RESEARCH ARTICLE

Random generation of associative algebras

Damian Sercombe¹ | Aner Shalev²

Dedicated to the memory of Peter Neumann

¹Faculty of Mathematics, Ruhr University, Bochum, Germany
²Institute of Mathematics, Hebrew University, Jerusalem, Israel

Correspondence
Damian Sercombe, Faculty of Mathematics, Ruhr University, Bochum D-44780, Germany.
Email: damian.sercombe@rub.de

Both authors are affiliated with the Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel.

Funding information
ISF, Grant/Award Number: 686/17

Abstract
There has been considerable interest in recent decades in questions of random generation of finite and profinite groups and finite simple groups in particular. In this paper, we study similar notions for finite and profinite associative algebras. Let \( k = \mathbb{F}_q \) be a finite field. Let \( A \) be a finite-dimensional, associative, unital algebra over \( k \). Let \( P(A) \) be the probability that two elements of \( A \) chosen (uniformly and independently) at random will generate \( A \) as a unital \( k \)-algebra. It is known that if \( A \) is simple, then \( P(A) \to 1 \) as \( |A| \to \infty \). We extend this result to a large class of finite associative algebras. For \( A \) simple, we find the optimal lower bound for \( P(A) \) and we estimate the growth rate of \( P(A) \) in terms of the minimal index \( m(A) \) of any proper subalgebra of \( A \). We also study the random generation of simple algebras \( A \) by two elements that have a given characteristic polynomial (resp. a given rank). In addition, we bound above and below the minimal number of generators of general finite algebras. Finally, we let \( A \) be a profinite algebra over \( k \). We show that \( A \) is positively finitely generated if and only if \( A \) has polynomial maximal subalgebra growth. Related quantitative results are also established.

MSC 2020
16P10 (primary), 15B52 (secondary)
1 | INTRODUCTION

In the past few decades, there has been extensive research on random generation of finite and profinite groups with emphasis on finite simple groups. See, for instance, the survey articles [11, 23] and the references therein.

The study of random generation of associative algebras is less well developed. Consider the algebra $M_n(q)$ of $n \times n$ matrices over a finite field $\mathbb{F}_q$. In 1995, it was shown by Peter Neumann and Cheryl Praeger [17] that the probability that two matrices in $M_n(q)$, chosen independently under the uniform distribution, generate $M_n(q)$ as an $\mathbb{F}_q$-algebra tends to 1 as $|M_n(q)| \to \infty$. See also the subsequent paper [9] by Kravchenko, Mazur and Petrenko for additional results on random generation of finite and infinite algebras.

One can refine this problem and consider random generation of an algebra by two elements that satisfy a certain property. A matrix in $M_n(q)$ is cyclic if its characteristic polynomial is equal to its minimal polynomial. Neumann and Praeger showed in [7] that almost all pairs of cyclic matrices in $M_n(q)$ will generate it as an $\mathbb{F}_q$-algebra. Amongst other results of this flavour, we show that — given a monic polynomial $f$ of degree $n$ over $\mathbb{F}_q$ — almost all pairs of matrices in $M_n(q)$ with characteristic polynomial $f$ will generate it as an $\mathbb{F}_q$-algebra.

In this paper, we study random generation of finite and profinite associative algebras, and we obtain some new results also in the case of simple algebras.

Let $k$ be a finite field, that is, $k = \mathbb{F}_q$ for some prime power $q$. Unless otherwise stated, all algebras in this paper are assumed to be over $k$, and are associative and unital. Subalgebras of a unital algebra are required to contain the multiplicative identity of the original algebra. We first focus on the study of finite algebras. Later on, we look at profinite algebras.

Let $A$ be an associative, unital, finite-dimensional algebra over $k$ (a.k.a. a finite algebra). Let $A^\times$ denote the group of units of $A$. Let $A^N$ denote the set of nilpotent elements of $A$. The Jacobson radical $J(A)$ of $A$ is a nilpotent ideal of $A$. If $J(A)$ is trivial, then $A$ is semisimple.

In this paragraph, we summarise the Wedderburn–Malcev principal theorem ([22, Theorems 5.3.20 and 5.3.21]). There exists a semisimple subalgebra $S$ of $A$ such that $A = S \oplus J(A)$ as vector spaces. If $S'$ is another subalgebra of $A$ satisfying $A = S' \oplus J(A)$, then $S'$ is conjugate to $S$ by an element of $1 + J(A)$. Wedderburn’s little theorem ([22, Theorem 7.1.11]) states that all finite division algebras are fields. Combining this with another theorem of Wedderburn ([22, Theorem 2.1.8]), it follows that there is an algebra isomorphism $S \cong \prod_{i=1}^{r} M_{n_i}(q^{m_i})$ for some integers $r, n_1, \ldots, n_r, m_1, \ldots, m_r$ that is unique up to permutation of the factors.

Denote $n := \min_{i=1,\ldots,r}\{n_i\}$ and $m := \min_{i=1,\ldots,r}\{m_i\}$. Fix constants $c > 1$ and $\lambda > 0$. We say that $A$ is bounded by $(c, \lambda)$ if $r \leq \lambda c^{\min\{m,n\}/2}$ and $\dim J(A)/J(A)^2 \leq \log_q \lambda + \min\{m,n\}^2 \log_q c$.

A subset $X$ of $A$ is a generating set if the set of all monomials in the elements of $X$ (including the trivial monomial) spans $A$ as a $k$-vector space. We define $P(A)$ to be the probability that two elements of $A$ chosen uniformly at random will generate $A$ as a (unital) $k$-algebra. That is,

$$P(A) = \frac{|\{(x,y) \in A \times A : \langle x,y \rangle = A\}|}{|A|^2}.$$

**Theorem 1.1.** Fix constants $1 < c < q$ and $\lambda > 0$. Let $A$ be a finite algebra, say $A = (\prod_{i=1}^{r} M_{n_i}(q^{m_i})) \oplus J(A)$, and denote $n := \min_{i=1,\ldots,r}\{n_i\}$ and $m := \min_{i=1,\ldots,r}\{m_i\}$. Assume that $A$ is bounded by $(c, \lambda)$. Then $P(A) \to 1$ as $n \to \infty$, as $m \to \infty$ or as $q \to \infty$. 
It is not true in general that $P(A) \to 1$ as $|A| \to \infty$. For example, let $A$ be as in the theorem above and suppose that there exists a positive integer $i \leq r$ such that $n_i = 1$ and $m_i = 2$. Then $A$ has a maximal subalgebra $B$ satisfying $A/B \cong k$. Hence, $|B|/|A| = q^{-1}$, so $1 - P(A) \geq |B|^2/|A|^2 = q^{-2}$. Fixing $q$ and letting $|A|$ tend to infinity, we see that $P(A) \leq 1 - q^{-2}$ is bounded away from 1.

Moreover, let $A = k^r$ for some $r \in \mathbb{N}$. Then, any maximal subalgebra $B$ of $A$ has codimension 1, and it is easy to see that $P(A) \to 0$ as $r \to \infty$. However, Theorem 1.1 implies the following known result.

**Corollary 1.2.** Let $A$ be a finite simple algebra. Then $P(A) \to 1$ as $|A| \to \infty$.

This corollary is somewhat more general than the Neumann–Praeger result stated above, in the sense that it also deals with $A = M_n(q^m)$ as a $\mathbb{F}_q$-algebra, but it is obtained in [9] using different methods.

An equivalent formulation of Corollary 1.2 is as follows. Let $A$ be a simple algebra and consider the free associative algebra $k\langle X_1, X_2 \rangle$. Then, the probability that a randomly chosen $k$-algebra homomorphism $k\langle X_1, X_2 \rangle \to A$ is surjective tends to 1 as $|A| \to \infty$.

It is well known that any finite simple algebra is 2-generated, see, for instance, [9, Theorem 6.4]. So, it follows from Corollary 1.2 that there exists an absolute constant $\delta > 0$ such that $P(A) \geq \delta$ for all finite simple algebras $A$. In the following result, we find the best possible value for this constant.

**Theorem 1.3.** Let $A$ be a finite simple algebra. Then $P(A) \geq 3/8$, with equality if and only if $A = M_2(2)$.

For $G$ a finite simple group, let $P(G)$ be the probability that two randomly chosen elements of $G$ will generate $G$. It is a consequence of [16, Theorem 1.1] that $P(G) \geq 53/90$, with equality if and only if $G = A_6$.

For $A$ simple and not a field, we investigate the growth rate of $P(A)$ in more detail. Let $m(A)$ be the minimal index (as an additive group) of any proper subalgebra of $A$.

**Theorem 1.4.** Let $A$ be a finite simple algebra that is not a field. Then

$$P(A) = 1 - \kappa(A)m(A)^{-1} + O(m(A)^{-4/3}),$$

where $\kappa : A \to \mathbb{R}$ is a function satisfying $1 < \kappa(A) < 4$.

