{Cay}(T^2, S)$ where S is an orbit of $\mathrm{Aut}\,(T) \times \mathrm{Sym}\,(3)$ with $S \subseteq (T^2)^\#$ and $S = S^{-1}$, and S does not contain $(t, 1_T)$, $(1_T, t)$, or (t, t) for any $t \in T$.*

Proof. By Theorems 2.1.1 and 2.2.4, it remains to prove that S does not contain $(t, 1_T)$, $(1_T, t)$ or (t, t) for any $t \in T^\#$. Suppose otherwise. Observe that if S contains an element of one of the three types above, then it must also contain elements of the other two types, so it is enough to consider the case where $S = (t, 1_T)^{\mathrm{Sym}(3)}$ for some $t \in T^\#$. (Indeed, $(t, 1_T)^{G_\omega} = (t, 1_T)^{\mathrm{Aut}(T)} \cup (1_T, t)^{\mathrm{Aut}(T)} \cup \left(t^{-1}, t^{-1}\right)^{\mathrm{Aut}(T)}$.) Let $C := t^{\mathrm{Aut}(T)}$. Then $S = \{(s, 1), (1, s), \left(s^{-1}, s^{-1}\right) \mid s \in C\}$, and thus $S = S^{-1}$ implies that $C = C^{-1}$. Hence, if $(x, y) \in S^2$ with $x, y \notin C \cup \{1_T\}$, then $(x, y) = \left(s_1^{-1}s_2^{-1}, s_1^{-1}s_2^{-1}\right)$ for some $s_1, s_2 \in C$. That is, S^2 does not contain elements (x, y) with $x, y \notin C \cup \{1_T\}$ and $x \neq y$. So $S \cup S^2 \neq T^2$ and $\mathrm{diam}(\Gamma) > 2$, a contradiction. Therefore S cannot contain $(t, 1_T)$, $(1_T, t)$ or (t, t) for any $t \in T$. □

Diameter 2 graphs do exist when $d = 3$, and some examples are given below.

Example 6.1.5. Let $G = T^3.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(3))$ with $T = \mathrm{Alt}\,(5)$. All connected G-symmetric graphs $\mathrm{Cay}(T^2, S)$, which were found using Magma [**1**], are given in Table 6.1.1. The graphs in lines 3, 4 and 6 all contain an element of the form $(t, 1_T)$ in the neighbourhood S of ω, and hence have diameter greater than 2 by Proposition 6.1.4. It is interesting to note that the other graphs with diameter greater than 2 (i.e., those in lines 1, 2, 5, 7, 8 and 9) all correspond to $S = (t_1, t_2)$ where t_1, t_2, and $t_1^{-1}t_2$ are all conjugate under T, while none of the graphs in lines 10 to 16 have this property. □

We can generalise Proposition 6.1.4 as follows.

Proposition 6.1.6. *Let Γ be a G-symmetric graph, where $G = T^d.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(d))$ for some $d \geq 4$ and nonabelian simple group T, and G is a quasiprimitive group on $V(\Gamma) = T^{d-1}$ of diagonal type. If $\mathrm{diam}(\Gamma) = 2$ then $\Gamma \cong \mathrm{Cay}(T^{d-1}, S)$, where S is an orbit of $\mathrm{Aut}\,(T) \times \mathrm{Sym}\,(d)$ satisfying the following: $S \subseteq (T^{d-1})^\#$; $S = S^{-1}$; and for all $\mathrm{Aut}\,(T)$-orbits C in $T^\#$ and $k \leq \frac{1}{2}\min\{d-1,\ |T| - |C| - 1\}$, S does not contain $(t_1, \ldots, t_k, 1_T, \ldots, 1_T)$ where $t_i \in C$ for all i.*

Proof. By Theorems 2.1.1 and 2.2.4, it remains to prove that S does not contain an element of the given form. Suppose otherwise. Since $S = S^{-1}$ it follows that $C = C^{-1}$.

	$S = (t_1, t_2)^{G_\omega}$	valency	diameter 2
1	$((3\,5\,4), (3\,4\,5))$	20	no
2	$((1\,3)(2\,5), (1\,5)(2\,3))$	30	no
3	$((1\,2)(4\,5), 1_T)$	45	no
4	$((1\,5\,3), (1\,5\,3))$	60	no
5	$((1\,3\,5\,2\,4), (1\,4\,2\,5\,3))$	72	no
6	$(1_T, (1\,2\,4\,3\,5))$	72	no
7	$((1\,5\,3\,4\,2), (1\,2\,5\,4\,3))$	120	no
8	$((1\,3\,2), (1\,5\,2))$	120	no
9	$((1\,2)(4\,5), (1\,2)(3\,4))$	180	no
10	$((1\,3)(4\,5), (1\,5\,3\,4\,2))$	360	yes
11	$((1\,5)(2\,3), (1\,2\,3))$	360	yes
12	$((1\,2\,5\,4\,3), (1\,2)(3\,5))$	360	yes
13	$((1\,5\,2), (1\,4\,3))$	360	yes
14	$((1\,4\,3), (1\,3\,2\,5\,4))$	360	yes
15	$((1\,2\,3), (1\,5\,3\,2\,4))$	360	yes
16	$((2\,5\,4), (1\,4)(2\,3))$	720	yes

TABLE 6.1.1. G-symmetric graphs for $G = T^3.(\mathrm{Out}\,(T) \times \mathrm{Sym}\,(3))$, $T = \mathrm{Alt}\,(5)$

Setting $t_i := 1_T$ for all i with $k+1 \le i \le d$, we have

$$S = \left\{ \left(t_{d'}^{-1}t_{1'}, \ldots, t_{d'}^{-1}t_{(d-1)'}\right)^{\sigma} \;\middle|\; \sigma \in \mathrm{Aut}\,(T),\ \pi \in \mathrm{Sym}\,(d),\ i' := i^{\pi^{-1}} \right\}.$$

The elements of S can be divided into two types as follows.

