J. Group Theory **21** (2018), 667–694
DOI 10.1515/jgth-2018-0012

Primary cyclic matrices in irreducible matrix subalgebras

Brian P. Corr and Cheryl E. Praeger

Communicated by Timothy C. Burness

Abstract. Primary cyclic matrices were used (but not named) by Holt and Rees in their version of Parker's MEAT-AXE algorithm to test irreducibility of finite matrix groups and algebras. They are matrices X with at least one cyclic component in the primary decomposition of the underlying vector space as an X-module. Let $\mathrm{M}(c, q^b)$ be an irreducible subalgebra of $\mathrm{M}(n, q)$, where $n = bc > c$. We prove a generalisation of the Kung–Stong cycle index theorem, and use it to obtain a lower bound for the proportion of primary cyclic matrices in $\mathrm{M}(c, q^b)$. This extends work of Glasby and the second author on the case $b = 1$.

1 Introduction

In order to improve and generalise the MEAT-AXE algorithm of Richard Parker [14], Holt and Rees [10] suggested the use of a family of matrices defined as follows: an $n \times n$ matrix X over a field $F = \mathrm{GF}(q)$ is *primary cyclic* if, for some irreducible polynomial f over F, the nullspace of $f(X)$ in $V(n, q) = F^n$ is an irreducible FX-submodule (see also Definition 2.3).

Given a group $G \leqslant \mathrm{GL}(n, F)$ acting on $V = F^n$, the irreducibility test in the MEAT-AXE algorithm, originally due to Simon Norton, tests whether or not G leaves invariant a proper nontrivial subspace of V. The version of the test used by Holt and Rees in [10] does so by randomly searching for primary cyclic matrices and analysing their actions on V: for the analysis it is crucial to know how abundant primary cyclic matrices are.

Holt and Rees in [10, pp. 7–8] obtain a positive constant lower bound on the proportion of primary cyclic matrices in the full matrix algebra $\mathrm{M}(n, F)$, and in [7] Glasby and the second author show that the proportion of primary cyclic matrices in $\mathrm{M}(n, F)$ lies in the interval $(1 - \frac{c_1}{q^n}, 1 - \frac{c_2}{q^n})$ for positive constants c_1, c_2. Here we focus on irreducible proper subalgebras of $\mathrm{M}(n, F)$: any such subalgebra can be identified with the full matrix algebra $\mathrm{M}(c, K)$ over some extension field

The first author was supported by an Australian Postgraduate Award and UWA Top-Up Scholarship. This research forms part of Australian Research Council project DP110101153.

$K = \mathrm{GF}(q^b)$, where $n = bc$ (see Section 2). We prove an analogous result to the Holt–Rees estimate for these subalgebras.

We treat the case of fixed degree extensions $\mathrm{GF}(q^b)$ of a field of fixed size q as the dimension $n = bc$ grows unboundedly. Let $P_M(c, q^b)$ be the proportion of matrices in $\mathrm{M}(c, q^b)$ which are primary cyclic in $\mathrm{M}(n, q)$ relative to some irreducible polynomial f of degree b over F (the minimal possible degree of such an f): then $P_M(c, q^b)$ is a lower bound for the proportion of primary cyclic matrices in $\mathrm{M}(c, q^b)$.

Theorem 1.1. *Let q be a prime power, and b, c positive integers with $b > 1$. Then*

(i) $\lim_{c\to\infty} P_M(c, q^b)$ *exists and equals*

$$P_M(\infty, q^b) := \lim_{c\to\infty} P_M(c, q^b) = 1 - \left(1 - \frac{bq^{-b}}{(1-q^{-b})^2}\omega(1, q^b)^b\right)^{N(q,b)}$$

where $\omega(1, q^b) = \prod_{i=1}^{\infty}(1 - q^{-bi})$ and $N(q, b)$ is the number of monic irreducible polynomials of degree b over F_q; and

(ii) *there exists a constant $k(q, b)$ such that, if $c \geq (\frac{\max\{b-1, q^b/b\}}{\log(3/4)})^2$, then*

$$|P_M(c, q^b) - P_M(\infty, q^b)| < k(q, b)q^{-bc}.$$

Remark 1.2. (i) To prove Theorem 1.1, we use generating functions and in particular, we obtain a new generalisation in Theorem 3.6 of the Kung–Stong cycle index theorem (see [11, 16]).

(ii) Theorem 1.1 shows that, for fixed q, b, the quantity $P_M(c, q^b)$ approaches its limiting value exponentially quickly. However the expression for the limit is rather complicated. We study the behaviour of the limiting value as q^b grows, and prove (in Proposition 5.5) that the limit as q^b approaches infinity of $P_M(\infty, q^b)$ exists and equals

$$\lim_{q^b\to\infty} P_M(\infty, q^b) = 1 - e^{-1}.$$

This is analogous to the original Holt–Rees estimate in [10] for the case $b = 1$.

(iii) We prove Theorem 1.1 (ii) with the following value for the quantity $k(q, b)$:

$$k(q, b) = \frac{8}{3(1-q^{-b})}\left(\frac{bq^b}{q^b - 1}2^{2b}q^{2b^2}\right)^{q^b/b}$$

(see Proposition 5.10). We believe that this may be far from the best value.

(iv) A different subfamily of primary cyclic matrices was studied in [3], namely the set of all f-primary cyclic matrices $X \in \mathrm{M}(c, q^b)$ for irreducible polynomials

f of degree strictly greater than half the rank of X. In [3, Theorem 1.4], an explicit lower bound is given for the proportion of such primary cyclic matrices in $\mathrm{M}(c, q^b)$ as a function of q, b and c. For large b, c the bound is close to $\log_e 2$.

In Section 2 we present essential results on minimal and characteristic polynomials. In Section 3 we prove the generalisation of the Kung–Stong cycle index theorem and apply it to estimating the proportion of primary cyclic matrices in $\mathrm{M}(c, q^b)$. Section 4 deals with asymptotics and introduces a generating function crucial for the proof of Theorem 1.1. Then in Section 5 we complete the proof of Theorem 1.1, and discuss how to use it.

A consequence of Theorem 1.1 is that, for sufficiently large c, an explicit lower bound on the proportion of primary cyclic matrices can be calculated. Computationally we determine the proportion exactly for small c, see for example, Table 1: combining these two methods, we may address all values of n, so long as the field size q^b is bounded.

2 Preliminaries

We first introduce some notation. Let F be a field of order q and let K be an extension field of F of degree b. The *Galois group* $G = \mathrm{Gal}(K/F) \leqslant \mathrm{Aut}\, K$ is cyclic of order b, generated by the Frobenius automorphism $\sigma_0 : x \mapsto x^q$, and has the subfield F as its fixed point set.

Let $V = F^n$ denote the space of n-dimensional row vectors over F, with standard basis $\{e_1, \ldots, e_n\}$, and let $\mathrm{M}(n, q)$ denote the full endomorphism ring of V, with elements written as $n \times n$ matrices with entries in F relative to the standard basis. For a divisor b of n (say $n = bc$), we can embed the algebra $\mathrm{M}(c, q^b)$ as an irreducible subalgebra of $\mathrm{M}(n, q)$ as follows. The extension field K is an F-vector space of dimension b, having as a basis $\{1, \omega, \omega^2, \ldots, \omega^{b-1}\}$, where ω is a primitive element of K. If $\{v_1, \ldots, v_n\}$ is a basis for $V(c, q^b) = K^c$, then $\{\omega^i v_j \mid 0 \leq i \leq b-1, 1 \leq j \leq c\}$ is an F-basis for $V(c, q^b)$ as an n-dimensional F-vector space, where $n = bc$, and the mapping $\varphi : \omega^i v_j \mapsto e_{(j-1)b+i+1}$ extends linearly to an F-vector space isomorphism from $V(c, q^b) = K^c$ to V.

Each $X \in \mathrm{M}(c, q^b)$ defines an F-endomorphism of $V(c, K)$, and so we have an action of $\mathrm{M}(c, q^b)$ on $V = F^n$ defined by

$$(v)X^\varphi := v\varphi^{-1} X \varphi,$$

for $v \in V$. Thus $X \mapsto X^\varphi$ defines an F-algebra monomorphism $\mathrm{M}(c, q^b) \to \mathrm{M}(n, q)$, and we may identify $\mathrm{M}(c, K)$ with its image. This image is an *irreducible* F-subalgebra of $\mathrm{M}(n, q)$, and each irreducible subalgebra arises in this way (by Schur's lemma, see for example [4]).

Throughout we will have to consider interchangeably the actions of a matrix in $\mathrm{M}(c, q^b)$ on *two* vector spaces, F^n and K^c. For this reason we introduce notation to help keep track of which field we are dealing with.

Notation 2.1. (i) Let V be the vector space K^c of c-dimensional row vectors over $K = \mathrm{GF}(q^b)$, with $n = bc$. Then, as an F-vector space, V is isomorphic, via φ as defined above, to the vector space F^n. We denote this F-vector space by V_F. If there is any ambiguity we use V_K to denote the K-vector space V. An element X of $M(c, q^b)$ thus acts as a linear transformation of V_F in a natural way (via the maps above): again we use the notation X_F to denote the action of X on V_F (and similarly X_K to denote the action on V_K if there may be ambiguity).

(ii) We denote by $F[t]$, $\mathrm{Irr}(q)$ and $\mathrm{Irr}(q, d)$ (where $d \geq 0$) the ring of polynomials over F, the set of monic irreducible polynomials over F, and the set of monic irreducibles of degree d over F, respectively. Let $N(q, d) = |\mathrm{Irr}(q, d)|$. Denote the characteristic and minimal polynomials of X_F by $c_{X,F}(t)$, $m_{X,F}(t)$, respectively, and similarly define $K[t]$, $\mathrm{Irr}(q^b, d)$, $N(q^b, d)$ and $c_{X,K}(t)$, $m_{X,K}(t)$ for the X-action on $V_K = K^c$.