We will see in Section 5 that the constants in Theorem 1.4 are best possible. Note that Theorem 1.4 gives us an alternate proof of Corollary 1.2. Results of this flavour for finite simple groups were obtained by Liebeck and Shalev, see [12, Theorems 1.5 and 1.6].

We next look at randomly generating a finite algebra by its nilpotent elements.

Define $P_N(A)$ to be the probability that two nilpotent elements of $A$ chosen uniformly at random will generate $A$ as a $k$-algebra. That is,

$$P_N(A) = \frac{|\{(x, y) \in A^N \times A^N : [x, y] = A\}|}{|A^N|^2}.$$

We prove an analogue of Theorem 1.1.
Theorem 1.5. Fix constants $1 < c < q^{1/4}$ and $\lambda > 0$. Let $A$ be a finite algebra, say $A = (\prod_{i=1}^{r} M_{n_i}(q^{m_i})) \oplus J(A)$, and denote $n := \min_{i=1, \ldots, r}\{n_i\}$ and $m := \min_{i=1, \ldots, r}\{m_i\}$. Assume that $A$ is bounded by $(c, \lambda)$ and that $n > 1$. Then $P_N(A) \to 1$ as $n \to \infty$, as $m \to \infty$ or as $q \to \infty$.

Note that Theorem 1.5 does not hold when $n = 1$. For example, let $A_0$ be a finite algebra and let $A = F_{q^m} \times A_0$ for some $m > 1$. Let $b$ be a prime divisor of $m$ and consider the maximal subalgebra $B = F_{q^m/b} \times A_0$ of $A$. Observe that all nilpotent elements of $A$ are contained in $B$. So, $P_N(A) = 0$, regardless of the choice of $q$, $m$, or $A_0$.

Theorem 1.5 immediately implies the following.

Corollary 1.6. Let $A$ be a finite simple algebra that is not a field. Then, $P_N(A) \to 1$ as $|A| \to \infty$.

We now consider random generation of a finite simple algebra by two elements that have a given characteristic polynomial. Let $A = M_n(q^m)$, let $f$ be a monic polynomial of degree $n$ over $F_{q^m}$ and let $A_f$ be the set of elements of $A$ with characteristic polynomial $f$. We define $P_f(A)$ to be the probability that two elements of $A_f$ chosen uniformly at random will generate $A$ as a $k$-algebra. That is,

$$P_f(A) = \frac{|\{(x, y) \in A_f \times A_f : \langle x, y \rangle = A\}|}{|A_f|^2}.$$ 

Theorem 1.7. Let $A$ be a finite simple algebra that is not a field, say $A = M_n(q^m)$ for $n > 1$. Let $f$ be a monic polynomial of degree $n$ over $F_{q^m}$. Then $P_f(A) \to 1$ as $|A| \to \infty$.

By applying Theorem 1.7 to the case where $f(X) = X^n$, we find an alternate proof of Corollary 1.6.

We now consider random generation of a finite simple algebra by two matrices that have a given rank. Let $\alpha$ be a non-negative integer. Let $A = M_n(q^m)$ where $n \geq \alpha$ and let $A_\alpha$ be the set of matrices in $A$ with rank $\alpha$. We define $P_\alpha(A)$ to be the probability that two elements of $A_\alpha$ chosen uniformly at random will generate $A$ as a $k$-algebra. That is,

$$P_\alpha(A) = \frac{|\{(x, y) \in A_\alpha \times A_\alpha : \langle x, y \rangle = A\}|}{|A_\alpha|^2}.$$ 

Theorem 1.8. Let $A$ be a finite simple algebra that is not a field, say $A = M_n(q^m)$ for $n > 1$. Let $\alpha := \alpha(n)$ be a positive integer.

(i) Let $p$ be the smallest prime divisor of $n$. If $\alpha \leq n/p$, then $P_\alpha(A) \leq 1 - q^{-2mp\alpha^2}$.

(ii) If $n - \sqrt{n}/3 \leq \alpha \leq n$, then $P_\alpha(A) \to 1$ as $|A| \to \infty$. 
It is not true that $P_\alpha(A)$ always tends to 1 as $|A| \to \infty$. This is an immediate consequence of Theorem 1.8(i). We can see this by taking $\alpha$ to be independent of $n$, and letting $n$ tend to infinity whilst fixing $q, m$ and $p$.

Let $P^\times(A)$ to be the probability that two invertible elements of $A$ chosen uniformly at random will generate $A$ as a $k$-algebra. Theorem 1.8(ii) implies the following.

**Corollary 1.9.** Let $A$ be a finite simple algebra. Then, $P^\times(A) \to 1$ as $|A| \to \infty$.

Next, we investigate the minimal number of generators $d(A)$ of a finite algebra $A$.

An obvious upper bound for $d(A)$ is $\log_q |A| - 1$ (the $-1$ term arises from our convention that the multiplicative identity of $A$ is automatically included in any generating set of $A$, and, of course, $\dim A = \log_q |A|$). This upper bound is strict, and is realised in the case where $J(A)$ has codimension 1 in $A$ and $J(A)^2 = 0$.

In general, $d(A)$ often grows much slower than $\log_q |A|$. For example, if $A$ is the direct product of finitely many copies of $k$, then $d(A) = \lfloor \log_q |A| \rfloor$. In particular, if $A = k^r$ for some $1 < r \leq q$, then $d(A) = 1$. Moreover, as remarked earlier, if $A$ is simple, then $d(A) = 2$.

**Theorem 1.10.** Let $A$ be a finite algebra, say $A = S \oplus J(A)$ where $S = \prod_{i=1}^r S_{\alpha_i}^n$ and, for each $i$, $S_{i} = M_{n_i}(q^{m_i})$ and $\alpha_i$ is the number of simple factors of $S$ that are isomorphic to $S_i$. Let $f(A, i) := m_{i}^{-1}n_{i}^{-2}\log q\alpha_{i}\log q\alpha_{i}$, let $f(A) := \max_{i}\{f(A, i)\}$ and let $\mu(A)$ be the minimal length of an unrefinable chain of $S$-subbimodules of $J(A)$. Then

$$-2.33 < d(A) - f(A) < \mu(A) + 3.42.$$  

In the final part of this paper, we study positively finitely generated (PFG) (profinite) algebras and related topics. For the theory of PFG groups, see [1, 3, 8, 13, 15, 18, 20] and the references therein.

A profinite algebra is a topological algebra (over $k$) that is isomorphic to a projective limit of discrete finite algebras. Henceforth, let $A$ be a profinite algebra.

For $d \geq 1$, let $P(A, d)$ be the probability that $d$ randomly chosen elements of $A$ generate $A$ (topologically if $A$ is infinite). We say that $A$ is PFG if $P(A, d) > 0$ for some $d$. We say that $A$ has polynomial maximal subalgebra growth (PMSG) if the number $m_n(A)$ of index $n$ (open) maximal subalgebras of $A$ is bounded by $n^c$ for some fixed constant $c$. It was shown in [15] that, for profinite groups, PFG is equivalent to PMSG. Here, we study these notions and related invariants for profinite algebras.

If we do not specify a base, $\log$ refers to base 2. Set

$$M(A) := \sup_{n>1} \log m_n(A) / \log n, \quad M^\ast(A) := \limsup_{n>1} \log m_n(A) / \log n,$$

which measure the degree of polynomial subgroup growth of $A$ (and are infinite unless $A$ has PMSG). Let $d_0(A) := \min\{d \geq 1 \mid P(A, d) > 0\}$.

We establish the following.

**Theorem 1.11.** Let $A$ be a profinite algebra. Then $A$ is PFG if and only if $A$ has PMSG. Moreover, if $A$ is infinite we have $M^\ast(A) \leq d_0(A) + 1$.  


The bound above is better than related bounds obtained for profinite groups. For any real number \( \eta \geq 1 \), define the Pomerance invariant of \( A \) by
\[
V_\eta(A) := \min\{d \geq 1 : P(A, d) > \eta^{-1}\}.
\]
Clearly \( V_\eta(A) \geq d_0(A) \), with equality for sufficiently large \( \eta \). The case where \( \eta = e \), which we denote by \( V(A) := V_e(A) \), was studied by Pomerance [20] for finite abelian groups.

Next, define the Pak invariant \( E(A) \) of \( A \) to be the expected number of random elements of \( A \) chosen uniformly and independently which generate \( A \) (topologically). A similar invariant was introduced by Pak [18] for finite groups.

Our final main result establishes bounds on these invariants, and is a ring-theoretic analogue of results of Lubotzky [13] and Lucchini-Moscatiello [14] for finite groups.

**Theorem 1.12.** Let \( A \) be a finite algebra, say \( A/J(A) = \prod_{i=1}^{r} S_i \). Then

- (i) \( M(A) \leq 2 \log_q r + d(A) + 2 \).
- (ii) \( [M(A) - 5.24] \leq V(A) \leq [M(A) + 2.02] \).
- (iii) \( [M(A) - 5.80] \leq E(A) \leq [M(A)] + 3 \).

