J. Aust. Math. Soc. **0** (2016), 1–13

Primitive prime divisors and the *n*-th cyclotomic polynomial

S. P. GLASBY ✉ , FRANK LÜBECK, ALICE C. NIEMEYER and CHERYL E. PRAEGER

(Received xx Month 2016)

Abstract

Primitive prime divisors play an important role in group theory and number theory. We study a certain number theoretic quantity, called $\Phi_n^*(q)$, which is closely related to the cyclotomic polynomial $\Phi_n(x)$ and to primitive prime divisors of $q^n - 1$. Our definition of $\Phi_n^*(q)$ is novel, and we prove it is equivalent to the definition given by Hering. Given positive constants c and k, we give an algorithm for determining all pairs (n, q) with $\Phi_n^*(q) \leqslant cn^k$. This algorithm is used to extend (and correct) a result of Hering which is useful for classifying certain families of subgroups of finite linear groups.

2010 *Mathematics subject classification*: 11T22, 11Y40, 20G05.

Keywords and phrases: Zsigmondy primes, Cyclotomic Polynomial.

Dedicated to the memory of our esteemed colleague L.G. (Laci) Kovács

1. Introduction

In 1974 Christoph Hering [15] classified the subgroups G of the general linear group $\mathrm{GL}(n, \mathbb{F}_q)$ which act transitively on the nonzero vectors $(\mathbb{F}_q)^n \setminus \{0\}$. In his investigations a certain number theoretic function, $\Phi_n^*(q)$, plays an important role. It divides the nth cyclotomic polynomial evaluated at a prime power q, and hence divides $|(\mathbb{F}_q)^n \setminus \{0\}| = q^n - 1$. It is not hard to prove that $\mathrm{GL}(n, \mathbb{F}_q)$ contains an element of order $\Phi_n^*(q)$, and every element g of $\mathrm{GL}(n, \mathbb{F}_q)$ whose order is not coprime to $\Phi_n^*(q)$ acts irreducibly on the natural module $(\mathbb{F}_q)^n$, c.f. [15, Theorem 3.5]. A key result [15, p.1] shows that if $1 < \gcd(|G|, \Phi_n^*(q)) \leqslant (n + 1)(2n + 1)$, then the structure of G is severely constrained.

Our definition below of $\Phi_n^*(q)$ differs from the one used by Hering [15, p. 1], Lüneburg [18, Satz 2] and Camina and Whelan [7, Theorem 3.23], who used the

---

definition in Lemma 7(c). We show in Section 3 that our definition is equivalent to theirs and that $\Phi_n^*(q)$ could have also been defined in several other ways.

Definition 1. Suppose $n, q \in \mathbb{Z}$ are such that $n \geqslant 1$ and $q \geqslant 2$. Write $\Phi_n(X)$ for the n-th cyclotomic polynomial $\prod_\zeta (X - \zeta)$ where ζ ranges over the primitive complex n-th roots of unity. Let $\Phi_n^*(q)$ be the largest divisor of $\Phi_n(q)$ which is coprime to $\prod_{1 \leqslant k < n}(q^k - 1)$.

Our definition of $\Phi_n^*(q)$ is motivated by the numerous applications of primitive prime divisors, see [19] or [1, 14]. As our primary motivation is geometric, we will assume later (after Section 4) that q is a prime power; before this point $q \geqslant 2$ is arbitrary unless otherwise stated. A divisor m of $q^n - 1$ is called a *strong primitive divisor of* $q^n - 1$ if $\gcd(m, q^k - 1) = 1$ for $1 \leqslant k < n$, and a *weak primitive divisor of* $q^n - 1$ if $m \nmid (q^k - 1)$ for $1 \leqslant k < n$. By our definition, $\Phi_n^*(q)$ is the largest strong primitive divisor of $q^n - 1$. A primitive divisor of $q^n - 1$ which is prime is called a *primitive prime divisor* (*ppd*) of $q^n - 1$ or a Zsigmondy prime (“strong” equals “weak” for primes). DiMuro [9] uses weak primitive *prime power* divisors or *pppds* to extend the classification in [14] to $d/3 < n \leqslant d$. Our application in Section 7 has $d/4 \leqslant n \leqslant d$.

Primitive prime divisors have been studied since Bang [2] proved in 1886 that $q^n - 1$ has a primitive prime divisor for all $q \geqslant 2$ and $n > 2$ except for $q = 2$ and $n = 6$. Given coprime integers $q > r \geqslant 1$ and $n > 2$, Zsigmondy [22] proved in 1892 that there exists a prime p dividing $q^n - r^n$ but not $q^k - r^k$ for $1 \leqslant k < n$ except when $q = 2$, $r = 1$, and $n = 6$. The Bang-Zsigmondy theorem has been reproved many times as explained in [20, p. 27] and [8, p. 3]; modern proofs appear in [18, 21]. Feit [11] studied ‘large Zsigmondy primes’, and these play a fundamental role in the recognition algorithm in [19]. Hering’s results in [15] influenced subsequent work on linear groups, including the classification of linear groups containing primitive prime divisor (ppd)-elements [14], and its refinements in [1, 9, 19].

We describe algorithms in Sections 4 and 5 which, given positive constants c and k, list all pairs (n, q) for which $n \geqslant 3$ and $\Phi_n^*(q) \leqslant cn^k$. The behaviour of $\Phi_n^*(q)$ for $n = 2$ is different from that for larger n (see Lemma 7(b) and Algorithm 12).

Theorem 2. *Let $q \geqslant 2$ be a prime power.*

(a) *There is an algorithm which, given constants $c, k > 0$ as input, outputs all pairs (n, q) with $n \geqslant 3$ and $q \geqslant 2$ a prime power such that $\Phi_n^*(q) \leqslant cn^k$.*

(b) *If $n \geqslant 3$, then $\Phi_n^*(q) \leqslant n^4$ if and only if (n, q) is listed in* Tables 1, 3 *or* 4. *Moreover, the prime powers q with $q \leqslant 5000$ and $\Phi_2^*(q) \leqslant 2^4 = 16$ are listed in* Table 2.