(iii) The Galois group $G = \mathrm{Gal}(K/F)$ acts faithfully on $K[t]$ and $\mathrm{M}(c, q^b)$ by acting on the coefficients of a polynomial and the entries of a matrix, respectively. The fixed points of G in these actions are respectively $F[t]$ and $\mathrm{M}(c, q)$.

(iv) If U is an X-invariant F-subspace of V, then we denote by $X|_U$ the restriction of X to U; if in addition U is a K-subspace, then we may write $(X|_U)_F$ and $(X|_U)_K$ if we wish to emphasise the field.

Definition 2.2. Let $X \in \mathrm{M}(n, q)$ and let $m_{X,F} = \prod_{i=1}^{r} f_i^{\alpha_i}$, with each $f_i \in \mathrm{Irr}(q)$ and $\alpha_i > 0$. A useful X-invariant decomposition of V_F is the *X-primary decomposition* (see [9, Theorem 11.8])

$$V_F = V_{f_1} \oplus \cdots \oplus V_{f_r},$$

where the subspace V_{f_i} is called the *f_i-primary component* of X (on V), and has the property that f_i does not divide the minimal polynomial of the restriction of X to $\bigoplus_{j \neq i} V_{f_j}$, and the minimal polynomial of $X|_{V_{f_j}}$ is $f_i^{\alpha_i}$. Let

$$\mathrm{Div}_F(X) := \{f_1, \ldots, f_k\}.$$

If $f \in \mathrm{Irr}(q) \setminus \mathrm{Div}_F(X)$, we say that the f-primary component is trivial and define $V_f = \{0\}$.

We also define $\mathrm{Div}_K(X)$ and the X_K-primary decomposition of V_K similarly.

Definition 2.3. Let $X \in \mathrm{M}(n,q)$ and $f \in \mathrm{Irr}(q)$. Then X is called *f-primary cyclic* if $X|_{V_f}$ is nontrivial and cyclic. Also, X is called *cyclic* if X is f-primary cyclic for all $f \in \mathrm{Div}_F(X)$, or equivalently, if $m_{X,F} = c_{X,F}$. We also say that X is *primary cyclic* if it is f-primary cyclic for some $f \in \mathrm{Irr}(q)$. We note that X is f-primary cyclic if and only if the nullspace $\mathrm{Null}\, f(X)$ is an irreducible FX-submodule of V.

2.1 Minimal and characteristic polynomials

We aim to count matrices X in the subalgebra $\mathrm{M}(c, q^b)$ of $\mathrm{M}(n,q)$ such that X_F is primary cyclic. To do so we derive necessary and sufficient conditions for this property which are intrinsic to their action on K^c: that is to say, conditions on X_K. Our analysis follows that of [13, Section 5].

We investigate the relationship between the characteristic and minimal polynomials of a matrix X over the two different fields F and K. We call two polynomials g, g' in $K[t]$ *conjugate* if there exists $\sigma \in G = \mathrm{Gal}(K/F)$ such that $g^\sigma = g'$. Recall Notation 2.1.

Lemma 2.4. *Let $f \in \mathrm{Irr}(q,d)$, let $b \geq 2$, and let $G = \langle \sigma_0 \rangle = \mathrm{Gal}(K/F)$. Suppose that $g \in \mathrm{Irr}(q^b)$ is a divisor of f in $K[t]$. Then the following hold:*

(i) $\deg g = d/\gcd(b,d)$;

(ii) $f = \mathrm{lcm}\{g^{\sigma_0^{i-1}} \mid 1 \leq i \leq b\} = \prod_{i=1}^{\gcd(b,d)} g^{\sigma_0^{i-1}}$;

(iii) $g = g^{\sigma_0^i}$ *if and only if* $i \equiv 0 \pmod{\gcd(b,d)}$;

(iv) f *is the unique element of* $\mathrm{Irr}(q)$ *divisible by g in $K[t]$.*

Proof. Part (i) follows immediately from [12, Theorem 3.46]. For (ii) and (iii), observe that since σ_0 fixes the field F, the image g^{σ_0} divides $f^{\sigma_0} = f$, and similarly, for every i we have $g^{\sigma_0^i} \mid f$, so

$$\mathrm{lcm}\{g^{\sigma_0^{i-1}} \mid 1 \leq i \leq b\} \text{ divides } f.$$

Since the set $\{g^{\sigma_0^{i-1}} \mid 1 \leq i \leq b\}$ is permuted under the action of σ_0, its least common multiple is fixed by σ_0, and so lies in $F[t]$. Then by the irreducibility of f, they are equal.

Since $\deg f = d = \gcd(b,d) \deg g$, it follows that $\{g^{\sigma_0^{i-1}} \mid 1 \leq i \leq b\}$ has size $\gcd(b,d)$, and the stabiliser of each $g^{\sigma_0^{i-1}}$ in G is $\langle \sigma_0^{\gcd(b,d)} \rangle$. This implies part (iii) and the last assertion of (ii). Part (iv) follows from part (ii). □

We now give a description of f-primary cyclic matrices in terms of their representations over the field K. The following result is derived from [13, Lemma 5.1 and Corollary 5.2]. Recall the notation for minimal polynomials from Notation 2.1.

Proposition 2.5. *Let $f \in \mathrm{Irr}(q,d)$, let $G = \mathrm{Gal}(K/F)$, and let $X \in \mathrm{M}(c,q^b)$ such that $f \in \mathrm{Div}_F(X)$. Then X_F is f-primary cyclic if and only if $b \mid d$ and the following hold for some irreducible divisor $g \in K[t]$ of f of degree d/b:*

(i) *$g \in \mathrm{Div}_K(X)$ and X_K is g-primary cyclic; and*

(ii) *for each nontrivial $\sigma \in G$, the conjugate $g^\sigma \neq g$ and $g^\sigma \notin \mathrm{Div}_K(X)$.*

Proof. By [13, Lemma 5.1],

$$m_{X,F} = \mathrm{lcm}\{m_{X,K}^\sigma \mid \sigma \in G\}. \tag{2.1}$$

If $g \in \mathrm{Irr}(q^b)$ divides f, then, by Lemma 2.4 (ii), f is the product of the distinct conjugates of g by elements of G. Since $f \mid m$, it follows from (2.1) that $m_{X,K}$ is divisible by at least one conjugate of g. Without loss of generality $g \mid m_{X,K}$. Note that, by Lemma 2.4 (ii), $f = \mathrm{lcm}\{g^\sigma \mid \sigma \in G\}$. Consider the following X_K-invariant decomposition of $V = V_K$:

$$V_K = V_0 \oplus V_1,$$

where V_0 is the sum of the g^σ-primary components of V, for $\sigma \in G$, and V_1 is the sum of the other primary components. Let $Y_i = X|_{V_i}$ for $i = 0, 1$. Then $g \mid m_{Y_0,K}$, and the only irreducible divisors of $m_{Y_0,K}$ are g^σ for certain $\sigma \in G$. Also $m_{Y_1,K}$ is coprime to $\mathrm{lcm}\{g^\sigma \mid \sigma \in G\} = f$. By [13, Lemma 5.1] applied to Y_0 acting on V_0, we have $m_{Y_0,F} = \mathrm{lcm}\{m_{Y_0,K}^\sigma \mid \sigma \in G\}$, and it follows from Lemma 2.4 (iv), that f is the only irreducible divisor of $m_{Y_0,F}$. Thus V_0 is the f-primary component of V_F.

By definition, X_F is f-primary cyclic if and only if $(Y_0)_F$ is cyclic (hence with minimum polynomial $m_{Y_0,F} = f$). By [13, Corollary 5.2] applied to Y_0, this holds if and only if (i) $(Y_0)_K$ is cyclic, and (ii) $m_{Y_0,K}$ is coprime with $m_{Y_0,K}^\sigma$ for all nontrivial $\sigma \in G$. Recall that $g \mid m_{Y_0,K}$ and $g^\sigma \nmid m_{Y_1,K}$ for all $\sigma \in G$. Thus condition (ii) is equivalent to (ii)′ $m_{Y_0,K} = g^k$ for some positive integer k and, for all nontrivial $\sigma \in G$, $g^\sigma \neq g$ and $g^\sigma \nmid m_{X,K}$. The first assertion of (ii)′ holds if and only if V_0 is the g-primary component of X_K. By Lemma 2.4 (iii), the second assertion in (ii)′ holds if and only if $b \mid d$, $\deg g = d/b$, and $g^\sigma \nmid m_{X,K}$ for all nontrivial $\sigma \in G$. Also if $(Y_0)_K$ is cyclic with minimal polynomial g^k, then k must be 1. Thus both of the conditions (i) and (ii) hold if and only if $b \mid d$, $\deg g = d/b$, X_K is g-primary cyclic, and $g^\sigma \neq g$ and $g^\sigma \nmid c_{X,K}$ for all nontrivial $\sigma \in G$ (recalling that $m_{X,K}$ and $c_{X,K}$ have the same set of irreducible divisors.) □

The next corollary follows immediately from Lemmas 2.5 and 2.4 (iii).

Corollary 2.6. *Let $X \in \mathrm{M}(c, q^b) \subseteq \mathrm{M}(n, q)$, where $n = bc$, let $G = \mathrm{Gal}(K/F)$, and let $I = \{f_1, \ldots, f_k\} \subset \mathrm{Irr}(q, b)$. Then X_F is f_i-primary cyclic, for every $i \leq k$, if and only if there exists a set $I' = \{g_1, \ldots, g_k\} \subseteq \mathrm{Irr}(q^b, 1)$ with $|I'| = k$ satisfying the following for each $i \in \{1, \ldots, k\}$:*

(i) *$g_i \mid f_i$, and X_K is g_i-primary cyclic;*

(ii) *for each nontrivial $\sigma \in G$, we have $g_i^\sigma \neq g_i$, and $g_i^\sigma \notin \mathrm{Div}_K(X)$.*

3 A generalised cycle index for matrix algebras

Our main tool in enumerating matrices is the cycle index of the matrix algebra $\mathrm{M}(n, q)$, introduced by Kung [11] and developed further by Stong [16], and based on Polya's cycle index (see for example [15]) of a permutation group. We continue to use Notation 2.1. To each pair (h, λ), with $h \in \mathrm{Irr}(q)$ and λ a partition of a nonnegative integer, denoted $|\lambda|$, with $|\lambda| \in [0, n]$, assign an indeterminate $x_{h,\lambda}$. Then the *cycle index* of $\mathrm{M}(n, q)$ is the multivariate polynomial

$$Z_{\mathrm{M}(n,q)}(\mathbf{x}) := \frac{1}{|\mathrm{GL}(n, q)|} \sum_{X \in \mathrm{M}(n,q)} \Big(\prod_{h \in \mathrm{Div}_F X} x_{h,\lambda(X,h)} \Big),$$

where $\mathbf{x}$ is a vector representing the set of indeterminates $x_{h,\lambda}$ occurring, and $\lambda(X, h)$ is a partition (of an integer) uniquely determined by the structure of the action of X on the primary component V_h as described in Definition 3.1 below.