In particular, the expected number of random elements of \( A \) which generate \( A \) is of the order of magnitude \( O(d(A) + \log_q \log_q |A|) \).

This paper is structured as follows. In Section 2, we present a classification of maximal subalgebras of a finite algebra \( A \), then we introduce and investigate a related zeta function of \( A \). In Sections 3–5, we investigate \( P(A) \) and its growth rate. In particular, in Section 3, we prove Theorem 1.1 and Corollary 1.2; in Section 4, we prove Theorem 1.3 and in Section 5, we prove Theorem 1.4. In Sections 6–8, we study random generation of a finite algebra by special elements. In Section 6, we prove Theorem 1.5 and Corollary 1.6; in Section 7, we prove Theorem 1.7 and in Section 8 we prove Theorem 1.8 and Corollary 1.9. In Section 9, we look at the minimal number of generators of a finite algebra, and prove Theorem 1.10. Finally, in Section 10, we investigate PFG profinite algebras and prove Theorems 1.11 and 1.12.

## 2 PRELIMINARIES

Recall that \( k = \mathbb{F}_q \) where \( q \) is a prime power.

Let \( A \) be an (associative, unital) finite simple algebra (over \( k \)). By Wedderburn’s theorem, we can write \( A = M_n(q^m) \) for some positive integers \( n \) and \( m \).

Some remarks on notation. Let \( \alpha = (\alpha_1, \ldots, \alpha_s) \) be a composition of \( n \) (i.e. \( n = \sum_{i=1}^{s} \alpha_i \) where the \( \alpha_i \)’s are positive integers) and suppose \( s \geq 2 \). Let \( P_\alpha(q^m) \) be the subalgebra of \( A \) that consists of all block upper triangular matrices with \( s \) blocks on the diagonal such that the \( i \)’th block has size \( \alpha_i \).

Let \( r \) be a positive integer. There is a natural embedding of \( \mathbb{F}_{q^r} \) in \( M_r(q) \) via the left regular representation. If \( r \) divides \( n \), then this extends to an embedding of \( M_{n/r}(q^{mr}) \) in \( M_n(q^m) \). If \( r \) divides \( m \), then the subfield \( \mathbb{F}_{q^{m/r}} \) of \( \mathbb{F}_{q^m} \) extends naturally to a subalgebra \( M_n(q^{m/r}) \) of \( M_n(q^m) \). Let \( \mathcal{P}(r) \) denote the set of prime divisors of \( r \) (not counting multiplicities). Let \( \omega(r) := |\mathcal{P}(r)| \).
We define three sets of subalgebras of $A$;

$S_1 := \{ P_{l,n-l}(q^m) \mid l \in \mathbb{N}, l < n \}$,

$S_2 := \{ M_{n/a}(q^m a) \mid a \in \mathbb{P}(n) \}$ and

$S_3 := \{ M_n(q^{m/b}) \mid b \in \mathbb{P}(m) \}$.

A subalgebra of $A$ that is conjugate to an element of $S_1$ (resp. $S_2, S_3$) is said to be of type $(S_1)$ (resp. $(S_2), (S_3)$).

Over any field $k$, Lemma 3.6 of Iovanov and Sistko [7] classifies the maximal subalgebras of any simple $k$-algebra up to isomorphism. In the case where $k = \mathbb{F}_q$, we show that the isomorphism classes of maximal subalgebras described in [7] coincide with the conjugacy classes. The $S_1$–$S_3$ notation is chosen to align with that of [7].

**Theorem 1.** Let $A$ be a finite simple algebra. With the above notation, $S_1 \cup S_2 \cup S_3$ is a set of representatives of the conjugacy classes of maximal subalgebras of $A$.

**Proof.** Let $B$ be a maximal subalgebra of $A$. If $B$ is not simple, then, by [7, Lemma 3.6], $B$ is conjugate to $P_{l,n-l}(q^m)$ for some positive integer $l < n$. Let $l' < n$ be a positive integer. It is well known that $P_{l,n-l}(q^m)$ is conjugate to $P_{l',n-l'}(q^m)$ if and only if $l = l'$ (see, e.g. §3 of [4]).

Henceforth let $B$ be simple. By [7, Lemma 3.6], there are two possibilities. Either $Z(B) \supset Z(A)$ or $Z(A) \supset Z(B)$.

Assume that $Z(B) \supset Z(A)$. Then, by [7, Lemma 3.6], $B = C_A(F)$ for some minimal field extension $F$ of $Z(A)$ that is contained in $A$. Observe that $Z(A) \cong \mathbb{F}_{q^n}$. So, $F \cong \mathbb{F}_{q^m}$ for some prime divisor $a$ of $n$. By the double centraliser theorem ([22, Theorem 7.1.9]), $Z(B) = F$ and $[F : Z(A)][B : Z(A)] = [A : Z(A)]$. Recall from Wedderburn’s little theorem that all finite division algebras are fields. It follows that $B \cong M_{n/a}(F)$. Any subalgebra of $A$ that is isomorphic to $B$ is then conjugate to $B$ by the Skolem–Noether theorem.

Now assume that $Z(A) \supset Z(B)$. Then, by [7, Lemma 3.6], $Z(B)$ is a maximal subfield of $Z(A)$ that contains $k$ such that $A \cong Z(A) \otimes_{Z(B)} B$. So $Z(B) \cong \mathbb{F}_{q^{m/b}}$ for some prime divisor $b$ of $m$. Since $A$ and $B$ are both simple, it follows from Wedderburn’s theorem that $B \cong M_{n/b}(q^m)$. Let $t : B \hookrightarrow A$ be inclusion. Observe that $t$ extends to a $Z(A)$-isomorphism $t^* : B \otimes_{Z(B)} Z(A) \to A$. Let $B'$ be another subalgebra of $A$ and let $f : B \to B'$ be a $k$-isomorphism. Let $t' : B' \hookrightarrow A$ be inclusion and denote $\tau := t' \circ f$. Then $\tau$ extends to a $Z(A)$-isomorphism $\tau^* : B \otimes_{Z(B)} Z(A) \to A$. By the Skolem–Noether theorem, there exists $g \in A^\times$ such that $g \tau^*(x) g^{-1} = t^*(x)$ for all $x \in B \otimes_{Z(B)} Z(A)$. Hence, $B'$ is conjugate to $B$. This completes the proof.

We call $S_1 \cup S_2 \cup S_3$ the **standard** set of representatives of the conjugacy classes of maximal subalgebras of $A$.

We now relax the assumption that $A$ is simple. Let $A$ be any finite algebra over $k$. By the Wedderburn–Malcev principal theorem, there exists a semisimple subalgebra $S$ of $A$ such that $A = S \oplus J(A)$. Decompose $S = \prod_{i=1}^r S_i$ where each $S_i$ is simple. Let $i \in \{1, \ldots, r\}$. Write $S_i = M_{n_i}(q^{m_i})$ for some integers $m_i$ and $n_i$. Let $B_i$ be the standard set of representatives of the conjugacy classes of maximal subalgebras of $S_i$. Let $\sigma_i$ be the outer $k$-automorphism of $S_i$ that sends each matrix entry to its $q$‘th power. If $S_j \cong S_i$ for some $j \neq i$, then, for any $l \in \mathbb{Z}/m_i \mathbb{Z}$, let $S_{i,j}^l$ denote the image of the diagonal embedding $S_i \to S_i \times S_j$ given by $x \mapsto (\sigma_i^l(x), x)$. We define three sets of subalgebras of $A$;

$T_1 := \{ (B_1 \times \prod_{i \neq j} S_i) \oplus J(A) \mid 1 \leq j \leq r; B_j \in B_j \}$,

$T_2 := \{ (S_{j_1,j_2} \times \prod_{i \neq j_1,j_2} S_i) \oplus J(A) \mid 1 \leq j_1 < j_2 \leq r, S_{j_1} \cong S_{j_2}, l \in \mathbb{Z}/m_{j_1} \mathbb{Z} \}$ and

$T_3 := \{ S \oplus H \mid H$ is a two-sided ideal of $A$ that is maximal with respect to $H \subset J(A) \}$.  


A subalgebra of $A$ that is conjugate to an element of $T_1$ (resp. $T_2, T_3$) is said to be of type $(T_1)$ (resp. $(T_2), (T_3)$).

**Theorem 2.** Let $A$ be a finite algebra. With the above notation, $T_1 \cup T_2 \cup T_3$ is a set of representatives of the conjugacy classes of maximal subalgebras of $A$.