In some group theoretic applications we need explicit information about $\Phi_n^*(q)$ when this quantity is considerably larger than n^4, but we have tight control over the sizes of its ppd divisors (each of which must be of the form $in + 1$ by Lemma 5(c)). We give an example of this kind of result in Theorem 3, where we require that the ppd divisors are sufficiently small for our group theoretic application in Section 7. This motivated our effort to strengthen Hering's result and we discovered two missing cases in [15, Theorem 3.9]; see Remark 4. We list in Theorem 2 all pairs (n, q) with $n \geqslant 3$ and $q \geqslant 2$ a prime power for which $\Phi_n^*(q) \leqslant n^4$; the implementations in [13] can handle much larger cases like $\Phi_n^*(q) \leqslant n^{20}$. In Theorem 3 we also require that the ppd divisors of $\Phi_n^*(q)$ be small for our group theoretic application in Section 7.

Theorem 3. *Suppose that* $q \geqslant 2$ *is a prime power and* $n \geqslant 3$. *Then all possible values of* (n, q) *such that* $\Phi_n^*(q)$ *has a prime factorisation of the form* $\prod_{i=1}^4 (in+1)^{m_i}$, *with* $0 \leqslant m_1 \leqslant 3$ *and* $0 \leqslant m_2, m_3, m_4 \leqslant 1$ *are listed in* Table 5.

The proof of Theorem 2(a) rests on the correctness of Algorithms 10 and 11 which are proved in Sections 4 and 5. Theorem 2(b) and 3 follow by applying these algorithms. For Theorem 3 we observe that $\Phi_n^*(q) \leqslant (n+1)^3 \prod_{i=2}^4 (in+1) \leqslant 16n^7$ for all $n \geqslant 4$, whereas for $n = 3$ only $2n+1$ and $4n+1$ are primes and again $\Phi_n^*(q) \leqslant 7 \cdot 13 \leqslant 16n^7$. Thus the entries in Table 5 were obtained by searching the output of our algorithms to find the pairs (n, q) for which $\Phi_n^*(q) \leqslant 16n^7$ and has the given factorisation. This factorisation arose from the application (Theorem 13) in Section 7.

Remark 4. The missing cases in part (d) of [15, Theorem 3.9] had $\Phi_n^*(q) = (n+1)^2$. We discovered the possibilities $n = 2, q = 17$, and $n = 2, q = 71$ when comparing Hering's result with output of the Magma [6] and GAP [12] implementations of our algorithms, see Table 2.

2. Cyclotomic polynomials: elementary facts

The product $\prod_{1 \leqslant k < n} (q^k - 1)$ has no factors when $n = 1$. An empty product is 1, by convention, and so $\Phi_1^*(q) = \Phi_1(q) = q - 1$.

The Möbius function μ satisfies $\mu(n) = (-1)^k$ if $n = p_1 \cdots p_k$ is a product of distinct primes, and $\mu(n) = 0$ otherwise. Our algorithm uses the following elementary facts.

Lemma 5. *Let* n *and* q *be integers satisfying* $n \geqslant 1$ *and* $q \geqslant 2$.

(a) *The polynomial* $\Phi_n(X)$ *lies in* $\mathbb{Z}[X]$ *and is irreducible. Moreover,*

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) \qquad \text{and} \qquad \Phi_n(X) = \prod_{d \mid n} (X^{\frac{n}{d}} - 1)^{\mu(d)}.$$

(b) *If* $d \mid n$ *and* $d > 1$, *then* $\Phi_n(X)$ *divides* $(X^n - 1)/(X^{n/d} - 1) = \sum_{i=0}^{d-1} (X^{n/d})^i$.

(c) *If* r *is a prime and* $r \mid \Phi_n^*(q)$, *then* n *divides* $r - 1$, *equivalently* $r \equiv 1 \pmod{n}$.

(d) *For any fixed integer* $n \geqslant 1$ *the function* $\Phi_n(q)$ *is strictly increasing for* $q > 1$.

(e) *Let* φ *be Euler's totient function which satisfies* $\varphi(n) = \deg(\Phi_n(X))$. *Then*

$$\varphi(n) \geqslant \frac{n}{\log_2(n) + 1} \qquad \text{for } n \geqslant 1.$$

(f) *For all* $n \geqslant 2$ *and* $q \geqslant 2$ *we have* $q^{\varphi(n)}/4 < \Phi_n(q) < 4q^{\varphi(n)}$.

PROOF. (a) The irreducibility of $\Phi_n(X) \in \mathbb{Z}[X]$ and the other facts, are proved in [10, §13.4].

(b) By part (a) $(X^n - 1)/(X^{n/d} - 1)$ equals $\prod_k \Phi_k(X)$ where $k \mid n$ and $k \nmid (n/d)$. Since $d > 1$, it follows that $\Phi_n(X)$ is a factor in this product.

(c) If $r \mid \Phi_n^*(q)$ then $r \mid (q^n - 1)$ and n is the order of q modulo r, so $n \mid (r - 1)$.

(d) This follows from Definition 1 because $\Phi_n(q) = |\Phi_n(q)| = \prod_\zeta |q - \zeta|$ and $|\zeta| = 1$.

(e) We use the formula $\varphi(n) = n \prod_{i=1}^{t} \frac{p_i - 1}{p_i}$ where $p_1 < p_2 < \cdots < p_t$ are the prime divisors of n. Using the trivial estimate $p_i \geqslant i + 1$ we get $\varphi(n) \geqslant n/(t + 1)$. It follows from $2^t \leqslant p_1 p_2 \cdots p_t \leqslant n$ that $t \leqslant \log_2(n)$. Hence $\varphi(n) \geqslant n/(\log_2(n) + 1)$ as claimed.

(f) Using the product formula for $\Phi_n(X)$ in (a) and $\mu(d) \in \{0, -1, 1\}$, we see that $\Phi_n(q)$ equals $q^{\varphi(n)}$ times a product of distinct factors of the form $(1 - 1/q^i)^{\pm 1}$ with $1 \leqslant i \leqslant n$. Since $\prod_{i=1}^{\infty}(1 - 1/q^i) \geqslant \prod_{i=1}^{\infty}(1 - 1/2^i) = 0.28878 \cdots > 1/4$ we get

$$\frac{q^{\varphi(n)}}{4} < \Phi_n(q) < 4q^{\varphi(n)}.$$

REMARK 6. Hering [15, Theorem 3.6] gives sharper estimates than those in Lemma 5(f). But our (easily established) estimates suffice for the efficient algorithms below.