(i) If $1 \le d' \le k$ then

$$\begin{aligned}&\left(t_{d'}^{-1}t_{1'},\ \ldots,\ t_{d'}^{-1}t_{(d-1)'}\right)^{\sigma}\\ &= (t_{d'}^{-1}t_1,\ \ldots, t_{d'}^{-1}t_{d'-1},\ t_{d'}^{-1}t_{d'+1},\ \ldots, t_{d'}^{-1}t_k,\ \underbrace{t_{d'}^{-1}, \ldots, t_{d'}^{-1}}_{d-k})^{\alpha\rho}\end{aligned}$$

for some $\alpha \in \mathrm{Aut}\,(T)$ and $\rho \in \mathrm{Sym}\,(d)$.

(ii) If $k+1 \le d' \le d$ then $t_{d'}^{-1} = 1_T$ and

$$\left(t_{d'}^{-1}t_{1'},\ \ldots,\ t_{d'}^{-1}t_{(d-1)'}\right)^{\sigma} = (t_1, \ldots, t_k, \underbrace{1_T, \ldots, 1_T}_{d-k-1})^{\alpha\rho}$$

for some $\alpha \in \mathrm{Aut}\,(T)$ and $\rho \in \mathrm{Sym}\,(d)$.

Let $\ell := \min\{d-1,\ |T|-|C|-1\}$.

Claim 1: If $\ell = d-1$, then S^2 does not contain an element $(s_1, \ldots, s_{d-1})$, where $s_i \notin C \cup \{1_T\}$ for all i and the components s_i are pairwise distinct. Indeed, if x, y are of type (i) then xy has at least $d-1-2(k-1) = d-2k+1$ components of the form $(t_{d'}^{-1})^{\phi}(t_{d''}^{-1})^{\tau}$, for some $\phi, \tau \in \mathrm{Aut}\,(T)$ and $d', d'' \in \{1, \ldots, k\}$. Since $d-2k+1 \ge d-\ell+1 = 2$, the product xy has at least two identical components — that is, the components of xy are not all pairwise distinct. If x, y are of type (ii) then either all components of xy are in C, or at least one component of xy is 1_T. So xy is not of the desired form. If x is type (i) and y is type (ii) then xy has at least $d-2k$ components equal to $(t_{d'}^{-1})^{\tau}$, for some $\tau \in \mathrm{Aut}\,(T)$

and $d' \in \{1, \dots, k\}$. Since $d - 2k \geq d - \ell = 1$, xy has at least one component in $C \cup \{1_T\}$. This proves Claim 1.

Claim 2: If $\ell = |T| - |C| - 1 < d - 1$, *then* S^2 *does not contain an element* $(s_1, \dots, s_{d-1})$ *such that* $T \setminus (C \cup \{1_T\}) \subseteq \{s_1, \dots, s_{d-1}\}$. Suppose that $xy = (s_1, \dots, s_{d-1})$. If x, y are of type (i) then xy has at least $d - 2k + 1$ identical components (equal to $(t_{d'}^{-1})^\phi (t_{d''}^{-1})^\tau$, for some $\phi, \tau \in \mathrm{Aut}\,(T)$ and $d', d'' \in \{1, \dots, k\}$), where $d - 2k + 1 \geq d - \ell + 1 \geq 2$. So xy has at most $d - (d - \ell + 1) = \ell - 1 = |T \setminus (C \cup \{1_T\})| - 1$ distinct components, and thus $T \setminus (C \cup \{1_T\}) \nsubseteq \{s_1, \dots, s_{d-1}\}$. If x, y are both of type (ii), then at least $d - k - 1$ components are in $C \cup \{1_T\}$, so there can be at most k components in $T \setminus (C \cup \{1_T\})$, where clearly $k < |T \setminus (C \cup \{1_T\})|$. If x is of type (i) and y is of type (ii), then xy has at least $d - 2k \geq d - \ell$ components equal to $(t_{d'}^{-1})^\tau$, for some $\tau \in \mathrm{Aut}\,(T)$ and $d' \in \{1, \dots, k\}$. That is, xy has at least $d - \ell$ components in $C \cup \{1_T\}$. So xy can have at most $\ell - 1 = |T \setminus (C \cup \{1_T\})| - 1$ distinct components from $T \setminus (C \cup \{1_T\})$, and thus $T \setminus (C \cup \{1_T\}) \nsubseteq \{s_1, \dots, s_{d-1}\}$. This proves the claim.

It follows immediately from claims 1 and 2 that $S^2 \cup S \neq T^{d-1}$ for any $d \geq 3$. Therefore $\mathrm{diam}(\Gamma) \neq 2$, a contradiction. Thus S does not contain an element $(t_1, \dots, t_k, 1_T, \dots, 1_T)$ with $t_i \in C$ for all i and $k \leq \ell/2$, as asserted. □

Theorem 5 summarises the preceding results.