In this section we generalise the cycle index of Kung and Stong to include variables associated with a finite number of irreducible polynomials which do not necessarily divide $c_{X,F}(t)$. We will apply this more general version in our study of primary cyclic matrices. We begin by presenting the original cycle index theorem. *In this section $V = F^c$ is viewed solely as an F-space, where, recall, $F = \mathrm{GF}(q)$.*

Definition 3.1. Let $X \in \mathrm{M}(n, q)$, $h \in \mathrm{Irr}(q)$, and let α_h be the multiplicity of h in $c_{X,F}(t)$, so that X acts on the h-primary component V_h of V_F with characteristic polynomial h^{α_h} and $\alpha_h \deg h = \dim(V_h)_F$. (In particular, $\alpha_h = 0$ if $V_h = 0$.) There is a direct sum decomposition of V_h into FX-submodules

$$V_h = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_r}$$

with each V_{λ_i} cyclic, such that the restriction of X to V_{λ_i} has minimal polynomial h^{λ_i}, and $\lambda_i \geq \lambda_{i+1}$ for all i. The λ_i are uniquely determined by X (see [9, Theorem 11.19]). Define the partition $\lambda(X, h)$ as the sequence

$$\lambda(X, h) := (\lambda_1, \lambda_2, \ldots, \lambda_r, 0, 0, \ldots).$$

Then $\lambda(X,h)$ is a partition of α_h, and as this partition is non-increasing, we often omit the 'trailing zeroes' and write $(\lambda_1,\ldots,\lambda_r)$ if $V_h \neq \{0\}$ and $() := (0,0,\ldots)$ (the empty partition of the integer zero) if $V_h = \{0\}$.

In particular, $\lambda(X,h) = ()$ if $h \notin \mathrm{Div}_F(X)$, and otherwise $\lambda(X,h)$ is determined by the sizes of the blocks in the Frobenius normal form of $X|_{V_h}$.

See [9] for more information on the cyclic and primary decompositions, and on $\lambda(X,h)$. Lemma 3.2 follows immediately from the definition of $\lambda(X,h)$:

Lemma 3.2. *Let $X \in \mathrm{M}(n,q)$, $h \in \mathrm{Irr}(q)$, and $\lambda = \lambda(X,h)$. Then the following hold:*

(i) *$h \notin \mathrm{Div}_F(X)$ if and only if $\lambda(X,h) = ()$;*

(ii) *$h \in \mathrm{Div}_F(X)$ and X is h-primary cyclic if and only if $\lambda(X,h) = (\lambda_1)$, with $\lambda_1 > 0$, and in this case λ_1 is the multiplicity of h in $c_{X,F}(t)$;*

(iii) *$h \in \mathrm{Div}_F(X)$ and X is not h-primary cyclic if and only if $\lambda(X,h)$ has at least two nonzero parts.*

Definition 3.3. Let λ be a partition of an integer $|\lambda|$, let $h \in \mathrm{Irr}(q)$, and let $s = |\lambda| \deg h$. If $\lambda = ()$, define $c(\lambda, \deg h, q) = 1$. If $|\lambda| \geq 1$, then there exists a matrix $X := X_{\lambda,h} \in \mathrm{M}(s,q)$ such that $c_{X,F}(t) = h^{|\lambda|}$, and the cyclic decomposition of F^s described in Definition 3.1 determines the partition λ. In this case we define

$$c(\lambda, \deg h, q) := |C_{\mathrm{GL}(s,q)}(X)|.$$

Note that $c(\lambda, \deg h, q)$ (the number of matrices in $\mathrm{GL}(s,q)$ which commute with X) depends only on $\deg h$ and λ, since all matrices X with these properties are conjugate under elements of $\mathrm{GL}(s,q)$ (see again [9, Theorem 11.19]). The number of such matrices X is $|\mathrm{GL}(s,q)|/c(\lambda, \deg h, q)$, and this holds also for $\lambda = ()$ if we take $\mathrm{GL}(0,q)$ as the trivial group. The Kung–Stong cycle index theorem is stated in terms of these quantities.

Theorem 3.4 (Cycle index theorem). *The generating function for the cycle index of a matrix algebra $\mathrm{M}(n,q)$ satisfies*

$$1 + \sum_{n=1}^{\infty} Z_{M(n,q)}(\mathbf{x}) u^n = \prod_{h \in \mathrm{Irr}(q)} \left(1 + \sum_{\lambda \neq ()} x_{h,\lambda(h)} \frac{u^{|\lambda| \deg h}}{c(\lambda, \deg h, q)}\right).$$

Theorem 3.4 assigns to each $X \in \mathrm{M}(n,q)$ a monomial $\prod_{h \in \mathrm{Div}_F X} x_{h,\lambda(X,h)}$, and sums over $\mathrm{M}(n,q)$. We generalise by forcing a certain finite collection of indeterminates to occur in the monomials for all matrices X, whether or not the

corresponding irreducibles divide $c_{X,F}(t)$. The reason for this generalisation will become apparent when we apply this to the proof of Lemma 4.4 in Section 4: it permits us to ask questions about whether some (fixed) $f \in \mathrm{Irr}(q)$ divides $c_{X,F}(t)$.

Definition 3.5. For a finite subset $I \subset \mathrm{Irr}(q)$, and partitions $\lambda(X,h)$ as in Definition 3.1 ($X \in \mathrm{M}(n,q)$, $h \in \mathrm{Irr}(q)$), the *I-cycle index* of $\mathrm{M}(n,q)$ is defined as

$$Z^{(I)}_{\mathrm{M}(n,q)}(\mathbf{x}) := \frac{1}{|\mathrm{GL}(n,q)|} \sum_{X \in \mathrm{M}(n,q)} \Big(\prod_{h \in \mathrm{Div}_F(X) \cup I} x_{h,\lambda(X,h)} \Big), \tag{3.1}$$

or equivalently

$$Z^{(I)}_{\mathrm{M}(n,q)}(\mathbf{x}) := \frac{1}{|\mathrm{GL}(n,q)|} \times \sum_{X \in \mathrm{M}(n,q)} \Big(\Big(\prod_{h \in \mathrm{Div}_F(X)} x_{h,\lambda(X,h)} \Big) \Big(\prod_{h \in I \setminus \mathrm{Div}_F(X)} x_{h,(\,)} \Big) \Big). \tag{3.2}$$

The Kung–Stong cycle index is precisely the I-cycle index with $I = \emptyset$. We now prove the I-cycle index theorem.

Theorem 3.6 (I-cycle index theorem). *For a finite subset $I \subseteq \mathrm{Irr}(q)$ and $\lambda(X,h)$, $c(\lambda, \deg h, q)$ as in Definitions* 3.1 *and* 3.3*, the generating function for the I-cycle index of $\mathrm{M}(n,q)$ satisfies*

$$\prod_{h \in I} x_{h,(\,)} + \sum_{n=1}^{\infty} Z^{(I)}_{M(n,q)}(\mathbf{x}) u^n = \prod_{h \in \mathrm{Irr}(q^b) \setminus I} \left(1 + \sum_{\lambda \neq (\,)} x_{h,\lambda} \frac{u^{|\lambda| \deg h}}{c(\lambda, \deg h, q)} \right) \times \prod_{h \in I} \left(x_{h,(\,)} + \sum_{\lambda \neq (\,)} x_{h,\lambda} \frac{u^{|\lambda| \deg h}}{c(\lambda, \deg h, q)} \right). \tag{3.3}$$

Proof. Our proof follows that of Stong in [16]. We consider the quantities in (3.3) as power series in the variables $x_{h,\lambda}$, and treat u as a constant. Note that since I is finite, and for $X \in \mathrm{M}(n,q)$ the set $\mathrm{Div}_F X$ is finite, each $Z^{(I)}_{\mathrm{M}(n,q)}(\mathbf{x})$ on the left-hand side of (3.3), when expressed as in (3.2), is clearly a sum of products of finitely many of the $x_{h,\lambda}$. Recall that $c((\,), \deg h, q) = 1$ for all $h \in \mathrm{Irr}(q)$, and so

$$x_{h,(\,)} = x_{h,(\,)} \frac{u^{0 \cdot \deg h}}{c((\,), \deg h, q)}.$$

Let $\{h_i \mid 1 \leq i \leq t\} \subseteq \mathrm{Irr}(q)$, and let $\{\lambda_i \mid 1 \leq i \leq t\}$ be a multiset of partitions such that λ_i may be $(\,)$ if $h_i \in I$, and otherwise $\lambda_i \neq (\,)$. For each i, let $n_i = |\lambda_i| \deg h_i$, and let $n = \sum_{i=1}^{t} n_i$. The coefficient of $\prod_{i=1}^{t} x_{h_i,\lambda_i}$ on the right-hand

side of (3.3) is

$$\left(\prod_{i=1}^{t}\frac{1}{c(\lambda_i,\deg h_i,q)}\right)u^n. \tag{3.4}$$

On the other hand, the coefficient of $\prod_{i=1}^{n} x_{h_i,\lambda_i}$ on the left-hand side of (3.3) is equal to 1 if $n=0$, and otherwise is $u^n/|\mathrm{GL}(n,q)|$ times the number of matrices $X\in \mathrm{M}(n,q)$ having characteristic polynomial $\prod_{i=1}^{t} h_i^{|\lambda_i|}$, with $\lambda(X,h_i)=\lambda_i$ for each i. Each of these matrices X is uniquely determined by the following data:

(i) its primary decomposition $V=V_{h_1}\oplus\cdots\oplus V_{h_n}$ is such that $\dim V_{h_i}=n_i$, noting that we may have $\lambda(X,h_i)=()$ if $h_i\in I$; and

(ii) for each primary component V_{h_i}, the partition $\lambda_i=\lambda(X_{h_i},h_i)$.