3. Equivalent definitions of $\Phi_n^*(q)$

We now state equivalent ways in which to define $\Phi_n^*(q)$ where $q \geqslant 2$ is an integer. Because our motivation for studying $\Phi_n^*(q)$ arose from finite geometry, we assume after the proof of Lemma 7 that q is a prime power. Observe that Lemma 7(b) suggests a much faster algorithm for computing $\Phi_n^*(q)$ than does Definition 1.

LEMMA 7. *Let* n, q *be integers such that* $n \geqslant 2$ *and* $q \geqslant 2$. *The following statements could be used as alternatives to the definition of* $\Phi_n^*(q)$ *given in Definition 1.*

(a) $\Phi_n^*(q)$ *is the largest divisor of* $\Phi_n(q)$ *coprime to* $\prod_{k \mid n,\, k<n} \Phi_k(q)$.

(b) *Let* $(q + 1)_2$ *be the largest power of* 2 *dividing* $q + 1$, *and let* r *be the largest prime divisor of* n. *Then*

$$\Phi_n^*(q) = \begin{cases} (q+1)/(q+1)_2 & \text{if } n = 2,\\ \Phi_n(q) & \text{if } n > 2 \text{ and } r \nmid \Phi_n(q),\\ \Phi_n(q)/r & \text{if } n > 2 \text{ and } r \mid \Phi_n(q).\end{cases}$$

(c) $\Phi_n^*(q) = \Phi_n(q)/f^i$ *where* f^i *is the largest power of* $f := \gcd(\Phi_n(q), n)$ *dividing* $\Phi_n(q)$.

Remark 8. For $n > 2$ the last paragraph of the proof of part (b) shows that $d := \gcd(\Phi_n(q), \prod_{1\leqslant k<n}(q^i - 1))$ equals $f := \gcd(\Phi_n(q), n)$. Either $d = f = 1$ and $r \nmid \Phi_n(q)$, of $d = f = r$ and $r \mid \Phi_n(q)$. Thus, part (c) simplifies to $\Phi_n^*(q) = \Phi_n(q)/f$ when $n > 2$.

Proof. (a) We use the following notation where m is a divisor of $\Phi_n(q)$:

$$P_n = \prod_{1\leqslant k<n}(q^k - 1), \qquad P_n' = \prod_{k\mid n,\, k<n} \Phi_k(q),$$
$$d_n(m) = \gcd(m, P_n), \qquad d_n'(m) = \gcd(m, P_n').$$

Fix a divisor m of $\Phi_n(q)$. We prove that $d_n(m) = 1$ holds if and only if $d_n'(m) = 1$. Certainly $d_n(m) = 1$ implies $d_n'(m) = 1$ as $P_n' \mid P_n$. Conversely, suppose that $d_n(m) \neq 1$. Then there exists a prime divisor r of m that divides $q^k - 1$ for some k with $1 \leqslant k < n$. However, $r \mid \Phi_n(q) \mid (q^n - 1)$ and $\gcd(q^n - 1, q^k - 1) = q^{\gcd(n,k)} - 1$, so r divides $q^{\gcd(n,k)} - 1$. Hence r divides $\Phi_\ell(q)$ for some $\ell \mid \gcd(n, k)$ by Lemma 5(a). In summary, $r \mid d_n(m)$ implies $r \mid d_n'(m)$, so $d_n(m) \neq 1$ implies $d_n'(m) \neq 1$.

For any divisor m of $\Phi_n(q)$ we have shown that $\gcd(m, P_n) = 1$ holds if and only if $\gcd(m, P_n') = 1$. Thus the largest divisor of $\Phi_n(q)$ coprime to P_n' is equal to the largest such divisor which is coprime to P_n, and this is $\Phi_n^*(q)$ by Definition 1.

(b) First consider the case $n = 2$. Now $d := d_2(\Phi_2(q)) = \gcd(q + 1, q - 1)$ divides 2. Indeed, $d = 1$ for even q, and $d = 2$ for odd q. In both cases, $(q + 1)/(q + 1)_2$ is the largest divisor of $q + 1$ coprime to $q - 1$. Thus $\Phi_2^*(q) = (q + 1)/(q + 1)_2$ by Definition 1.

Assume now that $n > 2$. Let $d = \gcd(\Phi_n(q), P_n)$ where $P_n = \prod_{1\leqslant k<n}(q^k - 1)$. If $d = 1$, then $\Phi_n^*(q) = \Phi_n(q)$ by Definition 1. Suppose that $d > 1$ and p is a prime divisor of d. Then the order of q modulo p is less than n, and Feit [11] calls p a non-Zsigmondy prime. It follows from [21, Proposition 2] or Lüneburg [18, Satz 1] that the prime p divides $\Phi_n(q)$ exactly once, and $p = r$ is the largest prime divisor of n. Thus we see that $\gcd(\Phi_n(q)/r, P_n) = 1$ and $\Phi_n^*(q) = \Phi_n(q)/r$ by Definition 1. This proves (b).

To connect with part (c), we prove when $n > 2$ that d equals $f := \gcd(\Phi_n(q), n)$. Indeed, we prove Remark 8 that either $d = f = 1$ and $r \nmid \Phi_n(q)$, or $d = f = r$ and $r \mid \Phi_n(q)$. If $d = 1$, then $\Phi_n^*(q) = \Phi_n(q)$ and a prime divisor p of $\Phi_n^*(q)$ satisfies $p \equiv 1 \pmod{n}$ by Lemma 5(c) and hence $p \nmid n$. Thus $f = 1$ and $r \nmid \Phi_n(q)$ since $r \mid n$. Conversely, suppose that $d > 1$. The previous paragraph shows that $d = r$ and $r^2 \nmid \Phi_n(q)$. Thus $r \mid f$. Let p be a prime dividing $f = \gcd(\Phi_n(q), n)$. Since $\Phi_n(q) \mid (q^n - 1)$, we have $p \mid (q^n - 1)$, and hence $p \nmid \Phi_n^*(q)$ by Lemma 5(c). Thus p divides P_n by Definition 1, and hence p divides $d = \gcd(\Phi_n(q), P_n)$. However, $d = r$ and so $p = r = f$, and in this case $r \mid \Phi_n(q)$.

(c) By part (b) and the last paragraph of the proof of (b), Definition 1 is equivalent to Hering's definition [15] in part (c).