Proof of Theorem 5. Part (1) follows from Theorem 2.2.4 and Lemma 2.2.5; part (2) follows from Proposition 6.1.4; and part (3) follows from Propositions 6.1.3 and 6.1.6. □

In general, it is quite difficult to obtain a "workable" sufficient condition for Γ to have diameter 2, and the search for one is a topic for further research.

Problem 2. Find sufficient conditions in order for $\mathrm{Cay}(T^{d-1}, S)$, with $d \geq 3$,to have diameter 2.

6.2. Quasiprimitive wreath products

We now consider graphs Γ with automorphism groups of the form $U \wr \mathrm{Sym}\,(m)$, where U is a quasiprimitive subgroup of $\mathrm{Sym}\,(\Lambda)$ with $m \geq 2$, acting with the product action (1.3.1) on $V(\Gamma) = \Lambda^m$. If U is of type HS, SD, or AS, then under some additional conditions, the group $G = U \wr \mathrm{Sym}\,(m)$ is quasiprimitive of type HC, CD, or PA, respectively. Moreover, $\mathrm{soc}(U) = T^k$ and $\mathrm{soc}(G) = T^{km}$ for some $k \geq 1$ and nonabelian simple group T. Clearly, a maximal intransitive subgroup of this form is $\mathrm{Sym}\,(\Lambda) \wr \mathrm{Sym}\,(m)$ with $|\Lambda| \geq 5$.

Hypothesis 6.2.1. Let $G = U \wr \mathrm{Sym}\,(m)$ and Γ be as above. Let

$$\omega := (\lambda, \dots, \lambda) \in V(\Gamma)$$

for some fixed $\lambda \in \Lambda$, and let $\alpha := (\alpha_1, \ldots, \alpha_m)$ be a fixed vertex in $\Gamma(\omega)$. For each $i \in \{1, \ldots, m\}$ let Δ_i be the orbital graph for U with arc set $(\lambda, \alpha_i)^U = \{(\lambda^u, \alpha_i^u) \mid u \in U\}$.

Example 6.2.2 gives an infinite family of graphs that admit as symmetric, vertex-transitive groups of automorphisms wreath products satisfying Hypothesis 6.2.1.

Example 6.2.2. The *Hamming graph* $H(m,q)$, for some $m \geq 2$ and $q \geq 2$, is the graph with vertex set Λ^m where $\Lambda = \{1, \ldots, q\}$, and edge set consisting of pairs of m-tuples that differ in exactly one component. The distance between vertices β and γ is the number of components in which they differ, which is also called the *Hamming distance* $d_H(\beta, \gamma)$ between β and γ. Hence $H(m,q)$ has diameter m. The full automorphism group of $H(m,q)$ is $\mathrm{Sym}\,(q) \wr \mathrm{Sym}\,(m)$, which is symmetric on $H(m,q)$; this is maximal of product type whenever $q \geq 5$. The graph $H(m,q)$ is isomorphic to the Cartesian product of m copies of the complete graph K_q (see Section 2.3).

For any fixed $\nu \in \{1, \ldots, m\}$, define $H^\nu(m,q)$ to be the graph with the same vertex set as $H(m,q)$, and whose edges are the pairs $\{\beta, \gamma\}$ such that $d_H(\beta,\gamma) = \nu$. The graph $H^\nu(m,q)$ is called the *distance-ν graph* of $H(m,q)$; this is also symmetric with automorphism group $\mathrm{Sym}\,(q) \wr \mathrm{Sym}\,(m)$. Note that $H^1(m,q) = H(m,q)$. □

Lemma 6.2.3. *Assume Hypothesis* 6.2.1 *and let β and γ be distinct vertices of Γ, with $\beta := (\beta_1, \ldots, \beta_m)$ and $\gamma := (\gamma_1, \ldots, \gamma_m)$. Then $\beta \sim_\Gamma \gamma$ if and only if the following conditions hold:*

(i) $d_H(\beta, \gamma) = d_H(\omega, \alpha)$; and

(ii) there exists $\pi \in \mathrm{Sym}\,(m)$ such that $\beta_j \sim_{\Delta_{j'}} \gamma_j$ whenever $\beta_j \neq \gamma_j$ and $j' := j^{\pi^{-1}}$.

Proof. Applying Theorem 2.1.2 and (1.3.1), the vertices β and γ are adjacent if and only if $(\beta, \gamma) \in (\gamma, \alpha)^G$, that is, for some $(u_1, \ldots, u_m) \in U^m$ and $\pi \in \mathrm{Sym}\,(m)$, we have $\beta = (\lambda^{u_{1'}}, \ldots, \lambda^{u_{m'}})$ and $\gamma = \left(\alpha_{1'}^{u_{1'}}, \ldots, \alpha_{m'}^{u_{m'}}\right)$, where $i' := i^{\pi^{-1}}$ for all i. Equivalently, $d_H(\beta, \gamma) = d_H(\omega, \alpha)$ and $\beta_i \sim_{\Delta_{i'}} \gamma_i$ whenever $\beta_i \neq \gamma_i$, as required. □