There are exactly

$$\frac{|\mathrm{GL}(n,q)|}{\prod_{i=1}^{n}|\mathrm{GL}(n_i,q)|}$$

direct sum decompositions of V with the appropriate dimensions, and on each of the parts V_{h_i}, there are exactly $|\mathrm{GL}(n_i,q)|/c(\lambda_i,\deg h_i,q)$ matrices X_{h_i} such that $\lambda(X_{h_i},h_i)=\lambda_i$, as noted in Definition 3.3. Thus the coefficient of $\prod_{i=1}^{t} x_{h_i,\lambda_i}$ on the left-hand side of (3.3) is

$$\begin{aligned}\frac{u^n}{|\mathrm{GL}(n,q)|}\cdot\frac{|\mathrm{GL}(n,q)|}{\prod_{1\le i\le t}|\mathrm{GL}(n_i,q)|}\cdot\prod_{1\le i\le t}\frac{|\mathrm{GL}(n_i,q)|}{c(\lambda_i,\deg h_i,q)}\\ =\prod_{1\le i\le t}\frac{1}{c(\lambda_i,\deg h_i,q)}u^n,\end{aligned}$$

which equals (3.4). □

4 Counting

By evaluating (3.3) in Theorem 3.6 at different values of $\mathbf{x}$, we can enumerate subsets of $\mathrm{M}(c,q^b)$ having certain properties based on their minimal polynomials. In particular, we wish to count matrices in $\mathrm{M}(c,q^b)\subseteq\mathrm{M}(n,q)$ which are f-primary cyclic for some $f\in\mathrm{Irr}(q,b)$ (recall that by Proposition 2.5, b is the smallest degree for which such f-primary matrices exist). We begin this section by introducing some quantities which will simplify our rather complicated calculations.

Note that while the I-cycle index theorem was presented for the full matrix algebra $\mathrm{M}(n,q)$, it may be applied directly to the irreducible subalgebra $\mathrm{M}(c,q^b)$, provided that we treat $\mathrm{M}(c,q^b)$ in its own right, rather than as a subalgebra of $\mathrm{M}(bc,q)$.

Definition 4.1. Define the following quantities:

$$\omega_n(u,q) := \prod_{i=1}^{n}(1-uq^{-i}) \qquad \text{for } \{u \in \mathbb{C} : |u| < q\};$$

$$\omega(u,q) := \prod_{i=1}^{\infty}(1-uq^{-i}) \qquad \text{for } \{u \in \mathbb{C} : |u| < q\};$$

$$G(u,q,n) := 1 + \sum_{\lambda \neq ()} \frac{u^{|\lambda|}}{c(\lambda,n,q)} \qquad \text{for } \{u \in \mathbb{C} : |u| < 1\};$$

$$P(u,q) := 1 + \sum_{n=1}^{\infty} \frac{u^n}{\omega_n(1,q)} \qquad \text{for } \{u \in \mathbb{C} : |u| < 1\};$$

$$S(u,q) := \sum_{n=1}^{\infty} \frac{u^n}{q^n(1-q^{-1})} \qquad \text{for } \{u \in \mathbb{C} : |u| < q\};$$

where $c(\lambda,n,q)$ is as in Definition 3.3. Note that

$$\omega_n(1,q) = \frac{|\mathrm{GL}(n,q)|}{|\mathrm{M}(n,q)|},$$

and that $\omega(1,q) = \lim_{n\to\infty}|\mathrm{GL}(n,q)|/|\mathrm{M}(n,q)|$ exists.

These definitions simplify our rather complicated calculations later. The following results will be used to manipulate the generating functions:

Lemma 4.2. *The following relations hold between the quantities in Definition* 4.1*, for* $|u| < 1$*, and in case* (4.3) *for* $|u| < q$*:*

$$G(u,q,1) = P(uq^{-1},q); \tag{4.1}$$

$$\prod_{h\in \mathrm{Irr}(q)} G(u^{\deg h},q,\deg h) = P(u,q); \tag{4.2}$$

$$P(u,q) = \frac{1}{1-u}P(uq^{-1},q) = \prod_{i=0}^{\infty}(1-uq^{-i})^{-1}; \tag{4.3}$$

$$S(u,q^b) = \frac{1}{(q^b-1)}\frac{u}{(1-uq^{-b})}; \tag{4.4}$$

Proof. (4.1): In equation (3.3) set $I = \emptyset$, and for all λ, set $x_{h,\lambda} = 0$ if $h \neq t-1$ and $x_{t-1,\lambda} = 1$. Using (3.1), we see that the right-hand side of (3.3) is equal to

$G(u, q, 1)$, while the left-hand side is

$$1 + \sum_{n=1}^{\infty} u^n \cdot \left(\frac{\#\text{ unipotent elements in } \mathrm{M}(n, q)}{|\mathrm{GL}(n, q)|} \right)$$

which by Steinberg's theorem [2, Theorem 6.6.1] is equal to

$$1 + \sum_{n=1}^{\infty} \frac{u^n q^{n(n-1)}}{|\mathrm{GL}(n, q)|} = P(uq^{-1}, q).$$

(4.2): The left-hand side of equation (4.2) is equal to the right-hand side of (3.3) if we set $I = \emptyset$ and all the $x_{h,\lambda} = 1$. Thus by (3.3), using also (3.1) and Definition 4.1, this is equal to

$$1 + \sum_{n=1}^{\infty} \frac{|\mathrm{M}(n, q)|}{|\mathrm{GL}(n, q)|} u^n = P(u, q).$$

(4.3): In [1, p. 19] we find the equality, for $|u| < q$,

$$\prod_{r=1}^{\infty} (1 - uq^{-r})^{-1} = 1 + \sum_{n=1}^{\infty} \frac{u^n q^{n(n-1)/2}}{\prod_{i=1}^{n} (q^i - 1)},$$

the right-hand side of which is equal to $P(uq^{-1}, q)$. This proves the second equality of (4.2), and the first equality follows on substituting u for uq^{-1} into the second equality.

(4.4): This is a routine geometric series calculation. □

Definition 4.3. Noting that $\mathrm{Irr}(q, b)$ is a finite set,

(i) for a nonempty subset $I \subseteq \mathrm{Irr}(q, b)$, define

$$\mathrm{pcbI}(I, c, q^b) := \left\{ X \in \mathrm{M}(c, q^b) \mid X_F \text{ is } f\text{-primary cyclic for all } f \in I \right\};$$

(ii) define

$$\mathrm{pcb}(c, q^b) := \bigcup_{\substack{I \subseteq \mathrm{Irr}(q,b) \\ I \neq \emptyset}} \mathrm{pcbI}(I, c, q^b);$$

so $P_M(c, q^b) = |\mathrm{pcb}(c, q^b)|/|M(c, q^b)|$;

(iii) for nonempty $I \subseteq \mathrm{Irr}(q,b)$, define generating functions for pcbI and pcb:

$$\mathrm{PCBI}(I,u,q^b) := 1 + \sum_{c=1}^{\infty} \frac{|\mathrm{pcbI}(I,c,q^b)|}{|\mathrm{GL}(c,q^b)|}u^c,$$

$$\mathrm{PCB}(u,q^b) := 1 + \sum_{c=1}^{\infty} \frac{|\mathrm{pcb}(c,q^b)|}{|\mathrm{GL}(c,q^b)|}u^c.$$

Note that $\mathrm{pcb}(c,q^b)$ is the set of matrices $X \in \mathrm{M}(c,q^b)$ such that X_F is f-primary cyclic for some $f \in \mathrm{Irr}(q,b)$: hence the name '**p**rimary **c**yclic, degree **b**'. Our end goal is to find and investigate $\mathrm{PCB}(u,q^b)$: to do so we compute a formula for $\mathrm{PCBI}(I,u,q^b)$, depending only on the size of I and the parameters q,b, and a relationship between the functions PCB, PCBI.

Lemma 4.4. *Let $I = \{f_1,\ldots,f_k\} \subseteq \mathrm{Irr}(q,b)$, with $|I| = k$. Then for the generating function* $\mathrm{PCBI}(I,u,q^b)$ *as in Definition* 4.3 *and $|u| < 1$, we have*

$$\mathrm{PCBI}(I,u,q^b) = P(u,q^b)H(u,q^b)^k,$$

where $H(u,q^b) := bP(u,q^b)^{-b}(1-u)^{-b}S(u,q^b)$, with $P(u,q^b), S(u,q^b)$ as in Definition 4.1.