Remark 9. When q is a prime power, there is a fourth equivalent definition: $\Phi_n^*(q)$ is the order of the largest subgroup of $\mathbb{F}_{q^n}^\times$ (the multiplicative group of q^n-1 nonzero elements of $\mathbb{F}_{q^n}$) that intersects trivially all the subgroups $\mathbb{F}_{q^d}^\times$ for $d \mid n$, $d<n$.

Proof. The correspondence $H \leftrightarrow |H|$ is a bijection between the subgroups H of the cyclic group $\mathbb{F}_{q^n}^\times$ and the divisors of q^n-1. Suppose $d \mid n$. Note that $H \cap \mathbb{F}_{q^d}^\times = \{1\}$ holds if and only if $\gcd(|H|, q^d-1)=1$ as $\mathbb{F}_{q^n}^\times$ is cyclic. Thus there exists a unique subgroup H whose order m is maximal subject to $H \cap \mathbb{F}_{q^d}^\times = \{1\}$ for all $d \mid n$, $d<n$. Hence m is the largest divisor of q^n-1 satisfying $\gcd(m, q^d-1)=1$ for all $d \mid n$, $d<n$. Since $q^n-1=\prod_{d \mid n}\Phi_d(q)$ and $\Phi_d(q) \mid q^d-1$, we see that $m \mid \Phi_n(q)$. It follows from Lemma 7 (a) that $\Phi_n^*(q)=m$.

4. The polynomial bound $\Phi_n(q) \leqslant cn^k$

As we will discuss in Section 5, the number of pairs $(2,q)$ with q a prime power satisfying $\Phi_2(q) \leqslant c2^k$ is potentially infinite. We therefore deal here with pairs (n,q) for $n \geqslant 3$. Given positive constants c and k, we now describe an algorithm for determining all pairs in the set

$$M(c,k) := \{(n,q) \in \mathbb{Z} \times \mathbb{Z} \mid n \geqslant 3,\ q \geqslant 2 \text{ a prime power, and } \Phi_n(q) \leqslant cn^k\}.$$

Algorithm 10. $M(c,k)$

Input: Positive constants c and k.
Output: The finite set $M(c,k)$.

10.1 [Definitions] Set $s := 2+\log_2(c)$, $t := (s+k)/\ln(2)$, $u := k/\ln(2)^2$ and $b := e^{1-t/(2u)}$ and define for $x \geqslant 3$ the function $g(x) := x-s-t\ln(x)-u\ln(x)^2$ where $\ln(x)=\log_e(x)$. Note that $g(x)$ has derivative $g'(x) := 1-t/x-2u\ln(x)/x$.
10.2 [Initialise] Set $n := 3$ and set $M(c,k)$ to be the empty set.
10.3 [Termination criterion] If $n>b$ and $g(n)>0$ and $g'(n)>0$ then return $M(c,k)$.
10.4 [For fixed n, find all q] If $g(n)<0$ and $2^{\varphi(n)-2}<cn^k$ then compute $\Phi_n(X)$ and find the smallest prime power $\tilde{q}$ such that $\Phi_n(\tilde{q})>cn^k$; add (n,q) to $M(c,k)$ for all prime powers $q<\tilde{q}$.
10.5 [Increment and loop] Set $n := n+1$ and go back to step 10.3.

Proof of correctness. Algorithm 10 starts with $n=3$ and it continues to increment n. We must prove that it does terminate at step 10.3, and that it correctly returns $M(c,k)$. Note first that for fixed n the values $\Phi_n(q)$ are strictly increasing with q by Lemma 5(d). Thus it follows from Lemma 5(e) and (f) that

$$\Phi_n(q) \geqslant \Phi_n(2) > \frac{2^{\varphi(n)}}{4} = 2^{\varphi(n)-2} \geqslant 2^{n/(\log_2(n)+1)-2}.$$

Consider the inequality $2^{n/(\log_2(n)+1)-2} \geqslant cn^k$. Taking base-2 logarithms shows

$$\begin{aligned} n &\geqslant (k\log_2(n) + \log_2(c) + 2)(\log_2(n) + 1) \\ &= (\log_2(c) + 2) + (k + \log_2(c) + 2)\log_2(n) + k\log_2(n)^2 \\ &= s + t\ln(n) + u\ln(n)^2 \end{aligned}$$

where the last step uses $\log_2(n) = \ln(n)/\ln(2)$ and the definitions in step 10.1. In summary, $2^{n/(\log_2(n)+1)-2} \geqslant cn^k$ is equivalent to $g(n) \geqslant 0$ with $g(n)$ as defined in step 10.1.

The inequalities above show that the conditions $g(n) < 0$ and $2^{\varphi(n)-2} < cn^k$, which we test in step 10.4, are necessary for $\Phi_n(2) \leqslant cn^k$. We noted above that for fixed n the values of $\Phi_n(q)$ strictly increase with q. Thus (if executed for a particular n) step 10.4 correctly adds to $M(c,k)$ all pairs (n,q) for prime powers q such that $\Phi_n(q) \leqslant cn^k$.

It remains to show (i) that the algorithm terminates, and (ii) that the returned set $M(c,k)$ contains *all* pairs (n,q) such that $\Phi_n(q) \leqslant cn^k$. The second derivative of $g(x)$ equals $g''(x) = (t - 2u(1 - \ln(x)))/x^2$. Since $u > 0$ this shows that $g''(x) > 0$ if and only if $x > b = e^{1-t/(2u)}$. Thus $g'(x)$ is increasing for all $x > b$. Because x grows faster than any power of $\ln(x)$ we have that $g(x) > 0$ and $g'(x) > 0$ for x sufficiently large. Thus there exists a (smallest) integer $\tilde{n}$ fulfilling the conditions in step 10.3, that is, $\tilde{n} > b$, $g(\tilde{n}) > 0$ and $g'(\tilde{n}) > 0$. The algorithm terminates when step 10.3 is executed for the integer $\tilde{n}$. To prove that the returned set $M(c,k)$ is complete, we verify that, for all $n \geqslant \tilde{n}$, there is no prime power q such that $\Phi_n(q) \leqslant cn^k$. Now, for all $x \geqslant \tilde{n}$, we have $x > b$ so that $g'(x)$ is increasing for $x \geqslant \tilde{n}$, and so $g'(x) \geqslant g'(\tilde{n}) > 0$, whence $g(x)$ is increasing for $x \geqslant \tilde{n}$. In particular, $n \geqslant \tilde{n}$ implies that $g(n) \geqslant g(\tilde{n}) > 0$ and so (from our displayed computation above), for all prime powers q, $\Phi_n(q) \geqslant \Phi_n(2) > cn^k$. Thus there are no pairs $(n,q) \in M(c,k)$ with $n \geqslant \tilde{n}$, so the returned set $M(c,k)$ is complete. □