Example 6.2.4. Assume Hypothesis 6.2.1 with $m = 2$ and $\alpha_1 \neq \lambda = \alpha_2$. Then $d_H(\omega, \alpha) = 1$ and $\Delta_2 = (\lambda, \lambda)^U$ is an empty graph. It follows that two vertices (β_1, β_2) and (γ_1, γ_2) are adjacent in Γ if and only if $\beta_1 = \gamma_1$ and $\beta_2 \sim_{\Delta_1} \gamma_2$, or $\beta_1 \sim_{\Delta_1} \gamma_1$ and $\beta_2 = \gamma_2$. Hence Γ is the Cartesian product $\Delta_1 \square \Delta_1$ (see Section 2.3). By Lemma 2.3.2 we get $\mathrm{diam}(\Gamma) = 2$ if and only if Δ_1 is a complete graph, in which case $\Gamma \cong H(2,q)$ with $q = |\Lambda|$. □

An easy necessary condition for Γ satisfying Hypothesis 6.2.1 to have diameter 2 is given below.

Proposition 6.2.5. *Assume Hypothesis* 6.2.1. *If* $\mathrm{diam}(\Gamma) = 2$, *then* $d_H(\omega, \alpha) \geq \frac{1}{2}m$.

PROOF. Suppose that $\mathrm{diam}(\Gamma) = 2$ and that $d_H(\omega, \alpha) < m/2$. Set $\beta := (\beta_0, \ldots, \beta_0)$ and $\gamma := (\gamma_0, \ldots, \gamma_0)$ where $\beta_0 \neq \gamma_0$. Then $d_H(\beta, \gamma) = m$ so that $\beta \nsim_\Gamma \gamma$ by Lemma 6.2.3, and by our assumption there is a vertex $\delta := (\delta_1, \ldots, \delta_m)$ with $\beta \sim_\Gamma \delta \sim_\Gamma \gamma$. Applying Lemma 6.2.3 again we then have $d_H(\beta, \delta) = d_H(\omega, \alpha) = d_H(\delta, \gamma)$. Since $\beta_0 \neq \gamma_0$, we have $d_H(\delta, \gamma) \geq m - d_H(\beta, \delta) = m - d_H(\omega, \alpha) > d_H(\omega, \alpha)$, a contradiction. So if $\mathrm{diam}(\Gamma) = 2$ then $d_H(\omega, \alpha) \geq m/2$. □

Observe that $m - d_H(\omega, \alpha)$ gives the number of U-orbital graphs Δ_i which are empty. The graph Δ_i is a complete graph for some i if and only if U is a 2-transitive subgroup of $\mathrm{Sym}\,(q)$ for $q = |\Lambda|$, and equivalently, for any $j \in \{1, \ldots, m\}$, either Δ_j is empty or Δ_j is complete. In this case, two distinct vertices β and γ are adjacent exactly when $d_H(\beta, \gamma) = d_H(\omega, \alpha)$. Thus Γ is the distance-ν graph $H^\nu(m, q)$ for $\nu := d_H(\omega, \alpha)$.

We are now ready to prove Theorem 6.

PROOF OF THEOREM 6. By the remarks above, Γ is the distance-ν graph $H^\nu(m, q)$ of $H(m, q)$ for some $\nu \in \{1, \ldots, m\}$. If $\mathrm{diam}(\Gamma) = 2$ then $\nu \geq m/2$ by Proposition 6.2.5, so it remains to prove the converse.

Suppose that $\nu \geq m/2$. Since $\mathrm{Sym}\,(\Lambda)$ is clearly 2-transitive it follows that all connected graphs Δ_i are complete, and by Lemma 6.2.3 two distinct vertices of Γ are adjacent if and only if their Hamming distance is ν. Let $\beta' := (\beta_1, \ldots, \beta_m)$ and $\gamma' := (\gamma_1, \ldots, \gamma_m)$ be distinct nonadjacent vertices of Γ. Without loss of generality, assume that $\beta_i \neq \gamma_i$ exactly when $1 \leq i \leq d_H(\beta, \gamma)$. Write $\mu := d_H(\beta, \gamma)$. We have two cases.

Case 1: Suppose that $d_H(\beta, \gamma) < \nu$. Choose $\delta_i \in \Lambda$ satisfying

$$\begin{cases} \delta_i \neq \beta_i, \gamma_i & \text{if } 1 \leq i \leq \nu; \\ \delta_i = \beta_i (= \gamma_i) & \text{if } \nu + 1 \leq i \leq m. \end{cases}$$

Let $\delta := (\delta_1, \ldots, \delta_m)$. Then $d_H(\beta, \delta) = d_H(\gamma, \delta) = \nu$, and therefore $\beta \sim_\Gamma \delta \sim_\Gamma \gamma$. So $\mathrm{dist}_\Gamma(\beta, \gamma) = 2$.