**Proof.** Consider the simple $k$-algebra $M_n(q^m)$. Let $\sigma$ be the outer $k$-automorphism of $M_n(q^m)$ that sends each matrix entry to its $q^t$th power. It is a consequence of the Skolem–Noether theorem that the group of outer $k$-algebra automorphisms of $M_n(q^m)$ is generated by (the equivalence class of) $\sigma$, and hence, it is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. Combining this fact with [7, Theorem 2.5] and the results in §3.2 of [7] tells us that every maximal subalgebra of $A$ is conjugate to an element of $T_1 \cup T_2 \cup T_3$.

It remains to check that all elements of $T_1 \cup T_2 \cup T_3$ are pairwise non-conjugate in $A$. We will need the following claim; there are precisely $m$ conjugacy classes of type $(T_2)$ subalgebras of $M_n(q^m) \times M_n(q^m)$.

Let $T := M_n(q^m) \times M_n(q^m)$, and consider its centre $Z := F_{q^m} \times F_{q^m}$. The group of $k$-algebra automorphisms $\text{Aut}_k(Z)$ of $Z$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. Let $D$ denote the image of the diagonal embedding $F_{q^m} \to F_{q^m} \times F_{q^m}$ given by $x \mapsto (x, x)$. We know from [7, Proposition 3.9] that any type $(T_2)$ subalgebra of $Z$ is conjugate to $D$ by an element of $\text{Aut}_k(Z)$. Hence, there are precisely $|\text{Aut}_k(Z)|/|\text{Stab}_{\text{Aut}_k(Z)}(D)| = m$ type $(T_2)$ subalgebras of $Z$. Now any inner automorphism of $T$ restricts to the identity on its centre $Z$, and hence, there are at least $m$ conjugacy classes of type $(T_2)$ subalgebras of $A$. But we have already shown that there are at most $m$ conjugacy classes of type $(T_2)$ subalgebras of $T$, and so, we have proved the claim.

We now show that all elements of $T_1 \cup T_2 \cup T_3$ are pairwise non-conjugate in $A$. Let $B, B' \in T_1 \cup T_2 \cup T_3$ and let $a \in A^\times$ such that $B^a := a^{-1}Ba = B'$. Assume (for a contradiction) that $B \neq B'$.

If $B \in T_3$ and $B' \in T_1 \cup T_2$ (or vice versa), then $B \not\cong B'$, a contradiction. If $B, B' \in T_3$, then $B = S \oplus H$ and $B' = S \oplus H'$ for some two-sided ideals $H$ and $H'$ of $A$, and hence, $H^a = H = H'$, again a contradiction.

Finally, assume that $B, B' \in T_1 \cup T_2$. Write $a = s + j$ for $s \in S$ and $j \in J(A)$, and say $B = M \oplus J(A)$ and $B' = M' \oplus J(A)$ for some subalgebras $M, M'$ of $S$. Observe that $M^s = M'$ since $J(A)$ is a two-sided ideal of $A$. Since $S$ is semisimple and all of its simple components commute with each other, the only remaining possibility is that there exists $1 \leq j_1 < j_2 \leq r$ and $l, l' \in \mathbb{Z}/m_{j_1}\mathbb{Z}$ such that $B = (S_{j_1,j_2} \times \prod_{i \neq j_1,j_2} S_i) \oplus J(A)$ and $B' = (S_{j_1,j_2}^{l'} \times \prod_{i \neq j_1,j_2} S_i) \oplus J(A)$. Then applying the aforementioned claim gives us a contradiction. This completes the proof.

We call $T_1 \cup T_2 \cup T_3$ the **standard** set of representatives of the conjugacy classes of maximal subalgebras of $A$.

We now introduce a ‘zeta function’ of $A$. Let $B$ be the standard set of representatives of the conjugacy classes of maximal subalgebras of $A$. For $\varepsilon > 0$, we define

$$
\zeta_A(\varepsilon) = \sum_{B \in B} (|A|/|B|)^{-\varepsilon},
$$

where $\zeta_A(0) = 0$ if $A = k$. Next, we prove a result which serves as a main tool in this paper. Recall the notation $A = (\prod_{i=1}^r M_{n_i}(q^{m_i})) \oplus J(A)$. Denote $n := \min_{i=1,\ldots,r} \{n_i\}$ and $m := \min_{i=1,\ldots,r} \{m_i\}$. 


Theorem 3. Fix constants $\epsilon > 0$, $\lambda > 0$ and $1 < c < q^2$. With the above notation, let $A$ be a finite algebra that is bounded by $(c, \lambda)$. Then $\zeta_A(\epsilon) \to 0$ as $n \to \infty$, as $m \to \infty$ or as $q \to \infty$.

Proof. Fix $\epsilon > 0$. Let $B$ be the standard set of representatives of the conjugacy classes of maximal subalgebras of $A$. Let $B \in B$.

We first consider the case where $A$ is simple, say $A = M_{n}(q^{m})$. Let $\Sigma_{1}$ (resp. $\Sigma_{2}$, $\Sigma_{3}$) be the contribution to the sum in (1) of the maximal subalgebras in $S1$ (resp. $S2$, $S3$). That is, for $i = 1, 2, 3$, denote

$$\Sigma_{i} := \sum_{B \in S_{i}} (|A|/|B|)^{-\epsilon}.$$  

We consider individually each of the possibilities that $B$ is in $S1$, $S2$ or $S3$.

Let $B \in S1$. That is, $B = P_{l,n-l}(q^{m})$ for some positive integer $l < n$. Observe that $|B| = q^{m(n^2 - l(n-l))}$. Then,

$$\Sigma_{1} = \sum_{l=1}^{n-1} q^{-\epsilon ml(n-l)} \leq (n-1)q^{-\epsilon m(n-1)}.$$  

Let $B \in S2$. That is, $B = M_{n}/a(q^{ma})$ for some prime divisor $a$ of $n$. Observe that $|B| = q^{mn^2/a}$. Then,

$$\Sigma_{2} = \sum_{a \in \mathbb{P}(n)} q^{-\epsilon mn^2(1-1/a)} \leq \omega(n)q^{-\epsilon mn^2/2}.$$  

Let $B \in S3$. That is, $B = M_{n}(q^{m/b})$ for some prime divisor $b$ of $m$. Observe that $|B| = q^{mn^2/b}$. Then,

$$\Sigma_{3} = \sum_{b \in \mathbb{P}(m)} q^{-\epsilon mn^2(1-1/b)} \leq \omega(m)q^{-\epsilon mn^2/2}.$$  

Observe that, since $\omega(n) \leq n - 1$, we have

$$\zeta_A(\epsilon) = \Sigma_{1} + \Sigma_{2} + \Sigma_{3} \leq (2(n-1) + \omega(m))q^{-\epsilon mn^2/2}.$$  

So $\zeta_A(\epsilon) \to 0$ as $n \to \infty$, as $m \to \infty$ or as $q \to \infty$.

This completes the proof for the case where $A$ is simple.

We now consider the general case. That is, $A = S \oplus J(A)$ where $S = \prod_{i=1}^{r} S_{i}$ is semisimple and $S_{i} = M_{n_{i}}(q^{m_{i}})$ for each $i$. Let $\Omega_{1}$ (resp. $\Omega_{2}$, $\Omega_{3}$) be the contribution to the sum in (1) of the maximal subalgebras in $T1$ (resp. $T2$, $T3$). That is, for $i = 1, 2, 3$ say

$$\Omega_{i} := \sum_{B \in T_{i}} (|A|/|B|)^{-\epsilon}.$$  

Let $i_{0} \in \{1, \ldots, r\}$ satisfy $\zeta_{S_{i_0}}(\epsilon) \geq \zeta_{S_{i}}(\epsilon)$ for all $1 \leq i \leq m$. For simplicity, denote $n_{0} := n_{i_0}$ and $m_{0} := m_{i_0}$.

Let $c \in \mathbb{R}$ such that $1 < c < q^\epsilon$ and let $\lambda > 0$. We impose the condition that $A$ is bounded by $(c, \lambda)$. That is, $r \leq \lambda c^{\min\{m, n\}/2}$ and $\dim J(A)/J(A)^{2} \leq \log_{q}\lambda + \min\{m, n\}2\log_{q}c$. Rearranging this second inequality gives us $|J(A)/J(A)^{2}| \leq \lambda c^{\min\{m, n\}/2}$.
Let \( B \in T_1 \). That is, 
\[ B = (B_j \times \prod_{i \neq j} S_i) \oplus J(A) \]
for some \( j \in \{1, \ldots, r\} \) and maximal subalgebra \( B_j \) of \( S_j \). Then, we have 
\[ \Omega_1 = \sum_{j=1}^{r} \zeta_{S_j}(\varepsilon) \leq r \zeta_{S_0}(\varepsilon) \leq r(2(n_0 - 1) + \omega(m_0))q^{-\epsilon m_0 n_0/2}. \]
So, \( \Omega_1 \to 0 \) as \( n \to \infty \), as \( m \to \infty \) or as \( q \to \infty \).