5. Determining when $\Phi_n^*(q) \leqslant cn^k$

We describe an algorithm to determine all pairs (n,q), with $n, q \geqslant 2$ and q a prime power, such that the value $\Phi_n^*(q)$ is bounded by a given polynomial in n, say $f(n)$. For $n \geqslant 3$ the algorithm determines the finite list of possible (n,q). For $n = 2$ the output is split between a finite list which we determine, and a potentially infinite (but very restrictive) set of prime powers q of the form $2^a m - 1$ where $m \leqslant f(2)$ is odd. Table 2 lists the prime powers $q \leqslant 5000$ such that $\Phi_2^*(q) \leqslant 16$; we see that some proper powers occur, though the majority of the entries are primes. For example, if $\Phi_2^*(q) = 1$ then the prime powers q of the form $2^a - 1$, must be a prime by [22]. Such primes are called Mersenne primes.

The set $M(c,k)$ of all pairs (n,q) satisfying $\Phi_n(q) \leqslant cn^k$ is finite by Lemma 5(f). By contrast the set of pairs (n,q) satisfying $\Phi_n^*(q) \leqslant cn^k$ may be infinite as $\Phi_2^*(q) = m$, m odd, may have infinitely many (but highly restricted) solutions for q. Algorithm 11 computes the following set (which we see below is a finite set)

$$M^*_{\geqslant 3}(c,k) = \left\{(n,q) \in \mathbb{Z}\times\mathbb{Z} \mid n \geqslant 3,\, q \geqslant 2 \text{ a prime power, and } \Phi^*_n(q) \leqslant cn^k\right\}.$$

Algorithm 11. $M^*_{\geqslant 3}(c,k)$

Input: Positive constants c and k.
Output: The finite set $M^*_{\geqslant 3}(c,k)$.

```
11.1 Compute $M(c, k+1)$ with Algorithm 10.
11.2 Initialise $M^*_{\geqslant 3}(c,k)$ as the empty set. For all $(n,q) \in M(c,k+1)$ with $n \geqslant 3$ check
     if $\Phi^*_n(q) \leqslant cn^k$. If yes, add $(n,q)$ to $M^*_{\geqslant 3}(c,k)$.
11.3 Return $M^*_{\geqslant 3}(c,k)$.
```

Proof of correctness. We need to show that all $M^*_{\geqslant 3}(c,k) \subseteq M(c,k+1)$. This follows from Lemma 7(b) which shows that $n\Phi^*_n(q) \geqslant \Phi_n(q)$ whenever $n \geqslant 3$. □

Case $n = 2$. We treat the case $n = 2$ separately as the classification has a finite part and a potentially infinite part. Suppose q is odd and $\Phi^*_2(q) = \frac{q+1}{2^a} = m \leqslant cn^k$ where m is odd by Lemma 7(b). Then solving for q gives $q = 2^a m - 1$.

If $m = 1$ then $q = 2^a - 1$ is a (Mersenne) prime as remarked in the first paragraph of this section. Lenstra-Pomerance-Wagstaff conjectured [17] that there are infinitely many Mersenne primes, and the asymptotic density of the set $\{a < x \mid 2^a - 1 \text{ prime}\}$ is $O(\log x)$. For fixed m with $m > 1$, the number of prime powers of the form $2^a m - 1$ may also be infinite (although in this case we cannot conclude that a must be prime). The set

$$M^*_2(c,k) = \{(2,q) \mid \Phi^*_n(q) \leqslant c2^k \text{ and } q \text{ is a prime power}\}$$

is a disjoint union of three subsets:

$$\begin{aligned}
R(c,k) &:= \{(2,q) \mid (2,q) \in M^*_2(c,k) \text{ and } q \not\equiv 3 \pmod 4\},\\
S(c,k) &:= \{(2,q) \mid (2,q) \in M^*_2(c,k) \text{ and } q \equiv 3 \pmod 4 \text{ and } q \text{ not prime }\},\\
T(c,k) &:= \{(2,q) \mid (2,q) \in M^*_2(c,k) \text{ and } q \equiv 3 \pmod 4 \text{ and } q \text{ prime}\}
\end{aligned}$$

As the set $T(c,k)$ may be infinite Algorithm 12 below takes as input a constant $B > 0$ and computes the finite subset $T(c,k,B) = \{(2,q) \mid q \in T(c,k) \text{ and } q \leqslant B\}$ of $M^*_2(c,k)$. Table 2 has $n = 2$ and $q \leqslant 5000$, so we input $B = 5000$.

Algorithm 12. $M^*_2(c,k,B)$

Input: Positive constants c, k and B.
Output: The (finite) set $R(c,k) \cup S(c,k) \cup T(c,k,B)$, see the notation above.

12.1 Initialise each of $R(c,k)$, $S(c,k)$, $T(c,k,B)$ as the empty set.
12.2 Add $(2,q)$ to $R(c,k)$ when q is a power of 2 with $q+1 \leqslant c2^k$.
12.3 Add $(2,q)$ to $R(c,k)$ when q is a prime power, $q \equiv 1 \pmod 4$ and $(q+1)/2 \leqslant c2^k$.
12.4 For all primes $p \equiv 3 \pmod 4$ with $p \leqslant B$ and $(p+1)/(p+1)_2 \leqslant c2^k$ add $(2,p)$ to $T(c,k,B)$. For all primes $p \equiv 3 \pmod 4$ (where $p \leqslant c2^{k-1}$ is allowed) and all odd $\ell \geqslant 3$ with $\sum_{i=0}^{\ell-1}(-p)^i \leqslant c2^k$ add $(2,p^\ell)$ to $S(c,k)$ if $\Phi_2^*(p^\ell) \leqslant c2^k$.
12.5 Return $R(c,k) \cup S(c,k) \cup T(c,k,B)$.