Case 2: Suppose that $d_H(\beta, \gamma) > \nu$. Observe that $\mu \leq m \leq 2\nu$, so that $\nu \geq \lfloor \mu/2 \rfloor$. Hence $\nu + \lfloor \mu/2 \rfloor + 1 \geq 2\lfloor \mu/2 \rfloor + 1 \geq \mu$, and thus $\beta_i = \gamma_i$ for all $i \geq \nu + \lfloor \mu/2 \rfloor + 1$. Choose $\delta_i \in \Lambda$ satisfying

$$\begin{cases} \delta_i = \beta_i (\neq \gamma_i) & \text{if } 1 \leq i \leq \lfloor \mu/2 \rfloor; \\ \delta_i = \gamma_i (\neq \beta_i) & \text{if } \lfloor \mu/2 \rfloor + 1 \leq i \leq 2\lfloor \mu/2 \rfloor; \\ \delta_i \neq \beta_i, \gamma_i & \text{if } 2\lfloor \mu/2 \rfloor + 1 \leq i \leq \nu + \lfloor \mu/2 \rfloor; \\ \delta_i = \beta_i (= \gamma_i) & \text{if } \nu + \lfloor \mu/2 \rfloor + 1 \leq i \leq m. \end{cases}$$

Then $d_H(\beta, \delta) = d_H(\gamma, \delta) = \lfloor \mu/2 \rfloor + \nu - \lfloor \mu/2 \rfloor = \nu$. So again $\beta \sim_\Gamma \delta \sim_\Gamma \gamma$ and $\mathrm{dist}_\Gamma(\beta, \gamma) = 2$. Therefore $\mathrm{diam}(\Gamma) = 2$. □

Remark. Theorem 6 is also true if $G = U \wr \mathrm{Sym}\,(m)$ for any 2-transitive group U. In particular, if $U = \mathrm{AGL}(k, q_0)$ for some $k \geq 2$ and prime power q_0, then G is maximal affine-type subgroup belonging to the Aschbacher class $\mathcal{C}_2$, and we get Proposition 5.3.2.

6.3. Almost simple subgroups

In this case the unique minimal normal subgroup of G is a nonabelian simple group T, which acts transitively on $V(\Gamma)$. A classification of symmetric, diameter 2 graphs admitting a maximal almost simple, vertex-quasiprimitive group of automorphisms — which would necessarily depend on the classification of quasiprimitive almost simple groups — is infeasible at this point. Examples are known to exist: for instance, orbital graphs for the almost simple quasiprimitive rank 3 graphs of even order (which are all known, see Section 1.4) are symmetric and diameter 2, and thus fall under this case.

There are many other examples with arbitrarily large rank, some of which we give below.

Example 6.3.1. Let $k \geq 2$ and $n \geq 2k+1$, and let Ω be the set of k-element subsets of $\{1, \ldots, n\}$. The *Kneser graph* $KG(n,k)$ is the graph with vertex set Ω and in which two vertices are adjacent if and only if they are disjoint. In [**42**] it is proved that $KG(n,k)$ has diameter

$$\left\lceil \frac{k-1}{n-2k} \right\rceil + 1.$$

In particular, $KG(n,k)$ has diameter 2 if and only if $n \geq 3k-1$. The full automorphism group of $KG(n,k)$ is $\mathrm{Sym}\,(n)$, which acts on Ω via

$$\alpha^g := \{x^g \mid x \in \alpha\} \quad \forall\, \alpha \in \Omega,\ g \in \mathrm{Sym}\,(n)\,.$$

Then $\mathrm{Sym}\,(n)$ is arc-transitive on $KG(n,k)$. The stabiliser of a point is isomorphic to $\mathrm{Sym}\,(k) \times \mathrm{Sym}\,(n-k)$, which is maximal in $\mathrm{Sym}\,(n)$, and hence the action of $\mathrm{Sym}\,(n)$ is primitive (and thus quasiprimitive) by Theorem 1.2.1. Furthermore, $\mathrm{Sym}\,(n)$ has rank $k+1$ in this action: indeed, for a fixed $\omega \in \Omega$, the G_ω-orbits in $\Omega \setminus \{\omega\}$ are the sets $\{\alpha \in \Omega \mid |\alpha \cap \omega| = \ell\}$ for each $\ell \in \{0, \ldots, k\}$. □

Although the quasiprimitive case is too difficult to handle, restricting to the primitive case might be reasonable, albeit the possibility of a classification also remains to be determined.

Problem 3. Classify the symmetric diameter 2 graphs with vertex-primitive automorphism groups that are maximal of almost simple type.

APPENDIX A

Magma codes

We present here some of the MAGMA algorithms used for computing the entries in Table 4.1.2, and for obtaining the results described in Examples 4.5.4 and 6.1.5.

A.1. Algorithms for Table 4.2

The algorithm used for computing the entries of Table 4.1.2 is quite straightforward, and consists of the following steps:

Construct the group $G_0 \leq \mathrm{GL}(V)$.
Get the orbits S of G_0 in $V^{\#}$.
Compare $V^{\#}$ and $S \cup (S + S)$.

Isomorphisms of graphs are checked by looking at the action of the normalizer of G_0, or if this doesn't work, by constructing the corresponding graphs and using MAGMA's `IsIsomorphic` function.