Let \( B \in T_2 \). That is, 
\[ B = (S \times S)^{\times} \times \prod_{i \neq j} S_i \oplus J(A) \]
for some \( 1 \leq j_1 < j_2 \leq r \) such that \( S_{j_1} \cong S_{j_2} \) and some \( l \in \mathbb{Z}/m_{j_1} \mathbb{Z} \). Consider the identity 
\[ x \leq q^{2x/3} \]
which holds for any \( q \geq 2 \) and \( x \in \mathbb{R} \).
Applying it to \( x = \varepsilon m n^2 \) and rearranging gives us 
\[ \varepsilon m n^2 q^{-\epsilon m n^2} \leq q^{-\epsilon m n^2/3}. \]
Combining this with 
\[ |A|/|B| = |S_{j_1}| \]
gives us 
\[ \Omega_2 \leq \sum_{1 \leq j_1 < j_2 \leq r} m_{j_1} q^{-\epsilon m_{j_1}(n_{j_1})^2} \leq \binom{r}{2} \varepsilon^{-1} q^{-\epsilon m n^2/3}. \]
So, \( \Omega_2 \to 0 \) as \( n \to \infty \), as \( m \to \infty \) or as \( q \to \infty \).

Finally, let \( B \in T_3 \). That is, 
\[ B = S \oplus H \]
where \( H \) is a two-sided ideal of \( A \) that is maximal with respect to the condition \( H \subset J(A) \).
Let \( S_{op} \) denote the opposite algebra of \( S \). Observe that \( J(A)/H \) is a non-trivial simple \( S \)-bimodule, and hence, by the equivalence of categories in [19, Proposition 10.1], \( J(A)/H \) also has the structure of a non-trivial simple left \( S \otimes_k S_{op} \)-module. Consider the \( k \)-algebra isomorphism 
\[ S \otimes_k S_{op} \cong \prod_{1 \leq i, j \leq r} M_{n_i n_j}(q^{m_i m_j}). \]
Then, by [19, Proposition 2.3], any simple left module of \( S \otimes_k S_{op} \) is isomorphic to \( (\mathbb{F}(q^{m_i m_j})) n_i n_j \) for some \( i, j \in \{1, \ldots, r\} \). Hence, \( |A|/|B| = |J(A)/H| \geq q^{m_i n_i^2} \).

Let \( H \) be the set of two-sided ideals of \( A \) that are maximal with respect to being properly contained in \( J(A) \). By the proof of Theorem 2.5 of [7], all ideals in \( H \) contain \( J(A)^2 \). So, certainly \( |H| \leq |J(A)/J(A)^2| \).
Hence 
\[ \Omega_3 \leq q^{-\epsilon m n^2} |J(A)/J(A)^2| \leq \lambda q^{m_i n_i^2(-\varepsilon + \log_q c)}. \]
So, \( \Omega_3 \to 0 \) as \( n \to \infty \), as \( m \to \infty \) or as \( q \to \infty \). This completes the proof.

**Corollary 4.** Let \( \varepsilon > 0 \) and let \( A \) be a finite simple algebra. Then \( \zeta_A(\varepsilon) \to 0 \) as \( |A| \to \infty \).

**Proof.** Write \( A = M_n(q^m) \). Recall from the proof of Theorem 3 that \( \zeta_A(\varepsilon) \to 0 \) as \( n \to \infty \), as \( m \to \infty \) or as \( q \to \infty \). The result follows immediately as \( |A| = q^{mn^2} \).

**Lemma 5.** Let \( A \) be a finite algebra and let \( S \) be a semisimple subalgebra of \( A \) such that \( A = S \oplus J(A) \). Then \( A^X = S^X \times J(A) \) and \( A^N = S^N \times J(A) \), where \( \times \) denotes Cartesian product of sets.

**Proof.** Let \( g \in A^X \). Write \( g = s + j \) and \( g^{-1} = s' + j' \) for \( s, s' \in S \) and \( j, j' \in J(A) \). Then \( 1 = gg^{-1} = ss' + sj' + js' + jj' \), where \( sj' + js' + jj' \in J(A) \). Hence, \( s' = s^{-1} \). Conversely, let \( a = s_0 + j_0 \in S^X \times J(A) \). Then, \( a = s_0(1 + s_0^{-1}j_0) \), which is a product of units in \( A^X \).

Let \( x \in A^N \) and let \( \alpha \) be the (nilpotency) index of \( x \). Write \( x = x_1 + j_1^0 \) for \( x_1, j_1 \in J(A) \). Then \( 0 = x^\alpha = s_1^\alpha + j_1^\alpha \), where \( s_1^\alpha \in S \). Conversely, let \( y = s_2 + j_2 \in S^N \times J(A) \) and let \( \beta \) be the index of \( s_2 \). Then, \( y^\beta \in J(A) \) and so \( y \in A^N \).
For positive integers \( u, v \), define a function

\[
F(u, v) = (1 - u^{-1})(1 - u^{-2}) \cdots (1 - u^{-v})
\]

where \( F(u, 0) = 1 \). This function is also known as the \( q \)-Pochhammer symbol \((u^{-1}; u^{-1})_v \) (a.k.a. \( q \)-shifted factorial, refer to (1.2.15) of [6]). We will need the following elementary lemmas.

**Lemma 6.** Let \( u, v, c \in \mathbb{N} \). Then \( F(u, v)^c \leq F(u^c, v) \leq 2^v F(u, v) \).

*Proof.* If \( u = 1 \), then \( F(u, v) = 0 \) and the inequality holds. So, assume that \( u > 1 \).

Observe that \( u^c - (u - 1)^c \geq 1 \). Rearranging, we have \( 1 - u^{-c} \geq (1 - u^{-1})^c \). The lower bound then follows immediately since \( u \) is arbitrary.

For the upper bound, observe that \( (1 - u^{-c}) \leq 2(1 - u^{-1}) \). Then we are done again since \( u \) is arbitrary.

**Lemma 7.** Let \( u, v, w \in \mathbb{N} \) such that \( w < v \). Then \( F(u, v) \leq \left( \frac{3}{2} \right)^{v/2} F(u, w) F(u, v - w) \).

*Proof.* If \( u = 1 \), then we are done. So, assume that \( u > 1 \). Let \( x \in \mathbb{N} \). We first show that

\[
\frac{(1 - u^{-(x+1)}) \cdots (1 - u^{-2x})}{(1 - u^{-1}) \cdots (1 - u^{-x})} \leq \left( \frac{3}{2} \right)^x
\]

by induction on \( x \). If \( x = 1 \), then it certainly holds. If \( x > 1 \), then

\[
\frac{(1 - u^{-(x+1)}) \cdots (1 - u^{-2x})}{(1 - u^{-1}) \cdots (1 - u^{-x})} \leq \left( \frac{3}{2} \right)^{x-1} \frac{1 - u^{-2x}}{1 - u^{-x}} \leq \left( \frac{3}{2} \right)^x
\]

using the inductive hypothesis.

Without loss of generality, assume that \( w \leq v/2 \) (otherwise we swap \( w \) and \( v - w \)). Using (2), we have

\[
\frac{F(u, v)}{F(u, w)F(u, v - w)} = \frac{(1 - u^{-(v-w+1)}) \cdots (1 - u^{-v})}{(1 - u^{-1}) \cdots (1 - u^{-w})} \leq \frac{(1 - u^{-(v/2)+1}) \cdots (1 - u^{-2[v/2]})}{(1 - u^{-1}) \cdots (1 - u^{-[v/2]})} \leq \left( \frac{3}{2} \right)^{v/2}.
\]

One can use Leibniz’s alternating series test to show that \( F(u, v) \) converges towards a positive limit as \( v \to \infty \) and \( u \geq 1 \) is fixed (this goes all the way back to Euler, see, for instance, [6, p.xvi]). We denote this limit by \( \phi(1/u) \), for example, \( \phi(1/2) \approx 0.2888 \). It is known that \( \phi(1/u) \) is transcendental.

**Lemma 8.** Let \( A \) be a finite simple algebra, say \( A = M_n(q^m) \). Then

\[
\phi(1/2) < \frac{|A^X|}{|A|} = F(q^m, n) < 1.
\]
Proof. It is easy to check that $|A^X|/|A| = q^{-mn^2} \prod_{i=0}^{n-1}(q^m - q^i) = F(q^m, n)$. Observe that $F(q^m, n)$ is monotonically decreasing (resp. increasing) in $n$ (resp. $q^m$). Then the result follows from the remark preceding this lemma.

Finally, we will need the elementary inequality

$$x/y \leq (x-1)/(y-1) \leq 2x/y$$

for all integers $x \geq y \geq 2$.