Proof of correctness. By Lemma 7(b), $\Phi_2^*(q) = \Phi_2(q) = q+1$ when q is an even prime power and $\Phi_2^*(q) = \Phi_2(q)/2 = (q+1)/2$ if $q \equiv 1 \pmod 4$. It is clear that steps 12.2 and 12.3 find all pairs $(2,q) \in R(c,k)$ with $q \not\equiv 3 \pmod 4$, and there are finitely many choices for q.

Any prime power $q \equiv 3 \pmod 4$ is an odd power $q = p^\ell$ of a prime $p \equiv 3 \pmod 4$. Write $q+1 = 2^a m$ with m odd and $a \geqslant 2$, then $\Phi_2^*(q) = m$. If q is a prime $(2,q) \in T(c,k,B)$ if and only if $q \leqslant B$ and $\Phi_2^*(q) \leqslant c2^k$, so step 12.4 adds such pairs. This is because, when $q \equiv 3 \pmod 4$ and $q \leqslant B$ we have, by Lemma 7(b), that $\Phi_2^*(q) = (q+1)/2 \leqslant B$. Suppose q is not a prime, that is $\ell > 1$. Then we have the factorisation $q+1 = (p+1)(\sum_{i=0}^{\ell-1}(-p)^i)$ where the second factor is odd and so divides m. Since $2p^{\ell-2} \leqslant p^{\ell-2}(p-1) < \sum_{i=0}^{\ell-1}(-p)^i \leqslant m$ and we require $m \leqslant c2^k$, we see $p^{\ell-2} \leqslant c2^{k-1}$. Since there are finitely many solutions to $p^{\ell-2} \leqslant c2^{k-1}$ with $\ell > 1$ odd, $S(c,k)$ is a finitely set, and step 12.4 correctly computes $S(c,k)$. Finally, the disjoint union $R(c,k) \cup S(c,k) \cup T(c,k,B)$ is the desired output set. □

Proofs of Theorems 2 and 3. Theorem 2(a) follows from the correctness of Algorithms 10 and 11, and Theorem 2(b) uses these algorithms with $(c,k) = (1,4)$. Similarly, Theorem 3 uses these algorithms with $(c,k) = (16,7)$. It is shown that in the penultimate paragraph of the proof of Theorem 13 that $\Phi_n^*(q) \leqslant 16n^7$ holds for $n \geqslant 4$. If $n = 3$ and $1 \leqslant i \leqslant 4$, then $in+1$ is prime for $i = 2, 4$, and again $\Phi_n^*(q) \leqslant 7 \cdot 13 \leqslant 16n^7$ holds. We then search the (rather large) output set for the pairs (n,q) for which $\Phi_n^*(q)$ has the prescribed prime factorisation. Magma [6] code generating the data for Tables 1–5 mentioned in Theorems 2 and 3 is available at [13]. □

6. The tables

By Lemma 5(c) the prime factorisation of $\Phi_n^*(q)$ has the form $\prod_{i\geqslant 1}(in+1)^{m_i}$ where $m_i = 0$ if $in+1$ is not a prime. It is convenient to encode this prime factorisation as $\Phi_n^*(q) = \prod_{i\in I}(in+1)$ where I is a multiset, and for each $i \in I$ the prime divisor $in+1$ of $\Phi_n^*(q)$ is repeated m_i times in $I = I(n,q)$. For example, $\Phi_4^*(8) = 65 = (4+1)(3\cdot 4+1)$ so $I(4,8) = \{\{1,3\}\}$ and $\Phi_5^*(3) = 121 = (2\cdot 5+1)^2$ so $I(5,3) = \{\{2,2\}\}$. To save space, we omit the double braces in our tables and denote the empty multiset (corresponding to $\Phi_6^*(2) = 1$) by '–'. All of our data did not conveniently fit into Table 1, so we created subsidiary tables 2, 3, 4 for $n = 2$, $n = 6$ and $n \geqslant 19$, respectively. For n and q such that $\Phi_n^*(q) \leqslant n^4$ Tables 1 and 4 record in row n and column q the multiset $I(n, q)$. The tables are the output from Algorithm 11 with $c = 1$ and $k = 4$.

Table 5 exhibits data for two different theorems. For Theorem 3 we record the triples (n, q, I) for which $n \geqslant 3$ and $\Phi_n^*(q)$ has prime factorisation $\prod_{i\in I}(i\,n + 1)$ where $I \subseteq \{\{1, 1, 1, 2, 3, 4\}\}$. For Theorem 13 we also list the possible degrees c that can arise, namely $c_0 \leqslant c \leqslant c_1$.

$n\backslash q$	2	3	4	5	7	8	9	11	13	17	19
2	Table 2										
3	2	4	2	10	6	24			20		
4	1	1	4	3	1, 1	1, 3	10	15	1, 4	1, 7	45
5	6	2, 2	2, 6								
6	Table 3										
7	18	156									
8	2	5	32	39	150		2, 24				
9	8	84	2, 8								
10	1	6	4	52	1, 19	1, 33	118				
11	2, 8										
12	1	6	20	50	1, 15	3, 9	540	1, 93			
13	630										
14	3	39	2, 8	2, 32							
15	10	304	10, 22								
16	16	1, 12									
18	1	1, 2	2, 6	287		4845					
$\geqslant 19$	Table 4										

TABLE 1. Triples (n, q, I) with $\Phi_n^*(q) \leqslant n^4$ and prime factorisation $\Phi_n^*(q) = \prod_{i\in I}(in + 1)$.

q	2	3	2^2	5	7	2^3	3^2	11	13	17	19	23	5^2	3^3	29	31
q	43	47	59	71	79	103	127	191	223	239	383	479	1151	1279	1663	3583

TABLE 2. Prime powers $q \leqslant 5000$ with $\Phi_2^*(q) \leqslant 2^4 = 16$, see Remark 4.

q	2	3	4	5	7	8	9	11	13	16	17
I	–	1	2	1	7	3	12	6	26	40	1, 2
q	19	23	25	27	29	31	32	41	47	53	59
I	1, 1, 1	2, 2	100	3, 6	45	1, 1, 3	55	91	1, 17	153	1, 27

Table 3. Pairs (q, I) with $\Phi_6^*(q) \leqslant 6^4$ and prime factorisation $\Phi_6^*(q) = \prod_{i \in I}(in + 1)$ where – means $\{\!\{\ \}\!\}$.