Proof. Let $G = \mathrm{Gal}(K/F)$. By Corollary 2.6, a matrix X_F is f_i-primary cyclic for all $i \in I$ if and only if there exists a subset $I' = \{g_1,\ldots,g_k\} \subseteq \mathrm{Irr}(q^b,1)$ with $|I'| = k$ such that, for each $i \leq k$, g_i divides f_i, the g_i-primary component of X_K is cyclic, and for $1 \neq \sigma \in G$, g_i^σ does not divide $m_{X,K}$. For such a subset I' and, for $h \in \mathrm{Irr}(q^b)$, set

$$x_{h,\lambda} = \begin{cases} 0 & \text{if } h \in I', \text{ and either } \lambda = (\,), \text{ or } \lambda \neq (|\lambda|,0,\ldots) \text{ with } |\lambda| > 0; \\ 0 & \text{if for some nontrivial } \sigma \in G,\ h^\sigma \in I'; \\ 1 & \text{if } h \in I',\ \lambda = (|\lambda|,0,\ldots) \text{ with } |\lambda| > 0, \text{ and } h^\sigma \notin I' \text{ for } 1 \neq \sigma \in G; \\ 1 & \text{if } h \notin \bigcup_{\sigma\in G}(I')^\sigma. \end{cases}$$

Let $X \in \mathrm{M}(c,q^b)$: then X contributes 1 to the I'-cycle index (3.1), evaluated at $\mathbf{x}$, if and only if, for every $g_i \in I'$, $\lambda(X,g_i) = (|\lambda|,0,\ldots)$, with $|\lambda| > 0$, and $\lambda(X,g_i^\sigma) = (\,)$ for all nontrivial $\sigma \in G$; and X contributes zero otherwise. This is precisely the set of matrices which, for every $g_i \in I'$ and nontrivial σ, are g_i-primary cyclic and $g_i^\sigma \nmid m_{X,K}(t)$.

Arguing as in the proof of Theorem 3.6 (and in particular noting (3.4)), the number of matrices X which contribute 1 to the I'-cycle index of $\mathrm{M}(c,q^b)$ is the same for each choice of the k-element set I'. There are b^k subsets I' corre-

sponding to a given k-subset $I \subseteq \mathrm{Irr}(q,b)$, and by Corollary 2.6, each member of $\mathrm{pcbI}(I,c,q^b)$ contributes 1 for exactly one of these subsets I'. Hence the number of $X \in \mathrm{M}(c,q^b)$ for which (3.1) evaluates to 1 with the above assignment of the $x_{h,\lambda}$ is therefore $|\mathrm{pcbI}(I,c,q^b)|/b^k$. Set $I^* = \bigcup_{\sigma\in G}(I')^\sigma$. Then since by Corollary 2.6 we have $g^\sigma \neq g$ for each $g \in I'$ and each nontrivial $\sigma \in G$, we have $|I^*| = bk$. Hence, by Theorem 3.6,

$$\mathrm{PCBI}(u,q^b) = b^k \prod_{h\in(\mathrm{Irr}(q^b)\setminus I^*)} \Bigg(1 + \sum_{\lambda\neq()} \frac{u^{|\lambda|\deg h}}{c(\lambda,\deg h,q^b)}\Bigg) \times \prod_{h\in I'} \Bigg(\sum_{\lambda=(|\lambda|,0,\ldots)\neq()} \frac{u^{|\lambda|\deg h}}{c(\lambda,\deg h,q^b)}\Bigg).$$

Now since every polynomial in I' is linear, and since by [7, Table 1] we have that $c((|\lambda|,0,\ldots),1,q^b) = q^{|\lambda|b}(1-q^{-b})$, it follows that

$$\prod_{h\in I'} \Bigg(\sum_{\lambda=(|\lambda|,0,\ldots)\neq()} \frac{u^{|\lambda|\deg h}}{c(\lambda,\deg h,q^b)}\Bigg) = \prod_{h\in I'} \Bigg(\sum_{\alpha=1}^{\infty} \frac{u^\alpha}{q^{\alpha b}(1-q^{-b})}\Bigg) = S(u,q^b)^k.$$

Then by Definition 4.1 and Lemma 4.2, and since $|I^*| = bk$,

$$\begin{aligned}
&\mathrm{PCBI}(u,q^b)\\
&= b^k S(u,q^b)^k \Big(\prod_{h\in(\mathrm{Irr}(q^b)\setminus I^*)} G(u^{\deg h},q^b,\deg h)\Big)\\
&= b^k S(u,q^b)^k \Big(\prod_{h\in\mathrm{Irr}(q^b)} G(u^{\deg h},q^b,\deg h)\Big)\Big(\prod_{h\in I^*} G(u,q^b,1)\Big)^{-1}\\
&= b^k S(u,q^b)^k P(u,q^b) P(uq^{-b},q^b)^{-bk}\\
&= b^k S(u,q^b)^k P(u,q^b)\big((1-u)P(u,q^b)\big)^{-bk}\\
&= P(u,q^b)\big(bS(u,q^b)(1-u)^{-b}P(u,q^b)^{-b}\big)^k
\end{aligned}$$

and the result follows. □

5 Combining results

The function $\mathrm{PCBI}(I,u,q^b)$ counts the number of elements of $\mathrm{M}(c,q^b)$ which are f-primary cyclic (when viewed as elements of the larger algebra $\mathrm{M}(bc,q)$) for all the irreducibles f in the k-subset $I \subseteq \mathrm{Irr}(q,b)$. We seek the proportion

of matrices which are f-primary cyclic for *some* $f \in \mathrm{Irr}(q,b)$. The inclusion-exclusion principle yields the following:

Theorem 5.1. *For any q, b, let $H(u,q^b) = bP(u,q^b)^{-b}(1-u)^{-b}S(u,q^b)$, where $S(u,q^b)$, $P(u,q^b)$ are as in Definition* 4.1*, and let $N = |\mathrm{Irr}(q,b)|$. Then*

$$\mathrm{PCB}(u,q^b) = P(u,q^b)\big(1-(1-H(u,q^b)^N\big).$$

Proof. Any $X \in \mathrm{M}(c,q^b)$ which is primary cyclic as an element of $\mathrm{M}(n,q)$, relative to some element of $\mathrm{Irr}(q,b)$, lies in $\mathrm{pcbI}(I,c,q^b)$ for at least one nonempty subset I of $\mathrm{Irr}(q,b)$. Thus for every positive integer c,

$$\mathrm{pcb}(c,q^b) = \bigcup_{\substack{I\subseteq \mathrm{Irr}(q,b)\\ I\neq\emptyset}} \mathrm{pcbI}(I,c,q^b),$$

and by the inclusion-exclusion principle, setting $N = |\mathrm{Irr}(q,b)|$,

$$|\mathrm{pcb}(c,q^b)| = \sum_{i=1}^{N}(-1)^{i+1}\Big(\sum_{I\subseteq \mathrm{Irr}(q,b),|I|=i} |\mathrm{pcbI}(I,c,q^b)|\Big).$$

By Lemma 4.4, the value of $|\mathrm{pcbI}(I,c,q^b)|$ depends only on $|I|$. Thus choosing an i-element subset I_i of $\mathrm{Irr}(q,b)$, we have

$$\sum_{I\subseteq \mathrm{Irr}(q,b),|I|=i} |\mathrm{pcbI}(I,c,q^b)| = \binom{N}{i}|\mathrm{pcbI}(I_i,c,q^b)|.$$

Hence

$$|\mathrm{pcb}(c,q^b)| = \sum_{i=1}^{N}(-1)^{i+1}\binom{N}{i}|\mathrm{pcbI}(I_i,c,q^b)|,$$

and a similar relationship holds for the generating functions:

$$\mathrm{PCB}(u,q^b) = \sum_{i=1}^{N}(-1)^{i+1}\binom{N}{i}|\mathrm{PCBI}(I_i,u,q^b)|.$$

Now by Lemma 4.4, writing $P = P(u,q^b)$ and $H = H(u,q^b)$, we have

$$\begin{aligned}\mathrm{PCB}(u,q^b) &= P\Big(\sum_{i=1}^{N}(-1)^{i+1}\binom{N}{i}PH^i\Big)\\ &= P\Big(1-\sum_{i=0}^{N}(-1)^i\binom{N}{i}H^i\Big)\\ &= P(1-(1-H)^N).\end{aligned}$$

□

c	$P_M(c, q^b)$
1	$1 - qq^{-b}$
2	$\frac{1}{2} + (\frac{3}{2} - \frac{b}{2})q^{-b} + (-\frac{b}{2} - q + \frac{bq}{2} - \frac{q^2}{2})q^{-2b}$ $+ (-1 + \frac{bq}{2} - \frac{q^2}{2})q^{-3b} + qq^{-4b}$
3	$\frac{2}{3} + (\frac{1}{3} - \frac{q}{2})q^{-b} + (\frac{4}{3} - \frac{b}{2} - \frac{b^2}{6} + q - \frac{bq}{2})q^{-2b}$ $+ (-\frac{1}{3} - \frac{b^2}{3} - \frac{bq}{2} + \frac{b^2q}{6} - q^2 + \frac{bq^2}{2} - \frac{q^3}{6})q^{-3b}$ $+ (-1 - \frac{b^2}{3} + \frac{q}{2} - bq + \frac{b^2q}{3} - q^2 + bq^2 - \frac{q^3}{3})q^{-4b}$ $+ (-1 + \frac{b}{2} - \frac{b^2}{6} - \frac{bq}{2} + \frac{b^2q}{3} + bq^2 - \frac{q^3}{3})q^{-5b}$ $+ (-\frac{bq}{2} + \frac{b^2q}{6} + q^2 + \frac{bq^2}{2} - \frac{q^3}{6})q^{-6b} + (1 + q^2)q^{-7b} - qq^{-8b}$

Table 1. The proportion $P_M(c, q^b)$ of f-primary cyclic matrices in a subalgebra $M(c, q^b)$ of $M(bc, q)$, relative to some $f \in \mathrm{Irr}(q, b)$. As q^b grows, $P_M(c, q^b)$ rapidly approaches a positive constant.

Theorem 5.1 shows us how to compute easily (using, e.g., *Mathematica* [17]) the Taylor coefficients of $\mathrm{PCB}(u, q^b)$, and hence values of $|\mathrm{pcb}(c, q^b)|/|\mathrm{M}(c, q^b)|$ for small c. We summarise some small cases in Table 1. The data suggests that the proportion has a nonzero constant term. If this were true in general, then for every triple (c, q, b) the proportion would be nontrivial. We use methods from complex analysis to examine the asymptotic behaviour as $c \to \infty$. The following fact can be found, for example, in [6, Lemma 1.3.3].