3 PROOF OF THEOREM 1.1 AND COROLLARY 1.2

Let $A$ be a finite algebra, say $A = S \oplus J(A)$ where $S = \prod_{i=1}^{r} S_i$ is semisimple and $S_i = M_{n_i}(q^{m_i})$ for each $i$. Denote $n := \min_{i=1,\ldots,r}\{n_i\}$ and $m := \min_{i=1,\ldots,r}\{m_i\}$. Recall that $\phi(1/2) \approx 0.2888$.

We begin by considering two examples. Let $p$ be a prime. Let $A = M_p(2p)$ and let $B = M_p(2)$. Then

$$|A^X|/|A| = F(2p, p)/F(2p, 2p) \to \phi(1/2)^{-1}$$

as $p \to \infty$. Now let $A = M_p(2)$ and let $B = F_{2p}$. Then

$$|A^X|/|A| = F(2p, 2)/F(2p, 1) \to \phi(1/2)$$

as $p \to \infty$. So, we see that the constants in the following lemma are best possible.

Lemma 9. Let $B$ be a maximal subalgebra of $A$. Then, $\phi(1/2) < |A^X|/|A| < \phi(1/2)^{-1}$.

Proof. We first consider the case where $A$ is simple. That is, $A = M_n(q^m)$. Note that $A^X = GL_n(q^m)$. For simplicity, denote $t := q^m$.

Assume that $B$ is of type (S1). That is, $B \cong P_{l, n-l}(t)$ for some positive integer $l < n$. Observe that $|B^X| = |(B/J(B))^X|/|J(B)|$ by Lemma 5. Then applying Lemma 8 gives us

$$|A^X|/|B^X|/|A| = |M_{l}(t)|/|M_{l}(t)^X|/|M_{n-l}(t)|/|M_{n-l}(t)^X| = \frac{F(t, n)}{F(t, l)F(t, n-l)},$$

and hence,

$$\phi(1/2) < \frac{|A^X|/|B^X|/|A|}{\frac{1}{F(t, l)}} < \phi(1/2)^{-1}.$$

Now assume that $B$ is not of type (S1). Then $B$ is simple by Theorem 1. Hence, by Lemma 8, we have

$$\phi(1/2) < \frac{|A^X|/|B^X|/|A|}{\frac{1}{F(t, l)}} < \phi(1/2)^{-1}.$$

This completes the proof for the case where $A$ is simple.

We now consider the general case. Recall that $A = S \oplus J(A)$ where $S = \prod_{i=1}^{r} S_i$ is semisimple. By Theorem 2, $B$ is of type (T1), (T2) or (T3). We consider each of these possibilities.
Let $B$ be of type (T1). That is, $B \cong (B_j \times \prod_{i \neq j} S_i) \oplus J(A)$ for some $j \in \{1, \ldots, r\}$ and maximal subalgebra $B_j$ of $S_j$. Applying Lemma 5 gives us

$$\frac{|A^\times|}{|B^\times|} = \frac{\prod_{i=1}^r |S_i^\times|}{|B_j^\times| \cdot \prod_{i \neq j} |S_i^\times|} = \frac{|S_j^\times|}{|B_j^\times|}.$$ 

Since $S_j$ is simple, Lemma 8 gives us

$$\phi(1/2) \frac{|A|}{|B|} = \phi(1/2) \frac{|S_j|}{|B_j|} < \phi(1/2)^{-1} \frac{|A^\times|}{|B^\times|} < \phi(1/2)^{-1} \frac{|S_j^\times|}{|B_j^\times|} = \phi(1/2)^{-1} \frac{|A|}{|B|}.$$

Let $B$ be of type (T2). That is, $B \cong (\prod_{i \neq j_0} S_i) \oplus J(A)$ for some $j_0 \in \{1, \ldots, r\}$. Again, using Lemma 5, we have

$$\frac{|A^\times|}{|B^\times|} = \frac{\prod_{i=1}^r |S_i^\times|}{\prod_{i \neq j_0} |S_i^\times|} = |S_{j_0}^\times|.$$ 

Again, using Lemma 8, we have

$$\phi(1/2) \frac{|A|}{|B|} = \phi(1/2) |S_{j_0}| < \frac{|A^\times|}{|B^\times|} < \frac{|A|}{|B|}.$$

Finally, let $B$ be of type (T3). That is, $B \cong S \oplus H$ where $H$ is a two-sided ideal of $A$ that is maximal with respect to the condition $H \subset J(A)$. Then,

$$\frac{|A^\times|}{|B^\times|} = \frac{|J(A)|}{|H|} = \frac{|A|}{|B|}$$

by Lemma 5 and since $J(B) \cong H$.

This completes the proof of the lemma.

Let $x, y \in A$ be chosen uniformly at random. If $\langle x, y \rangle \neq A$, then $x$ and $y$ are both contained in a maximal subalgebra $B$ of $A$. For a given $B$, the probability that this occurs is $|B|^2/|A|^2$. Let Max $A$ denote the set of maximal subalgebras of $A$. Then

$$1 - P(A) = P(\langle x, y \rangle \neq A) \leq \sum_{B \in \text{Max } A} |B|^2/|A|^2. \quad (4)$$

Let $B$ be the standard set of representatives of the conjugacy classes of maximal subalgebras of $A$. For a given $B \in B$, there are $|A^\times|/|N_{A^\times}(B^\times)|$ conjugates of $B$ in $A$. Combining (4) with Lemma 9 gives us

$$1 - P(A) \leq \phi(1/2)^{-1} \sum_{B \in B} (|A|/|B|)^{-1} = \phi(1/2)^{-1} \zeta_A(1). \quad (5)$$

If $A$ is simple, then, by Corollary 4, $P(A) \to 1$ as $|A| \to \infty$. This completes the proof of Corollary 1.2.
Let $c \in \mathbb{R}$ such that $1 < c < q$ and let $\lambda > 0$. For the general case, we need the assumption that $A$ is bounded by $(c, \lambda)$. Then, by Theorem 3 (and its proof), $P(A) \to 1$ as $n \to \infty$, as $m \to \infty$ or as $q \to \infty$. This completes the proof of Theorem 1.1.

4 PROOF OF THEOREM 1.3

Let $A$ be a finite simple algebra. Write $A = M_n(q^m)$. Recall from §3 that

$$1 - P(A) \leq \sum_{B \in B} \frac{|B|^2|A^X|}{|A|^2|N_{A^X}(B^\infty)|} \leq \phi(1/2)^{-1} \zeta_A(1).$$  (6)

Since $\phi(1/2) \approx 0.2888$, it suffices to show that $\zeta_A(1) \leq 0.18$. We will first show that $\zeta_A(1) \leq 0.18$ if $n \neq 1$ and $(m, n) \neq (1, 2), (1, 3), (1, 4)$ or $(2, 2)$. We will then consider the remaining cases.

Recall from the proof of Theorem 3 that

$$\zeta_A(1) \leq (2(n - 1) + \omega(m))q^{-m(n-1)}.$$  

It follows that $\zeta_A(1) \leq 0.18$ if $n \neq 1$ and $(m, n) \neq (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 7), (2, 2), (2, 3), (3, 2)$ or $(4, 2)$. For some of these remaining cases, we compute $\zeta_A(1)$ directly.

- If $(m, n) = (1, 5)$, then $\zeta_A(1) = 2q^{-4} + 2q^{-6} + q^{-20} \leq 0.16$.
- If $(m, n) = (1, 6)$, then $\zeta_A(1) = 2q^{-5} + 2q^{-8} + q^{-18} + q^{-24} \leq 0.08$.
- If $(m, n) = (1, 7)$, then $\zeta_A(1) = 2q^{-6} + 2q^{-10} + 2q^{-12} + q^{-42} \leq 0.04$.
- If $(m, n) = (2, 3)$, then $\zeta_A(1) = 2q^{-4} + q^{-12} + q^{-9} \leq 0.13$.
- If $(m, n) = (3, 2)$, then $\zeta_A(1) = q^{-3} + q^{-6} + q^{-8} \leq 0.15$.
- If $(m, n) = (4, 2)$, then $\zeta_A(1) = q^{-4} + q^{-8} + q^{-8} \leq 0.08$.

At this point, we have shown that $P(A) > 3/8$ if $n \neq 1$ and $(m, n) \neq (1, 2), (1, 3), (1, 4)$ or $(2, 2)$. For the remaining cases, we use other methods to bound $P(A)$. Define

$$\nu_q(x) := \frac{1}{x} \sum_{d|x} \mu(d)q^{x/d},$$

where $\mu$ is the Möbius function.

Let $n = 1$. Let $G(A)$ be the set of generators of $A$ as a $k$-algebra. That is, $G(A)$ is the subset of $A$ consisting of all elements whose minimal polynomial over $k$ has degree $m$. It is a classical result, dating back to Gauss, that the number of monic irreducible polynomials over $k$ of degree $m$ is $\nu_q(m)$. So, $|G(A)| = m\nu_q(m)$. Hence

$$P(A) \geq m\nu_q(m)q^{-m} \geq 1 - q^{-1} \geq 1/2.$$  

Now let $(m, n) = (1, 2)$. Then, by Equation (9) of [9], we have

$$P(A) = (q - 1)(q^2 - 1)q^{-3} \geq 3/8$$

with equality if and only if $q = 2$.  