$n\backslash q$	2	3	4	5	$n\backslash q$	2	3	$n\backslash q$	2
20	2	59	3084		33	18166		50	5, 81
21	16				34	1285		54	1615
22	31	3, 30			36	1, 3	14742	60	1, 22
24	10	270	4, 28		38	4599		66	1, 316
26	105	15330			40	1542		72	6, 538
27	9728				42	129	1, 54	78	286755
28	1, 4	1, 589			44	9, 48		84	17, 172
30	11	1, 9	2, 44	2, 254	46	60787		90	209300
32	2048				48	2, 14			

Table 4. All (n, q, I) with $n \geqslant 19$, $\Phi_n^*(q) \leqslant n^4$, and factorisation $\Phi_n^*(q) = \prod_{i \in I}(in + 1)$.

n	q	I	c_0	c_1	n	q	I	c_0	c_1	n	q	I	c_0	c_1
3	2	2			4	13	1, 4	17	17	8	2	2	17	34
3	3	4			4	47	1, 3, 4	17	17	10	2	1	15	42
3	4	2			6	2	–	15	26	10	4	4	41	42
3	9	2, 4			6	3	1	15	25	12	2	1	15	50
3	16	2, 4			6	4	2	15	26	14	2	3	43	58
4	2	1	15	18	6	5	1	15	25	18	2	1	19	74
4	3	1	15	18	6	8	3	19	26	18	3	1, 2	37	73
4	4	4	17	18	6	17	1, 2	15	25	20	2	2	41	82
4	5	3	15	17	6	19	1, 1, 1	15	25	28	2	1, 4	113	114
4	7	1, 1	15	17	6	31	1, 1, 3	19	25	36	2	1, 3	109	146
4	8	1, 3	15	18										

Table 5. For Theorem 3 we list all (n, q, I) where $n \geqslant 3$ and $\Phi_n^*(q)$ has prime factorisation $\prod_{i \in I}(in + 1)$ with $I \subseteq \{\!\{1, 1, 1, 2, 3, 4\}\!\}$. For Theorem 13 we also list the possible degrees c where $c_0 \leqslant c \leqslant c_1$ and in this case we must have $n \geqslant 4$. Here – denotes the empty multiset.

7. An Application

Various studies of configurations in finite projective spaces have involved a subgroup G of a projective group $\mathrm{PGL}(d, q)$ (or equivalently, a subgroup of $\mathrm{GL}(d, q)$) with order divisible by $\Phi_n^*(q)$ for certain n, q. This situation was analysed in detail by Bamberg and Penttila [1] for the cases where $n > d/2$, making use of the classification in [14]. In turn, Bamberg and Penttila applied their analysis to certain geometrical questions, in particular proving a conjecture of Cameron and Liebler from 1982 about irreducible subgroups with equally many orbits on points and lines [1, Section 8]. In their group theoretic analysis Hering's theorem [15, Theorem 3.9] was used repeatedly, notably to deal with the 'nearly simple cases' where G has a normal subgroup H containing $\mathrm{Z}(G)$ such that H is absolutely irreducible, $H/\mathrm{Z}(G)$ is a nonabelian simple group, and $G/\mathrm{Z}(G) \leqslant \mathrm{Aut}(H/\mathrm{Z}(G))$. Incidentally, the missing cases $(n, q) = (2, 17)$ and $(2, 71)$ mentioned in Remark 4 do not affect the conclusions in [1].

To study other related geometric questions we have needed similar results which allow the parameter n to be as small as $d/4$. We give here an example of how our extension of Hering's results might be used to deal with nearly simple groups in this more general case where no existing general classifications are applicable. For example, there are several theorems about translation planes that include restrictive hypotheses such as two-transitivity [3, 4, 5]. In order to remove some of these restrictions, we require results similar to Theorem 13 for all nearly simple groups. For simplicity we now consider representations of the alternating or symmetric groups of degree $c \geqslant 15$ with $\Phi_n^*(q) \mid c!$ and, as we see below, $c - 1 \geqslant n \geqslant (c - 2)/4$.

Theorem 13. *Let $G \leqslant \mathrm{GL}(d, q)$ where $G \cong \mathrm{Alt}(c), \mathrm{Sym}(c)$, for some $c \geqslant 15$, and suppose that $\mathrm{Alt}(c)$ acts absolutely irreducibly on $(\mathbb{F}_q)^d$ where q is a power of the prime p. Suppose $\Phi_n^*(q)$ divides $c!$ for some $n \geqslant d/4$. Then $n \geqslant 4$, $d = c - \delta(c, q)$ where $\delta(c, q)$ equals 1 if $p \nmid c$, and 2 if $p \mid c$, also $c_0 \leqslant c \leqslant c_1$, and $\Phi_n^*(q)$ has prime factorisation $\prod_{i \in I}(in + 1)$, where all possible values for (n, q, I, c_0, c_1) are listed in* Table 5.

Proof. The smallest and the second smallest dimensions for $\mathrm{Alt}(c)$ and $\mathrm{Sym}(c)$ modules over $\mathbb{F}_q$ are very roughly, c and $c^2/2$ respectively. The precise statement below follows from James [16, Theorem 7], where the dimension formula $(*)$ on p. 420 of [16] is used for part (ii). Since $c \geqslant 15$, these results show that either:

(i) $(\mathbb{F}_q)^d$ is the fully deleted permutation module for $\mathrm{Alt}(c)$ with $d = c - \delta(c, q)$, or
(ii) $d \geqslant c(c - 5)/2$.

In particular, since $c \geqslant 15$ and $n \geqslant d/4$, we have $n \geqslant 4$. Since $n > 2$ it follows from Theorem 3.23 of [7] that $\Phi_n^*(q) > 1$ except when $n = 6$ and $q = 2$. As the case $(n, q) = (6, 2)$ is included in Table 5, we assume henceforth that $\Phi_n^*(q) > 1$. Thus $\Phi_n^*(q) = r_1^{m_1} \cdots r_\ell^{m_\ell}$ where $\ell \geqslant 1$, each r_i is a prime, and each $m_i \geqslant 1$. Then $r_i = a_i n + 1$ for some $a_i \geqslant 1$ by Lemma 5(c), and since r_i divides $|\mathrm{S}_c| = c!$ we see $c \geqslant r_i$. Let r be the largest prime divisor of $\Phi_n^*(q)$, so $c \geqslant r \geqslant n + 1 > d/4$. In case (ii) this implies that $c > c(c - 5)/8$ which contradicts the assumption $c \geqslant 15$. Thus case (i) holds.