A.1.1. Lines 1-10.

```
Q8 := ExtraSpecialGroup(2,1 :  Type:= "-");
n := 0;
H := []; HH := [];
for p in [5,7,11,23] do
print "p", "=", p;
U := VectorSpace(GF(p),2); V := DirectSum(U,U);
k := Subgroups(GL(U) : OrderEqual:=8);
c := {@ j :  j in [1..#k] | IsIsomorphic(k[j]`subgroup,Q8) @};
K := k[c[1]]`subgroup;
N := Normalizer(GL(U),K);
h := Subgroups(N);
I := {@ i :  i in [1..#h] | IsTransitive(OrbitImage(h[i]`subgroup,
(Set(U) diff U!0))) @};
O := [];
for i in [1+n..#I+n] do
   H[i] := h[I[i-n]]`subgroup;
   HH[i] := sub< GL(V) | { DirectSum(h,h) :  h in H[i] } >;
   O[i] := Orbit(HH[i],V![1,0,1,1]);
   if #( { x+y :  x,y in O[i] } join Set(O[i]) ) eq #V then
      print "H",i, "order", #H[i], ":", #GL(U)/#O[i], "graphs with diameter 2";
      elif sub< V | O[i] > eq V then
```

```
      print "H",i, "order", #H[i], ":", #GL(U)/#O[i], "connected graphs with
      diameter greater than two";
      else print "H",i, "order", #H[i], ":", "no connected graphs";
   end if;
end for;
n := n + #I;
end for;
```

A.1.2. Lines 11-17. To obtain the entries for lines 11-17 of Table 4.1.2, the same code as above was used, apart the first eight lines which are replaced with:

```
for p in [11,19,29,59] do
print "p", "=", p;
U := VectorSpace(GF(p),2); V := DirectSum(U,U);
k := Subgroups(GL(U) : OrderEqual:=120);
c := {@ j :  j in [1..#k] | IsIsomorphic(k[j]`subgroup,SL(2,5)) @};
```

A.1.3. Lines 18-49. The code below computes the entries for lines 18-33; the code for lines 34-49 is similar.

```
U := VectorSpace(GF(3),4); V := DirectSum(U,U);
X := SemiLinearGroup(GL(2,9),GF(3));
y := Subgroups(X : OrderEqual:=#GL(2,9));
i := {@ j :  j in [1..#y] | IsIsomorphic(y[j]`subgroup,GL(2,9)) @};
Y := y[i[1]]`subgroup;
k := Subgroups(X : OrderEqual:=120);
i := {@ j :  j in [1..#k] | IsIsomorphic(k[j]`subgroup,SL(2,5)) @};
K := k[i[1]]`subgroup;
N := Normalizer(X,K); #N;
h := Subgroups(N : OrderMultipleOf:=(#U-1));
I := {@ i :  i in [1..#h] | IsTransitive(OrbitImage(h[i]`subgroup,
(Set(U) diff {U!0}))) @};
A := [];
for i in [1..#I] do
   A[i] := h[I[i]]`subgroup;
end for;
AA := []; MA := [];
for i in [1..#A] do
AA[i] := sub< GL(V) | { DirectSum(h,h) :  h in A[i] } >;
MA[i] := Normalizer(GL(V),AA[i]);
end for;
for i in [1..#A] do
   print "A",i, "order", #A[i];
   S[i] := []; s[i] := [];
   o := {@ j :  j in [1..#Orbits(MA[i])] | #Orbits(MA[i])[j] gt 1 @};
```

```
  for j in [1..#o] do
    s[i][j] := {@ k : k in [1..#Orbits(AA[i])] | Orbits(AA[i])[k] subset
    Orbits(MA[i])[o[j]] @};
    S[i][j] := Set(Orbits(AA[i])[s[i][j][1]]);
    SS := { x+y : x,y in S[i][j] };
    if (SS join S[i][j]) eq Set(V) then
      print "S", i,j, ":", #s[i][j], "of length", #S[i][j], ";",
      "diameter 2", ";", "|S+S| =", #SS;
      elif sub< V | S[i][j] > eq V then
      print "S", i,j, ":", #s[i][j], "of length", #S[i][j], ";", "connected
      with diameter > 2", ";", "|S+S| =", #SS;
      else print "S", i,j, ":", #s[i][j], "of length", #S[i][j], ";",
      "disconnected";
    end if;
  end for;
end for;
for i in [2..#A] do
  for j in [2..#Orbits(MA[i])-1] do
    for k in [1..(i-1)] do
      for l in [2..#Orbits(MA[k])-1] do
        r := #{ m : m in s[k][l] | Orbits(AA[k])[m] subset S[i][j] };
        if r ge 1 then
          print "S",i,j, ":", r, x, "S",k,l;
        end if;
      end for;
    end for;
  end for;
end for;
```

A.1.4. Lines 53-72.

```
U := VectorSpace(GF(3),6); V := DirectSum(U,U);
h := Subgroups(GL(U) : OrderEqual:=#SL(2,13));
i := {@ j : j in [1..#h] | IsIsomorphic(h[j]`subgroup,SL(2,13)) @};
H := h[i[1]]`subgroup;
HH := sub< GL(V) | { DirectSum(h,h) : h in H } >;
M := sub< GL(V) | { KroneckerProduct(g,h) : g in GL(2,3), h in H } >;
O := Orbits(HH);
A := {@ #{ x+y : x,y in O[i] } : i in [1..#O] @};
B := []; X := [];
for j in [1..#A] do   B[j] := { o : o in O | #{ x+y : x,y in o } eq A[j] };
  X[j] := OrbitImage(M,B[j]);
  print j, ":", #B[j], "orbits,", "at most", #Orbits(X[j]), "class(es) with
  valency", { #o : o in B[j] }, ";", "|S+S| =", A[j];
```

```
end for;
```