If \((m, n) = (2, 2)\), then we have just shown that the probability of two randomly chosen elements of \(A\) generating \(A\) as a \(\mathbb{F}_{q^2}\)-algebra is strictly greater than \(3/8\). So, certainly, \(P(A) > 3/8\) as a \(\mathbb{F}_q\)-algebra.

Let \((m, n) = (1, 3)\). By Equation (10) of [9], we have

\[
P(A) = (q^2 - 1)^2(q^3 - 1)q^{-7} \geq 63/128.
\]

Let \((m, n) = (1, 4)\). Then,

\[
\sum_{B \in \mathcal{A}} \frac{|B|^2|A^x|}{|A|^2|N_{A^x}(B^x)|} = 2q^{-6}q^4 - 1 + q^{-8}(q^4 - 1)(q^3 - 1) + 2^{-1}q^{-16}(q^4 - q)(q^4 - q^3)
\]

\[
= 2^{-1}q^{-12}(4q^9 + 6q^8 + 6q^7 + 8q^6 + 2q^5 + 3q^4 - q^3 - q + 1)
\]

\[
\leq 0.61.
\]

Hence \(P(A) > 3/8\) by (6). This completes the proof.

5 \hspace{1cm} PROOF OF THEOREM 1.4

Let \(A\) be a finite simple algebra, say \(A = M_n(q^m)\). Recall that \(m(A)\) is the minimal index of any proper subalgebra of \(A\). Note that \(m(A)\) is undefined if \(m = n = 1\).

**Lemma 10.** Let \(C\) be the set of conjugacy classes of subalgebras of \(A\) that have index \(m(A)\). If \(m > 1\), then let \(p\) be the smallest prime divisor of \(m\). Then \(m(A)\) and \(C\) are as follows:

| \(m(A)\)       | \(|C|\)       | standard reps of \(C\)                                      |
|----------------|--------------|-------------------------------------------------------------|
| \(n > 2\)      | \(q^{m(n-1)}\) | \(P_{1,n-1}(q^m), P_{n-1,1}(q^m)\)                         |
| \(n = 2\)      | \(q^m\)      | 2                                                           |
| \(n = 1, m > 1\)| \(q^{m(1-1/p)}\) | 1                                                           |
|                |               | \(\mathbb{F}_{q^{n/p}}\).                                  |

**Proof.** Let \(B\) be a subalgebra of \(A\) with index \(m(A)\). Then, \(B\) is maximal, so we refer to the classification in Theorem 1.

We first assume that \(n = 1\). There do not exist any subalgebras of \(A\) of type (S1) or (S2). So, \(B \cong q^{m/p}\), where \(p\) is the smallest prime divisor of \(m\). There is one conjugacy class of such a \(B\).

Now assume that \(n > 1\). Observe that \(\dim B\) divides \(\dim A\) if \(B\) is of type (S2) or (S3), whilst \(2 \dim B > \dim A\) if \(B\) is of type (S1). So \(B\) is of type (S1), that is, \(B\) is conjugate to \(P_{1,n-1}(t)\) for some \(1 \leq l < n\). We compute \([A : B] = q^{m(n-1)}\). Hence, \(m(A) = q^{m(n-1)}\), which is realised when \(B\) is conjugate to \(P_{1,n-1}(q^m)\) or to \(P_{n-1,1}(q^m)\). If \(n > 2\), then \(P_{1,n-1}(q^m)\) is not conjugate to \(P_{n-1,1}(q^m)\) (they are not even isomorphic).

Henceforth, assume that \(A\) is not a field. That is, \(n > 1\).

**Lemma 11.** Let \(B\) be a subalgebra of \(A\).

(i) If \([A : B] < m(A)^{4/3}\), then \([A : B] = m(A)\).
If \( m(A)^{4/3} \leq [A : B] < m(A)^{5/3} \), then either \( n = 4, 5 \) or \( 6 \) and \( B \) is conjugate to \( P_{2,n-2}(q^m) \) or \( P_{n-2,2}(q^m) \), or \( B \) is non-maximal in \( A \) and \( B \) does not contain \( Z(A) \).

Proof. Note that \( m(A) = q^{m(n-1)} \) by Lemma 10 (since \( n > 1 \)). We first consider the case where \( B \) is maximal. By Theorem 1, \( B \) is of type \((S1)\), \((S2)\), or \((S3)\). We consider each of these possibilities.

Let \( B \) be of type \((S1)\). That is, \( B \) is conjugate to \( P_{l,n-l}(q^m) \) for some positive integer \( l < n \). Observe that \( [A : B] = q^{m(n-1)} \). If \( l = 1 \) or \( n-1 \), then \( [A : B] = m(A) \). If \( n = 4, 5 \) or \( 6 \) and \( l = 2 \) or \( n-2 \), then \( m(A)^{4/3} \leq [A : B] < m(A)^{5/3} \). Otherwise, \( [A : B] \geq m(A)^{5/3} \).

Now let \( B \) be of type \((S2)\) or \((S3)\). Then, \( [A : B] = q^{m(n-1)} \). So, \( [A : B] \geq q^{m(n-1)} \geq m(A)^{5/3} \). We have shown that there exist no maximal subalgebras (and hence no subalgebras) \( B \) of \( A \) that satisfy \( m(A) < [A : B] < m(A)^{4/3} \). This proves (i).

Now assume (for a contradiction) that \( B \) is a non-maximal \( \mathbb{F}_q \)-subalgebra of \( A \) that contains \( Z(A) \) and satisfies \( m(A)^{4/3} \leq [A : B] < m(A)^{5/3} \). Let \( M \) be a maximal \( \mathbb{F}_q \)-subalgebra of \( A \) that contains \( B \). By the previous argument, either \( M \) is isomorphic to \( P_{1,n-1}(q^m) \) or \( P_{n-1,1}(q^m) \), or \( n = 4, 5 \) or \( 6 \) and \( M \) is isomorphic to either \( P_{2,n-2}(q^m) \) or \( P_{n-2,2}(q^m) \).

Let \( M \cong P_{2,n-2}(q^m) \) and \( n = 4, 5 \) or \( 6 \). It follows from Theorems 1 and 2 that the minimal index of an \( \mathbb{F}_q \)-subalgebra of \( M \) is \( q^{m(n-2)+m} \). Then \( [A : B] \geq q^{2m(n-2)+m} \geq m(A)^{5/3} \), which is a contradiction. An identical argument works for \( M \cong P_{n-2,2}(q^m) \).

Let \( M \cong P_{1,n-1}(q^m) \). Since \( B \) contains \( Z(A) = Z(M) \), we may interpret \( B < M < A \) as a chain of \( \mathbb{F}_q \)-algebras. If \( n = 2 \), then the minimal index of a \( \mathbb{F}_q \)-subalgebra of \( M \) is \( q^{2m} \). Then, \( [A : B] \geq q^{2m} \geq Z(A)^{(5/3)} \). If \( n > 2 \), then, again using Theorems 1 and 2, the minimal index of a \( \mathbb{F}_q \)-subalgebra of \( M \) is \( q^{2m(n-2)+m(n-1)} \). Then, \( [A : B] \geq q^{2m(n-2)+m(n-1)} \geq m(A)^{5/3} \). We have a contradiction, and similarly, for \( M \cong P_{n-1,1}(q^m) \). This proves (ii).

Let \( \{B_i\}_{i=1}^\alpha \) denote the set of maximal subalgebras of \( A \). Let \( \beta \) be the number of maximal subalgebras of \( A \) with index \( m(A) \). We arrange the \( B_i \)'s such that \( B_i \) has index \( m(A) \) if and only if \( i \leq \beta \).

Let \( x : A \to \mathbb{R} \) be defined by \( x(A) := \beta m(A)^{-1} \). Note that \( \sum_{1 \leq i \leq \beta} [A : B_i]^{-2} = x(A)m(A)^{-1} \).

Let \( x, y \in A \) be chosen uniformly at random. If \( \langle x, y \rangle \neq A \), then \( x \) and \( y \) are both contained in a maximal subalgebra of \( A \). For a given \( B_i \), the probability that this occurs is \( |B_i|^2/|A|^2 \). Then, as in §3, we have

\[
1 - P(A) \leq \sum_{1 \leq i \leq \alpha} [A : B_i]^{-2} = x(A)m(A)^{-1} + \sum_{\beta+1 \leq i \leq \alpha} [A : B_i]^{-2}.
\]

The probability that \( \langle x, y \rangle \neq A \) is bounded below by \( |\bigcup_{1 \leq i \leq \alpha} B_i \times B_i|/|A \times A| \), and hence, by \( |\bigcup_{1 \leq i \leq \beta} B_i \times B_i|/|A \times A| \). Using the inclusion–exclusion principle, we obtain

\[
1 - P(A) \geq x(A)m(A)^{-1} - \sum_{1 \leq i < j \leq \beta} [A : B_i \cap B_j]^{-2}.
\]

Let \( \xi = \xi(n) \) be defined by \( \xi = 2 \) if \( n > 2 \) and \( \xi = 1 \) if \( n = 2 \).