The inequalities $c - 2 \leqslant d$ and $d \leqslant 4n$ show $a_i n + 1 \leqslant c \leqslant 4n + 2$ and hence $a_i \leqslant 4$.

The exponent m_i of r_i is severely constrained. If $a_i \geqslant 2$, then

$$r_i = a_i n + 1 \geqslant 2n + 1 \geqslant \frac{d+3}{2} \geqslant \frac{c+1}{2} > \frac{c}{2}.$$

Thus the prime r_i divides $c!$ exactly once, and $m_i = 1$. If $a_i = 1$, then a similar argument shows $r_i = n + 1 \geqslant \frac{d+4}{4} \geqslant \frac{c+2}{4} \geqslant \frac{17}{4} > 4$. The inequalities $r_i > \frac{c}{4}$ and $r_i > 4$ imply that r_i divides $c!$ at most three times, and $m_i \leqslant 3$. In summary, $\Phi^*_n(q)$ divides $f(n) := (n+1)^3(2n+1)(3n+1)(4n+1)$. Since $n \geqslant 4$, we have $f(n) \leqslant 16n^7$. All possible pairs (n, q) for which $\Phi^*_n(q) \mid f(n)$ can be computed using Algorithm 11 with input $c = 16$, $k = 7$. The output is listed in Table 5, and computed using [13].

For given n and q the possible values for c form an interval $c_0 \leqslant c \leqslant c_1$. Since $c - \delta(c, q) = d \leqslant 4n$ the entries c_0, c_1 in Table 5 can be determined as follows: $c_0 = \max(r, 15)$ where r is the largest prime divisor of $\Phi^*_n(q)$, and $c_1 = 4n + \delta(4n + 2, q)$. □

Acknowledgements We thank the referee for numerous helpful suggestions. The first, third and fourth authors acknowledge the support of ARC Discovery grant DP140100416.

References

[1] John Bamberg and Tim Penttila. Overgroups of Cyclic Sylow Subgroups of Linear Groups. *Communications in Algebra* **36** (2008), 2503–2543.

[2] A. S. Bang. Taltheoretiske Undersøgelser. *Tidsskrift Math.* (5) **4** (1886), 70–80 and 130–137.

[3] M. Biliotti, V. Jha, N. L. Johnson and A. Montinaro. Translation planes of order q^2 admitting a two-transitive orbit of length $q + 1$ on the line at infinity. *Designs, Codes and Cryptography* **44** (2007), 69–86.

[4] M. Biliotti, V. Jha, N. L. Johnson and A. Montinaro. Two-transitive groups on a hyperbolic unital. *J. Combin. Theory Series A* **115** (2008), 526–533.

[5] M. Biliotti, V. Jha, N. L. Johnson and A. Montinaro. Classification of projective translation planes of order q^2 admitting a two-transitive orbit of length $q + 1$. *J. Geom.*, in press.

[6] W. Bosma, J. Cannon and C. Playoust. The MAGMA algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997) (3-4), 235–265.

[7] A. R. Camina and E. A. Whelan. Linear groups and permutations. Research Notes in Mathematics, **118**. Pitman (Advanced Publishing Program), Boston, MA, 1985.

[8] G. G. Dandapat, J. L. Hunsucker and Carl Pomerance. Some new results on odd perfect numbers. *Pacific J. Math.* **57** (1975), 359–364.

[9] Joseph DiMuro. On prime power order elements of general linear groups. *J. Algebra* **367** (2012), 222–236.

[10] D. S. Dummit and R. M. Foote. *Abstract algebra*. Third edition. Wiley & Sons, 2004. xii+932.

[11] W. Feit. On large Zsigmondy primes. *Proc. Amer. Math. Soc.* **102** (1988), 29–36.

[12] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.7.7; 2015, `http://www.gap-system.org`

[13] S. P. Glasby. Supporting GAP and MAGMA code, `http://www.maths.uwa.edu.au/~glasby/RESEARCH`

[14] R. Guralnick, T. Penttila, C. E. Praeger and J. Saxl. Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc.* **78** (1999), 167–214.

[15] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata* **2** (1974), 425–460.

[16] G. D. James. On the minimal dimensions of irreducible representations of symmetric groups. *Math. Proc. Cambridge Philos. Soc.* **94** (1983), 417–424.
[17] Lenstra-Pomerance-Wagstaff Conjecture, `http://primes.utm.edu/mersenne/heuristic.html`.
[18] Heinz Lüneburg. Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $A^N - 1$. [A simple proof of Zsigmondy's theorem on primitive prime divisors of $A^N - 1$.] *Geometries and groups* (Berlin, 1981), pp. 219–222.
[19] Alice C. Niemeyer and Cheryl E. Praeger. A recognition algorithm for classical groups over finite fields. *Proc. London Math. Soc.* **77** (1998), 117–169.
[20] P. Ribenboim. The little book of big primes. Springer, 1991.
[21] Moshe Roitman. On Zsigmondy primes. *Proc. Amer. Math. Soc.* **125** (1997), 1913–1919.
[22] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatshefte für Mathematik* **3** (1892), 265–284.

S. P. Glasby, Centre for Mathematics of Symmetry and Computation, University of Western Australia; also affiliated with The Department of Mathematics, University of Canberra. `GlasbyS@gmail.com` `http://www.maths.uwa.edu.au/~glasby/`

Frank Lübeck, Lehrstuhl D für Mathematik, RWTH Aachen University, Templergraben 64, 52062 Aachen, Germany. `Frank.Luebeck@Math.RWTH-Aachen.De`
`http://www.math.rwth-aachen.de/~Frank.Luebeck/`

Alice C. Niemeyer, Department of Mathematics and Statistics, NUI Maynooth, Ireland. `Alice.Niemeyer@nuim.ie`

Cheryl E. Praeger, Centre for Mathematics of Symmetry and Computation, University of Western Australia; also affiliated with King Abdulaziz University, Jeddah, Saudi Arabia. `Cheryl.Praeger@uwa.edu.au` `http://www.maths.uwa.edu.au/~praeger`