Lemma 5.2. *Suppose that* $g(u) = \sum a_n u^n$ *and* $g(u) = f(u)/(1-u)$ *for* $|u| < 1$. *If* $f(u)$ *is analytic with a radius of convergence* $R > 1$, *then* $a_n \to f(1)$ *as* $n \to \infty$, *and* $|a_n - f(1)| = O(d^{-n})$ *for any* $d < R$.

We apply this lemma to $\mathrm{PCB}(u, q^b)$ to obtain one of our main results:

Proof of Theorem 1.1 (i). By Lemma 5.1, writing $N = |\mathrm{Irr}(q, b)| = N(q, b)$,

$$\mathrm{PCB}(u, q^b) = P(u, q^b)\big(1 - (1 - H(u, q^b))^N\big).$$

Set $L(u, q^b) = (1-u)\,\mathrm{PCB}(u, q^b)$. By (4.3) and Definition 4.1 we have

$$L(u, q^b) = \omega(1, q^b)^{-1}\big(1 - (1 - H(u, q^b))^N\big).$$

Now by Lemma 4.2, writing $S = S(u, q^b)$ and $P = P(u, q^b)$ for brevity,

$$H(u, q^b) = bP^{-b}(1-u)^{-b}S = \frac{b}{q^b - 1}\,\frac{u}{1 - uq^{-b}}\prod_{i=1}^{\infty}(1 - uq^{-bi})^b \qquad (5.1)$$

which converges for all $|u| < q^b$. In particular, $H(1, q^b)$ exists and satisfies

$$H(1, q^b) = \frac{bq^{-b}}{(1 - q^{-b})^2}\omega(1, q^b)^b. \tag{5.2}$$

It follows that

$$L(1, q^b) = \omega(1, q^b)^{-1}\big(1 - (1 - H(1, q^b))^N\big).$$

By Lemma 5.2, we have $\lim_{c\to\infty}|\mathrm{pcb}(c, q^b)|/|\mathrm{GL}(c, q^b)| = L(1, q^b)$, and so

$$\begin{aligned} P_M(\infty, q^b) &= \lim_{c\to\infty} \frac{|\mathrm{pcb}(c, q^b)|}{|\mathrm{M}(c, q^b)|} \\ &= \omega(1, q^b) \lim_{c\to\infty} \frac{|\mathrm{pcb}(c, q^b)|}{|\mathrm{GL}(c, q^b)|} \\ &= 1 - \big(1 - H(1, q^b)\big)^N. \end{aligned}$$

Theorem 1.1 (i) is proved. □

The following lemma is used to study the asymptotics of $P_M(\infty, q^b)$ as q^b grows:

Lemma 5.3. (i) *If* $x \in [0, \frac{1}{3})$, *then* $\prod_{i=1}^{\infty}(1 - x^i) > 1 - x - x^2 > \frac{5}{9}$.

(ii) *If* $x \in [0, \frac{1}{2}]$ *and* b *is a positive integer, then* $1 - 2bx \le (1 - x - x^2)^b$.

(iii) *If* $x > 1$, *then* $\frac{x}{\log x} > x^{1/2}$.

(iv) *If* $x \in (0, \frac{1}{2})$, *then* $\frac{1}{1-x} < 1 + x + 2x^2$.

Proof. (i) This is proved in [13, Lemma 3.5].

(ii) We prove this inductively on b. For $b = 1$ the inequality holds since $0 \le x < 1$. Suppose that $b \ge 1$ and $1 - 2bx \le (1 - x - x^2)^b$. Then

$$(1-x-x^2)^{b+1} \ge (1-x-x^2)(1-2bx) = 1-(2b+1)x+(2b-1)x^2-2bx^3,$$

and this is at least $1 - 2(b + 1)x - x^2$ since $2bx^2(1 - x) \ge 0$. Then since $0 \le x \le \frac{1}{2}$, we have $-x^2 \ge -x$, which yields the required inequality, and hence the result is proved by induction.

(iii) Since $x > 1$, the required inequality is equivalent to $x^{1/2} > \log x$. Examining the derivative of $f(x) := x^{1/2} - \log x$, we see that, for $x > 1$, $f(x)$ has a unique minimum at $x = 4$. Then since $f(4) > 0$, it follows that $f(x) > 0$ for all $x > 1$.

(iv) Let $f(x) = (1 + x + 2x^2)(1 - x)$. The required inequality holds if and only if $f(x) > 1$ (since $x \in (0, \frac{1}{2})$). On multiplying we find $f(x) = 1 + x^2 - 2x^3$ and this is greater than 1 since $x^2 - 2x^3 = x^2(1 - 2x) > 0$. □

Lemma 5.4. *Let $t \geq 1$, $\epsilon \in (0, 1)$, and suppose that $c > \max\{1, (\frac{t}{\log(1-\epsilon)})^2\}$. Then*

$$c^t \leq (1 - \epsilon)^{-c}.$$

Proof. The inequality is equivalent to $t \log c \leq -c \log(1 - \epsilon)$. Since $\log c > 0$, and since $0 < 1 - \epsilon < 1$ implies $\log(1 - \epsilon) < 0$, this holds if and only if

$$-\frac{t}{\log(1 - \epsilon)} \leq \frac{c}{\log c}. \tag{5.3}$$

By Lemma 5.3 (iii), $c/\log c > c^{1/2}$, and by assumption $c^{1/2} \geq -t/\log(1 - \epsilon)$, yielding inequality (5.3). □

Proposition 5.5. *Let $P_M(\infty, q^b) = \lim_{c\to\infty} |\mathrm{pcb}(c, q^b)|/|\mathrm{M}(c, q^b)|$, where $b \geq 2$ and $q^b > 4$. Then*

$$-\frac{4b}{eq^{b/2}} < P_M(\infty, q^b) - (1 - e^{-1}) < \frac{1 + b}{eq^b} + \frac{2(1 + b)^2}{eq^{2b}},$$

so that

$$|P_M(\infty, q^b) - (1 - e^{-1})| < 4e^{-1}bq^{-b/2}.$$

Proof. By Theorem 1.1 (i), $P_M(\infty, q^b) = 1 - (1 - H(1, q^b))^N$, with $H(1, q^b)$ as in (5.2) above. We consider the behaviour of $(1 - H(1, q^b))^N$ as q and b grow. Since $\omega(1, q^b) = \prod_{i=1}^{\infty}(1 - q^{-bi})$, and since $q^{-b} \leq \frac{1}{4}$, it follows from Lemma 5.3 (i) that

$$1 - q^{-b} - q^{-2b} < \omega(1, q^b) < 1 - q^{-b}.$$

Applying Lemma 5.3 (ii) with $x = q^{-b}$ gives

$$1 - 2bq^{-b} < \omega(1, q^b)^b < 1 - q^{-b}. \tag{5.4}$$

Now as $N := N(q, b) = \frac{1}{b}\sum_{d\,|\,b} \mu(d)q^{d/b}$, we have

$$\frac{1}{b}(q^b - 2q^{b/2}) \leq N(q, b) \leq \frac{q^b}{b}.$$

Thus

$$(1 - H(1, q^b))^{(1/b)q^b} \leq (1 - H(1, q^b))^N \leq (1 - H(1, q^b))^{(1/b)(q^b - 2q^{b/2})},$$

and so (with H denoting $H(1, q^b)$ for simplicity):

$$\frac{q^b}{b}\log(1-H) \le N\log(1-H) \le \frac{1}{b}(q^b - 2q^{b/2})\log(1-H).$$

Using the inequality $1 - \frac{1}{x} \le \log x \le x - 1$, which holds for all $x > 0$, we have

$$\frac{q^b}{b}\frac{H}{H-1} \le N\log(1-H) \le -\frac{1}{b}(q^b - 2q^{b/2})H.$$

Substituting for H using (5.2) and rearranging gives

$$\begin{aligned}\frac{-\omega(1,q^b)^b}{(1-q^{-b})^2 - bq^{-b}\omega(1,q^b)^b} &\le N\log(1-H)\\ &\le -\frac{1}{b}(q^b - 2q^{b/2})\frac{bq^{-b}}{(1-q^{-b})^2}\omega(1,q^b)^b.\end{aligned}$$

Using the right inequality of (5.4) and observing a geometric series gives

$$\begin{aligned}\frac{-\omega(1,q^b)^b}{(1-q^{-b})^2 - bq^{-b}\omega(1,q^b)^b} &> \frac{-(1-q^{-b})}{(1-q^{-b})^2 - bq^{-b}(1-q^{-b})}\\ &= \frac{-1}{1-q^{-b}-bq^{-b}}\\ &= \frac{-1}{1-(1+b)q^{-b}}.\end{aligned}$$

If $q^b \ge 9$, then applying Lemma 5.3 (iv) with $x = (1+b)q^{-b}$ gives

$$\frac{-1}{1-(1+b)q^{-b}} \ge -1 - (1+b)q^{-b} - 2(1+b)^2q^{-2b},$$

and this is true also (with equality) if $q^b = 8$. Thus for all $q^b > 4$, we have

$$N\log(1-H) > -1 - (1+b)q^{-b} - 2(1+b)^2q^{-2b}.$$

On the other hand, we have, using the left inequality in (5.4), and since $q^b > 4$ implies

$$\frac{1}{(1-q^{-b})^2} < \frac{1}{(3/4)^2} = \frac{16}{9} < 2,$$

that

$$\begin{aligned}
&-\frac{1}{b}(q^b - 2q^{b/2})\frac{bq^{-b}}{(1-q^{-b})^2}\omega(1,q^b)^b \\
&\quad = -(1-2q^{-b/2})\frac{\omega(1,q^b)^b}{(1-q^{-b})^2} \\
&\quad < \frac{-(1-2q^{-b/2})(1-2bq^{-b})}{(1-q^{-b})^2} \\
&\quad = -1 + \frac{2q^{-b/2} + 2(b-1)q^{-b} - 4bq^{-3b/2} + q^{-2b}}{(1-q^{-b})^2} \\
&\quad < -1 + 2\big(2q^{-b/2} + 2(b-1)q^{-b} - 4bq^{-3b/2} + q^{-2b}\big).
\end{aligned}$$