A.2. Algorithms for Example 4.5.4

```
F<w> := GF(3^4);
U := VectorSpace(GF(3),4); V := DirectSum(U,U);
X := SemiLinearGroup(GL(1,F),GF(3));
s := {@ g : g in G | (U!Eltseq(F!1))*g eq U!Eltseq(w) and
(U!Eltseq(w))*g eq U!Eltseq(w^2) @}[1];
t := {@ g : g in G | (U!Eltseq(F!1))*g eq U!Eltseq(F!1) and
(U!Eltseq(w))*g eq U!Eltseq(w^3) @}[1];
H := sub< GL(U) | s^2, t*s >;
HH := sub< GL(8,3) | { DirectSum(h,h) : h in H } >; O := Orbits(HH);
for i in [1..#O] do
  print i, ":", < { Seqelt([u[i] : i in [1..4]],F) : u in U | V!
  Insert([(U!Eltseq(F!1))[i] : i in [1..4]],5,4,[u[i] : i in [1..4]]) in
  O[i] }, #O[i], #{ x+y : x,y in O[i] } >;
  if #(O[i] join { x+y : x,y in O[i] }) eq #V then
    print "diameter two";
    else print "not diameter two";
  end if;
end for;
```

A.3. Algorithms for Example 6.1.5

```
n := 5; T := Alt(n); d := 3;
N := CartesianProduct([T : i in [1..d]]);
diagN := { a : a in N | forall{ i : i in [1..d-1] | a[i] eq a[d] } };
V := { a : a in N | a[d] eq Id(T) };
G1 := CartesianProduct(Sym(n),Sym(d));
f := map< CartesianProduct(V,G1) -> V | c :-> < (Inverse(c[1][d^c[2][2]])*
c[1][j^c[2][2]])^c[2][1] : j in [1..d] > >;
s := []; O := [];
s[1] := N!< Id(T) : i in [1..d] >;
O[1] := f(Set(CartesianProduct({s[1]},G1)));
S := O[1]; j := 1;
for i in [1..#V] do
  if exists(t){ u : u in Set(V) diff S } then
    j := 1+j;
    s[j] := t;
    O[j] := f(Set(CartesianProduct({s[j]},G1)));
    S := S join O[j];
  end if;
end for;
```

```
H := CartesianProduct(N,Sym(d));
g := map< CartesianProduct(V,H) -> V | c :-> <
Inverse(c[2][1][d^c[2][2]])*Inverse(c[1][d^c[2][2]])*
c[1][j^c[2][2]]*c[2][1][j^c[2][2]] :  j in [1..d] > >;
W := { < v[1],v[2] > :  v in V };
R := []; S := []; SS := [];
for i in [2..#O] do
   t1 := s[i][1]; t2 := s[i][2]; t3 := Inverse(t1)*t2;
   R[i] := {@ < t1, t2 >, < t2, t1 >, < Inverse(t1), Inverse(t1)*t2 >,
   < Inverse(t1)*t2, Inverse(t1) >, < Inverse(t2)*t1, Inverse(t2) >,
   < Inverse(t2), Inverse(t2)*t1 > @};
   print i, ":", s[i], "   ", "valency =", #O[i], ",", "undirected -",
   <Inverse(t1),Inverse(t2)> in S[i], ",", "diameter two -",
   #(W diff (SS[i] join S[i])) eq 0;
end for;
```

Bibliography

[1] MAGMA *Handbook*. `http://magma.maths.usyd.edu.au/magma/handbook/`.

[2] S. B. Akers and B. Krishnamurthy, *A group-theoretic model for symmetric interconnection networks*, IEEE Trans. Comput., 38 (1989), pp. 555–566.

[3] C. Amarra, M. Giudici, and C. E. Praeger, *Quotient-complete arc-transitive graphs*, European J. Combin., (2012). DOI: 10.1016/j.ejc.2012.04.006.

[4] ———, *Symmetric diameter 2 graphs with affine-type vertex-quasiprimitive automorphism group*, Des. Codes Cryptogr., (2012). DOI: 10.1007/s10623-012-9644-z.

[5] Z. Arad and M. Herzog, eds., *Products of Conjugacy Classes in Groups*, no. 1112 in Lecture Notes in Mathematics, Springer-Verlag, 1985.

[6] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math., 76 (1984), pp. 469–514.

[7] E. Bannai, *Maximal subgroups of low rank of finite symmetric and alternating groups*, J. Fac. Sci. Univ. Tokyo, 18 (1972), pp. 475–486.

[8] E. Bertram, *Even permutations as a product of two conjugate cycles*, J. Combinatorial Theory Ser. A, 12 (1972), pp. 368–380.

[9] N. A. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1964.

[10] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc., 13 (1981), pp. 1–22.

[11] L. Campbell, G. E. Carlsson, M. J. Dinneen, V. Faber, M. R. Fellows, M. A. Langston, J. W. Moore, A. P. Mullhaupt, and H. B. Sexton, *Small diameter symmetric networks from linear groups*, IEEE Transactions on Computers, 41 (1992), pp. 218–220.

[12] F. Comellas and M. A. Fiol, *Vertex-symmetric digraphs with small diameter*, Discrete Applied Mathematics, (1995), pp. 1–11.

[13] B. N. Cooperstein, *The geometry of root subgroups in exceptional groups. I*, Geom. Dedicata, (1979), pp. 317–338.

[14] ———, *Maximal subgroups of* $G_2(2^n)$, J. Algebra, (1981), pp. 23–36.