Since $-4bq^{-3b/2}$ is negative, and $2q^{-b} > q^{-2b}$, this is less than $-1 + 4q^{-b/2} + 4bq^{-b}$. Thus we have proved that

$$\begin{aligned}
-1 - (1+b)q^{-b} - 2(1+b)^2q^{-2b} &< N\log(1-H) \\
&< -1 + 4q^{-b/2} + 4bq^{-b},
\end{aligned}$$

and so exponentiating,

$$\begin{aligned}
\exp\big(-1 - (1+b)q^{-b} - 2(1+b)^2q^{-2b}\big) &< (1-H)^N \\
&< \exp\big(-1 + 4q^{-b/2} + 4bq^{-b}\big).
\end{aligned}$$

Now for $0 \le x \le 1$ we have $e^x \le 1 + x + \frac{3}{4}x^2$ and $e^{-x} > 1 - x$ (see for example [8, Lemma 2.3]). The first inequality implies that

$$\begin{aligned}
(1-H)^N &< e^{-1}\Big(1 + 4q^{-b/2} + 4bq^{-b} + \frac{3}{4}(4q^{-b/2} + 4bq^{-b})^2\Big) \\
&= e^{-1} + 4e^{-1}q^{-b/2} + 4e^{-1}(b+3)q^{-b} + 24e^{-1}bq^{-3b/2} \\
&\quad + 12e^{-1}b^2q^{-2b} \\
&< e^{-1} + 4be^{-1}q^{-b/2},
\end{aligned}$$

and the second inequality gives

$$\begin{aligned}
(1-H)^N &> e^{-1}\big(1 - (1+b)q^{-b} - 2(1+b)^2q^{-2b}\big) \\
&= e^{-1} - e^{-1}(1+b)q^{-b} - 2e^{-1}(1+b)^2q^{-2b}.
\end{aligned}$$

Recalling that $P_M(\infty, q^b) = 1 - (1-H)^N$, the first inequality in the statement is proved by subtracting these two values from 1. The second inequality follows immediately from the first. □

5.1 Proof of Theorem 1.1 (ii)

Finally, we apply the method of Wall (see [6]) to $\mathrm{M}(c, q^b)$ to prove the second part of our main result, which gives a useful lower bound on $|\mathrm{pcb}(c, q^b)|/|\mathrm{M}(c, q^b)|$ for sufficiently large c. The inequality we require is proved in Proposition 5.10, thus completing the proof of Theorem 1.1. We introduce the following notation, following Fulman in [5]: for a function $X(u)$ of a complex variable, we denote by $[u^c]X$ the coefficient of u^c in the Maclaurin series of X.

Lemma 5.6. *Let $X(u)$ be an analytic function of a complex variable, and let t be a positive integer.*

(i) *For all $c \geq 1$, we have*

$$[u^c]\left(\frac{X(u)}{1-u}\right) = \sum_{i=0}^{c} [u^i]X(u).$$

(ii) *Suppose there exist constants a_1, a_2 such that $|[u^c]X(u)| \leq a_1 a_2^{-c}$, for all $c \geq 0$. Then for all $c \geq 0$, we have*

$$|[u^c](X(u)^t)| \leq a_1^t (c+1)^{t-1} a_2^{-c}.$$

Proof. (i) Let $x_i := [u^i]X(u)$. Then

$$\begin{aligned}\frac{X(u)}{1-u} &= (x_0 + x_1 u + \cdots)(1 + u + u^2 + \cdots) \\ &= x_0 + (x_0 + x_1)u + (x_0 + x_1 + x_2)u^2 + \cdots\end{aligned}$$

and (i) follows.

(ii) We proceed by induction on t. The result holds for $t = 1$ by assumption. Let $x_{ij} := [u^j]X(u)^i$, and suppose that $t \geq 2$ and that part (ii) holds for $X(u)^{t-1}$. Then

$$\begin{aligned}X(u)^t &= X(u)^{t-1}X(u) \\ &= (x_{t-1,0} + x_{t-1,1}u + \cdots)(x_{10} + x_{11}u + \cdots) \\ &= \sum_{c=0}^{\infty} \sum_{i=0}^{c} (x_{t-1,i})(x_{1,c-i})u^c,\end{aligned}$$

and so by induction

$$\begin{aligned}|[u^c]X(u)^t| &= \left|\sum_{i=0}^{c} x_{t-1,i}\, x_{1,c-i}\right| \\ &\le \sum_{i=0}^{c}\big(a_1^{t-1}(i+1)^{t-2}a_2^{-i}\big).(a_1 a_2^{-(c-i)}) \\ &= a_1^t \sum_{i=0}^{c}\big((i+1)^{t-2}a_2^{-c}\big) \\ &\le a_1^t (c+1)^{t-1} a_2^{-c},\end{aligned}$$

since $\sum_{j=1}^{c+1} j^{t-2} \le (c+1)^{t-1}$. The result now follows by induction. □

Lemma 5.7. *Let* $J(u, q^b) = (1 - uq^b)\,\mathrm{PCB}(uq^b, q^b)$. *Then for* $c \ge 2$, *we have*

$$[u^c]J(u, q^b) = \left(\frac{|\mathrm{pcb}(c, q^b)|}{|\mathrm{M}(c, q^b)|} - \frac{|\mathrm{pcb}(c-1, q^b)|}{|\mathrm{M}(c-1, q^b)|}\right)q^{bc}.$$

Proof. By definition of $J(u, q^b)$ we have

$$\begin{aligned}J(u, q^b) &= (1 - uq^b)\sum_{c=1}^{\infty}\frac{|\mathrm{pcb}(c, q^b)|}{|\mathrm{M}(c, q^b)|}(uq^b)^c \\ &= \frac{|\mathrm{pcb}(1, q^b)|}{|\mathrm{M}(1, q^b)|}uq^b + \sum_{c=2}^{\infty}\left(\frac{|\mathrm{pcb}(c, q^b)|}{|\mathrm{M}(c, q^b)|} - \frac{\mathrm{pcb}(c-1, q^b)}{|\mathrm{M}(c-1, q^b)|}\right)q^{bc}u^c,\end{aligned}$$

which completes the proof. □

The remainder of this section is devoted to finding an upper bound on the coefficient $[u^c]J(u, q^b)$, and using this to prove Theorem 1.1 (ii).

Lemma 5.8. *Define* $L(u, q^b) := \prod_{i=1}^{\infty}(1 - uq^{-bi}) = (P(u, q^b)(1 - u))^{-1}$, *and suppose* $b > 1$. *Then*

$$L(u, q^b) = \frac{1}{1-u}\left(1 + \sum_{c=1}^{\infty}\frac{(-1)^c q^{bc} u^c}{\prod_{i=1}^{c}(q^{bi} - 1)}\right)$$

and for all $c \ge 1$, *we have*

$$|[u^c]L(u, q^b)| \le a_L q^{-bc},$$

where $a_L = 2q^b$.

Proof. The first assertion follows from [1, Corollary 2.2]. For the second, observe that

$$\begin{aligned}
[u^c]L &= 1 + \sum_{k=1}^{c} \frac{(-1)^k q^{bk}}{\prod_{i=1}^{k}(q^{bi}-1)} \\
&= 1 + \sum_{k=1}^{c} \left(\frac{(-1)^k (q^{bk}-1)}{\prod_{i=1}^{k}(q^{bi}-1)} + \frac{(-1)^k}{\prod_{i=1}^{k}(q^{bi}-1)} \right) \\
&= 1 + \sum_{k=1}^{c} \left(\frac{(-1)^k}{\prod_{i=1}^{k-1}(q^{bi}-1)} + \frac{(-1)^k}{\prod_{i=1}^{k}(q^{bi}-1)} \right) \\
&= 1 - 1 + \frac{(-1)^c}{\prod_{i=1}^{c}(q^{bi}-1)} \\
&= \frac{(-1)^c q^{-bc(c-1)/2}}{\prod_{i=1}^{c}(1-q^{-bi})},
\end{aligned}$$

as all but the first and last terms of the alternating sum cancel. Now for all c, we have both $q^{-bc(c-1)} \leq q^b.q^{-bc}$, and

$$\prod_{i=1}^{c}(1-q^{-bi}) > \prod_{i=1}^{\infty}(1-q^{-bi}) > \frac{1}{2}$$

by Lemma 5.3 (i), and so $|[u^c]L| \leq 2q^b.q^{-bc}$. □

Lemma 5.9. *Let $J(u, q^b)$ be as defined in Lemma* 5.7*, and suppose that $b > 1$. Let*

$$M_{q^b} = \left(\frac{\max\{b-1, q^b/b\}}{\log(3/4)} \right)^2.$$

Then for $c \geq M_{q^b}$, and

$$a_J = \frac{8}{3} \left(\frac{bq^b}{q^b-1} 2^b (2q^b)^b q^{b^2} \right)^{q^b/b}$$

we have

$$|[u^c]J(u, q^b)| < a_J,$$

and hence

$$\left| \frac{\mathrm{pcb}(c+1, q^b)}{|\mathrm{M}(c+1, q^b)|} - \frac{\mathrm{pcb}(c, q^b)}{|\mathrm{M}(c, q^b)|} \right| < a_J q^{-bc}.$$