[15] A. Devillers, M. Giudici, C. H. Li, G. Pearce, and C. E. Praeger, *On imprimitive rank 3 permutation groups*, J. London Math. Soc., 84 (2011), pp. 649–669.

[16] M. Dinneen, M. Fellows, and V. Faber, *Algebraic constructions of efficient broadcast networks*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, H. Mattson, T. Mora, and T. Rao, eds., vol. 539 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 1991, pp. 152–158.

[17] J. D. Dixon and B. Mortimer, *Permutation Groups*, no. 163 in Graduate Texts in Mathematics, Springer, 1996.

[18] E. Ellers and N. Gordeev, *On the conjectures of J. Thompson and O. Ore*, Trans. Amer. Math. Soc., 350 (1998), pp. 3657–3671.

[19] M. Giudici, C. H. Li, and C. E. Praeger, *Locally s-arc transitive graphs with two different quasiprimitive actions*, J. Algebra, 299 (2006), pp. 863–890.

[20] M. Giudici, M. W. Liebeck, C. E. Praeger, J. Saxl, and P. H. Tiep, *Arithmetic results on orbits of linear groups.* arXiv:1203.2457v1 [math.GR], 2012.

[21] D. P. Goodwin, *Regular orbits of linear groups with an application to the $k(gv)$-problem, 1*, J. Algebra, 227 (2000), pp. 395–432.

[22] ———, *Regular orbits of linear groups with an application to the $k(gv)$-problem, 2*, J. Algebra, 227 (2000), pp. 433–473.

[23] R. Guralnick and G. Malle, *Products of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc., 25 (2012), pp. 77–121.

[24] C. hao Hsü, *The commutators of the alternating group*, Sci. Sinica, 14 (1965), pp. 339–342.

[25] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order, ii*, J. Algebra, 93 (1985), pp. 151–164.

[26] M.-C. Heydemann, *Cayley graphs and interconnection networks*, in Graph Symmetry: Algebraic Methods and Applications, G. Hahn and G. Sabidussi, eds., vol. 497 of NATO ASI Series C: Mathematical and Physical Sciences, Kluwer Academic Publishers, 1997, pp. 167–226.

[27] T. W. Hungerford, *Algebra*, no. 73 in Graduate Texts in Mathematics, Springer, 1974.

[28] W. M. Kantor and R. A. Liebler, *The rank 3 permutation representations of the finite classical groups*, Trans. Amer. Math. Soc., 271 (1982), pp. 1–71.

[29] L.-C. Kappe and R. F. Morse, *On commutators in groups*, in Groups St. Andrews 2005: Volume 2, C. M. Campbell, M. R. Quick, E. F. Robertson, and G. C. Smith, eds., no. 340 in London Mathematical Society Lecture Note Series, Cambridge University Press, 2005, pp. 531–558.

[30] O. H. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, in Surveys in Combinatorics '05, 2005, pp. 29–56.

[31] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, no. 129 in London Math. Soc. Lecture Note Series, Cambridge University Press, 1990.

[32] S. Kohl, *A bound on the order of the outer automorphism group of a finite simple group of given order.* http://www.gap-system.org/DevelopersPages/StefanKohl/preprints/ctpz.pdf, 2003.

[33] C. H. Li, T. K. Lim, and C. E. Praeger, *Homogeneous factorisations of complete graphs with edge-transitive factors*, J. Algebr. Comb., 29 (2009), pp. 107–132.

[34] M. W. Liebeck, *The affine permutation groups of rank 3*, Proc. London Math. Soc., 3 (1987), pp. 477–516.

[35] M. W. Liebeck and J. Saxl, *The finite permutation groups of rank 3*, Bull. London Math. Soc., 18 (1986), pp. 165–172.

[36] P. Lorimer, *Vertex-transitive graphs: Symmetric graphs of prime valency*, J. Graph Theory, 8 (1984), pp. 55–68.

[37] J. Morris, C. E. Praeger, and P. Spiga, *Strongly regular edge-transitive graphs*, Ars Math. Contemp., 2 (2009), pp. 137–155.

[38] J. Neubüser, H. Pahlings, and E. Cleuvers, *Each sporadic finasig G has a class C such that $CC = G$*, Abstracts AMS, 34 (1984), p. 6.

[39] C. E. Praeger, *An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs*, J. London Math. Soc., 2 (1993), pp. 227–239.

[40] ———, *Finite transitive permutation groups and finite vertex-transitive graphs*, in Graph Symmetry: Algebraic Methods and Applications, G. Hahn and G. Sabidussi, eds., vol. 497 of NATO ASI Series C: Mathematical and Physical Sciences, Kluwer Academic Publishers, 1997, pp. 277–318.

[41] ———, *Finite symmetric graphs*, in Topics in Algebraic Graph Theory, L. W. Beineke and R. J. Wilson, eds., vol. 102 of Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 2004, pp. 179–202.

[42] M. Valencia-Pabon and J.-C. Vera, *On the diameter of Kneser graphs*, Discrete Mathematics, 305 (2005), pp. 383 – 385.

[43] R. A. Wilson, *The Finite Simple Groups : An Introduction*, Springer, 2009.

[44] Z. xian Wan, *Geometry of Classical Groups over Finite Fields*, Studentlitteratur, 1993.

[45] J. Xu, *On closures of finite permutation groups*, PhD thesis, The University of Western Australia, 2005.