Proof. Using Theorem 5.1, the fact that $P(uq^b, q^b) = P(u, q^b)(1-uq^b)^{-1}$, the definition of $H(uq^b, q^b)$ from the right-hand side of (5.1), and (4.3), we have (with $N = |\mathrm{Irr}(q, b)|$)

$$\begin{aligned}
J(u, q^b) &= (1-uq^b)P(uq^b, q^b)\big(1-(1-H(uq^b, q^b))^N\big) \\
&= P(u, q^b)\left[1-\left(1-\frac{bq^b}{q^b-1}\,\frac{u}{1-u}\prod_{i=1}^{\infty}(1-uq^{b-bi})^b\right)^N\right] \\
&= P(u, q^b)\left[1-\left(1-\frac{bq^b}{q^b-1}\,\frac{u}{1-u}\prod_{i=0}^{\infty}(1-uq^{-bi})^b\right)^N\right] \\
&= P(u, q^b)\left[1-\left(1-\frac{bq^b}{q^b-1}\,\frac{u}{1-u}P(u, q^b)^{-b}\right)^N\right] \\
&= P(u, q^b)\left[1-\left(1-\frac{bq^b}{q^b-1}u(1-u)^{b-1}L(u, q^b)^b\right)^N\right], \qquad (5.5)
\end{aligned}$$

since $L(u, q^b) = ((1-u)P(u, q^b))^{-1}$ by definition. By Lemma 5.8, we have $|[u^c]L| \le a_L q^{-bc}$, where $a_L = 2q^b$, and hence by Lemma 5.6 (ii), $|[u^c]L^b|$ is bounded above by $a_L^b(c+1)^{b-1}q^{-bc}$. Then

$$\begin{aligned}
\big|[u^c]((1-u)^{b-1}L^b)\big| &\le \sum_{k=0}^{b}\binom{b}{k}a_L^b(c-k+1)^{b-1}q^{-b(c-k)} \\
&< \sum_{k=0}^{b}\binom{b}{k}a_L^b(c+1)^{b-1}q^{-b(c-b)} \\
&= a_L^b(c+1)^{b-1}q^{-b(c-b)}\Big(\sum_{k=0}^{b}\binom{b}{k}\Big) \\
&= 2^b a_L^b q^{b^2}(c+1)^{b-1}q^{-bc}.
\end{aligned}$$

Multiplication by u 'shifts' the coefficients, so that c is replaced with $c-1$: that is,

$$\big|[u^c]\big(u(1-u)^{b-1}L(u, q^b)^b\big)\big| < 2^b a_L^b q^{b^2+b}c^{b-1}q^{-bc}.$$

It follows that

$$\left|[u^c]\left(\frac{bq^b}{q^b-1}u(1-u)^{b-1}L(u, q^b)^b\right)\right| < \frac{bq^{2b}}{q^b-1}2^b a_L^b q^{b^2}c^{b-1}q^{-bc},$$

and since subtracting the function from 1 has no effect on the absolute value of any coefficients when $c \geq 1$, we have (for $c > 1$) that

$$\left|[u^c]\left(1 - \frac{bq^b}{q^b-1}u(1-u)^{b-1}L(u,q^b)^b\right)\right| < \frac{bq^b}{q^b-1}2^b a_L^b q^{b^2} c^{b-1} q^{-bc},$$

and so by Lemma 5.4 with $t = b-1$, $\epsilon = \frac{1}{4}$, we have, for $c \geq (\frac{b-1}{\log(3/4)})^2$ (and hence $c > 1$),

$$\left|[u^c]\left(1 - \frac{bq^b}{q^b-1}u(1-u)^{b-1}L(u,q^b)^b\right)\right| < \frac{bq^b}{q^b-1}2^b a_L^b q^{b^2}\left(\frac{3q^b}{4}\right)^{-c}.$$

Again applying Lemma 5.6 (ii), with $t = N$, and since by [12], $N \leq q^b/b$, we have

$$\left|[u^c]\left(1 - \frac{bq^b}{q^b-1}u(1-u)^{b-1}L(u,q^b)^b\right)^N\right| < \left(\frac{bq^b}{q^b-1}2^b a_L^b q^{b^2}\right)^{q^b/b}(c+1)^{q^b/b}\left(\frac{3q^b}{4}\right)^{-c}.$$

Then setting

$$a_J = \frac{8}{3}\left(\frac{bq^b}{q^b-1}2^b a_L^b q^{b^2}\right)^{q^b/b}$$

and again applying Lemma 5.4 (with $c+1$ in place of c and $t = q^b/b$), we have, for $c > (\frac{q^b}{b\log(3/4)})^2$, that

$$(c+1)^{q^b/b} < \left(1 - \frac{1}{4}\right)^{-c-1} = \frac{4}{3}\left(\frac{3}{4}\right)^{-c},$$

and so

$$\left|[u^c]\left(1 - \frac{bq^b}{q^b-1}u(1-u)^{b-1}L(u,q^b)^b\right)^N\right| < \frac{3a_J}{8}.\frac{4}{3}\left(\frac{9q^b}{16}\right)^{-c} = \frac{a_J}{2}\left(\frac{9q^b}{16}\right)^{-c}.$$

Now by (5.5), we may attain an expression for $J(u,q^b)$ by multiplying the above equation by $P(u,q^b)$: doing so, and recalling that by definition

$$[u^c]P(u,q^b) = \omega(c,q^b)^{-1} = \prod_{j=1}^{c}(1-q^{-bj}),$$

gives

$$|[u^c]J(u,q^b)| < \sum_{i=0}^{c}\prod_{j=i}^{c}(1-q^{-bj})\frac{a_J}{2}\left(\frac{9q^b}{16}\right)^{-i} < \frac{a_J}{2}\left(\sum_{i=0}^{c}\left(\frac{9q^b}{16}\right)^{-i}\right) < a_J,$$

since $\sum_{i=0}^{c}(9q^b/16)^{-i} < 2$ when $q^b \geq 4$.

The second assertion follows directly from Lemma 5.7. □

Proposition 5.10. *Suppose $b \geq 2$, and let a_J, M_{q^b} be as defined in Lemma* 5.9. *Then for $c > M_{q^b}$,*

$$\left|P_M(c,q^b) - P_M(\infty,q^b)\right| = \left|\frac{|\mathrm{pcb}(c,q^b)|}{|\mathrm{M}(c,q^b)|} - \lim_{n\to\infty}\frac{|\mathrm{pcb}(c',q^b)|}{|\mathrm{M}(c',q^b)|}\right| \leq \frac{a_J}{1-q^{-b}}q^{-bc}.$$

In particular, Theorem 1.1 (ii) *holds.*

Proof. By Lemma 5.9, we have

$$\left|\frac{\mathrm{pcb}(c+1,q^b)}{|\mathrm{M}(c+1,q^b)|} - \frac{\mathrm{pcb}(c,q^b)}{|\mathrm{M}(c,q^b)|}\right| < a_J q^{-bc},$$

and so for every $c' > c > M_{q^b}$ we have

$$\begin{aligned}\left|\frac{|\mathrm{pcb}(c',q^b)|}{|\mathrm{M}(c',q^b)|} - \frac{|\mathrm{pcb}(c,q^b)|}{|\mathrm{M}(c,q^b)|}\right| &\leq \sum_{m=c}^{c'-1}\left|\frac{|\mathrm{pcb}(m+1,q^b)|}{|\mathrm{M}(m+1,q^b)|} - \frac{|\mathrm{pcb}(m,q^b)|}{|\mathrm{M}(m,q^b)|}\right| \\ &< \sum_{m=c}^{c'-1} a_J q^{-bm} \\ &= q^{-bc}a_J\left(\sum_{m=0}^{c'-c-1} q^{-bm}\right) \\ &< q^{-bc}a_J\left(\sum_{m=0}^{\infty} q^{-bm}\right) \\ &= q^{-bc}a_J\left(\frac{1}{1-q^{-b}}\right).\end{aligned}$$

□

Bibliography

[1] G. E. Andrews, *The Theory of Partitions*, Cambridge University Press, Cambridge, 1998.

[2] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, John Wiley & Sons, New York, 1993.

[3] B. P. Corr, T. Popiel and C. E. Praeger, Nilpotent-independent sets and estimation in matrix algebras, *LMS J. Comput. Math.* **18** (2015), 404–418.

[4] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice Hall, New Jersey, 1999.

[5] J. E. Fulman, *Probability in the classical groups over finite fields: Symmetric functions, stochastic algorithms, and cycle indices*, Ph.D. thesis, Harvard University, Cambridge, 1997.

[6] J. Fulman, P. M. Neumann and C. E. Praeger, A generating function approach to the enumeration of matrices in classical groups over finite fields, *Mem. Amer. Math. Soc.* **176** (2005), no. 830, 1–90.

[7] S. P. Glasby and C. E. Praeger, Towards an efficient Meat-Axe algorithm using f-cyclic matrices: The density of uncyclic matrices in $M(n, q)$, *J. Algebra* **322** (2009), no. 3, 766–790.

[8] S. Guest and C. E. Praeger, Proportions of elements with given 2-part order in finite classical groups of odd characteristic, *J. Algebra* **372** (2012), 637–660.

[9] B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman & Hall, London, 1980.

[10] D. F. Holt and S. Rees, Testing modules for irreducibility, *J. Aust. Math. Soc. Ser. A* **57** (1994), no. 1, 1–16.

[11] J. P. S. Kung, The cycle structure of a linear transformation over a finite field, *Linear Algebra Appl.* **36** (1981), 141–155.

[12] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge University Press, Cambridge, 1997.

[13] P. M. Neumann and C. E. Praeger, Cyclic matrices over finite fields, *J. Lond. Math. Soc. (2)* **52** (1995), no. 2, 263–284.

[14] R. A. Parker, The computer calculation of modular characters (the meat-axe), in: *Computational group theory* (Durham 1982), Academic Press, London (1984), 267–274.

[15] G. Pólya and R. Read, *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*, Springer, New York, 1987.

[16] R. Stong, Some asymptotic results on finite vector spaces, *Adv. in Appl. Math.* **9** (1988), no. 2, 167–199.

[17] Wolfram Research Inc., Mathematica 8.0, Champaign, Illinois, 2010.

Received November 22, 2017; revised March 29, 2018.

Author information

Brian P. Corr, Centre for Mathematics of Symmetry and Computation,
School of Mathematics and Statistics, The University of Western Australia,
Crawley, WA 6009, Australia.
E-mail: brian.p.corr@gmail.com

Cheryl E. Praeger, Centre for Mathematics of Symmetry and Computation,
School of Mathematics and Statistics, The University of Western Australia,
Crawley, WA 6009, Australia.
E-mail: cheryl.praeger@uwa.edu.au