Lemma 12. \( \beta = \xi(q^{mn} - 1)/(q^m - 1) \).
Proof. Recall from Lemma 10 that \( \{B_i \mid i = 1, \ldots, \beta \} \) splits into \( \xi \) conjugacy classes. Let \( i \in \{1, \ldots, \beta \} \). Again, by Lemma 10, \( B_i \) is isomorphic to either \( P_{1,n-1}(q^m) \) or \( P_{n-1,1}(q^m) \). So, \( B_i^\times \) is self-normalising in \( A^\times \). Hence, there are \( |A^\times|/|B_i^\times| = (q^{mn} - 1)/(q^m - 1) \) conjugates of \( B_i \) in \( A \).

We are now able to bound \( \kappa(A) \).

**Corollary 13.** \( 1 < \kappa(A) < 4 \).

**Proof.** Observe that \( \kappa(A) = \xi q^{-m(n-1)}(q^{mn} - 1)/(q^m - 1) \) by Lemmas 10 and 12. It is then easy to check that \( 1 < \kappa(A) < 4 \).

Note that the bounds in Corollary 13 are best possible. For example, if \( n = 2 \), then \( \kappa(A) \to 1 \) as \( q \to \infty \) or as \( m \to \infty \). If \( q = 2 \) and \( m = 1 \), then \( \kappa(A) \to 4 \) as \( n \to \infty \).

It remains to estimate the final term in both of the inequalities (7) and (8).

**Lemma 14.** \( \sum_{\beta+1<i\leq\alpha}[A : B_i]^{-2} = O(m(A)^{-4/3}) \).

**Proof.** Let \( A \) be the standard set of representatives of the conjugacy classes of maximal subalgebras of \( A \). Let \( B_0 \) be the subset of \( B \) consisting of subalgebras with index \( m(A) \). Let \( B \in B \setminus B_0 \). Note that there are \( [A^\times : N_{A^\times}(B^\times)] \) conjugates of \( B \) in \( A \).

Let \( \rho(A) \) denote the number of conjugacy classes of maximal subalgebras of \( A \). Observe that \( \rho(A) = n - 1 + \omega(n) + \omega(m) \) by Theorem 1. Recall from Lemma 10 that \( m(A) = q^{m(n-1)} \). If \( m(A) \to \infty \), then at least one of the following occurs: \( n \to \infty \), \( m \to \infty \) or \( q \to \infty \). So, \( \rho(A)m(A)^{-1/3} \to 0 \) as \( m(A) \to \infty \). That is,

\[
\rho(A) = o(m(A)^{1/3}).
\]  

Combining (9) with Lemmas 9 and 11 gives us

\[
\sum_{\beta+1<i\leq\alpha}[A : B_i]^{-2} = \sum_{B \in B \setminus B_0}[A : B]^{-2}[A^\times : N_{A^\times}(B^\times)]
\]

\[
< \phi(1/2)^{-1} \left( 2m(A)^{-4/3} + \rho(A)m(A)^{-5/3} \right)
\]

\[
= O(m(A)^{-4/3}).
\]

We note that the constant \( 4/3 \) in Lemma 14 is best possible. For example, consider the case where \( n = 4 \) and \( B = P_{2,2}(q^m) \). Then \( m(A) = q^{3m} \) and \( [A : B] = q^{4m} \).

**Lemma 15.** \( \sum_{1\leq i<j\leq\beta}[A : B_i \cap B_j]^{-2} = O(m(A)^{-4/3}) \).

**Proof.** Fix \( i, j \) such that \( 1 \leq i < j \leq \beta \). By Lemma 10, \( B_i \) and \( B_j \) are both over \( \mathbb{F}_{q^m} \). So, \( B_i \cap B_j \) is a \( \mathbb{F}_{q^m} \)-algebra that is not maximal in \( A \). Hence, \( [A : B_i \cap B_j] \geq m(A)^{5/3} \) by Lemma 11. Then

\[
\sum_{1\leq i<j\leq\beta}[A : B_i \cap B_j]^{-2} \leq \beta^2 m(A)^{-10/3} < 16m(A)^{-4/3}
\]

using Corollary 13.
The theorem then follows from combining the inequalities (7) and (8) with Corollary 13 and Lemmas 14 and 15.

We conclude this section with the following estimate of the zeta function of $A$. Let $\epsilon > 0$. By the same argument as in the proof of Lemma 14, it is easy to see that $\rho(A) = o(m(A)^{\epsilon / 3})$. Combining this with Lemmas 10 and 11 gives us

$$\zeta_A(\epsilon) = \delta(A)m(A)^{-\epsilon} + O(m(A)^{-4\epsilon / 3}),$$

(10)

where $\delta : A \to \mathbb{R}$ is a function given by $\delta(A) = 1$ if $n = 2$ and $\delta(A) = 2$ otherwise.

## 6 | PROOF OF THEOREM 1.5 AND COROLLARY 1.6

Let $A$ be a finite algebra, say $A = S \oplus J(A)$ where $S = \prod_{i=1}^{r} S_i$ is semisimple and $S_i = M_{n_i}(q^{m_i})$ for each $i$. Denote $n := \min_{i=1,\ldots,r}\{n_i\}$ and $m := \min_{i=1,\ldots,r}\{m_i\}$. If $A$ is simple, note that $n = 1$ if and only if $A$ is a field.

Recall that $A^N$ refers to the set of nilpotent elements of $A$, and that $P_N(A)$ is the probability that two elements of $A^N$ chosen uniformly at random will generate $A$ as a $k$-algebra.

Let $T$ denote the group of scalar matrices of $S^\times$. Recall that $\phi(1/2) \approx 0.2888$. Assume that $n > 1$.

We will need the following lemma.

**Lemma 16.** Let $B$ be a maximal subalgebra of $A$. Then $\frac{|B^N|A^X|}{|A^N|N_{A^X}(B^X)|} < \phi(1/2)^{-1}\left(\frac{|A|}{|B|}\right)^{-\frac{1}{2}}$.

**Proof.** We first consider the case where $A$ is simple. That is, $A = M_{n}(q^{m})$. For simplicity, denote $t := q^m$. By Theorem 1, $B$ is of type (S1), (S2) or (S3). We consider individually each of these possibilities. We will repeatedly use the fact that $|A^N| = t^{n^2-n}$, which was proved in [5, Theorem 1].

Let $B$ be of type (S1). That is, $B \cong P_{l,n-l}(t)$ for some positive integer $l < n$. Observe that $|B^N| = |(B/J(B))^N| |J(B)|$ by Lemma 5. Then we have

$$\frac{|B^N|}{|A^N|} = \frac{t^l}{t^{-l}} \cdot t^{(n-l)^2-(n-l)} \cdot t^{l(n-l)} \cdot t^{-l(n-l)} = \frac{|B|}{|A|}.$$ 

Let $B$ be of type (S2). That is, $B \cong M_{n/a}(t^a)$ for some prime divisor $a$ of $n$. Then

$$\frac{|B^N|}{|A^N|} = \frac{t^{a(n^2/a^2-n/a)}}{t^{n^2-n}} = t^{-n^2/(1-1/a)} = \frac{|B|}{|A|}.$$ 

Hence, by Lemma 9, we have

$$\frac{|B^N|N_{A^X}(B^X)|}{|A^N|^2|N_{A^X}(B^X)|} < \phi(1/2)^{-1}\left(\frac{|A|}{|B|}\right)^{-\frac{1}{2}}$$

for all $B$ of type (S1) or (S2).

Let $B$ be of type (S3). That is, $B \cong M_{n}(t^{1/b})$ for some prime divisor $b$ of $m$. Observe that $N_{A^X}(B^X) = B^X T$, and so, $|N_{A^X}(B^X) : B^X| = (t-1)/(t^{1/b} - 1) \geq t^{1-1/b}$ (using (3)). Then
\[
\frac{|B^N|^2|A^x|}{|A^N|^2|N_{A^x}(B^x)|} < \frac{t^{2(n^2-n)/b}}{t^{2(n^2-n)}} \cdot \phi(1/2) - t^{n^2(1-1/b)} \cdot t^{1/b-1} = \phi(1/2)^{-1}t^{-(1-1/b)(n^2-2n+1)}.
\]

\[
\leq \phi(1/2)^{-1}t^{-(1-1/b)n^2/4} = \phi(1/2)^{-1}\left(\frac{|A|}{|B|}\right)^{-\frac{1}{2}}.
\]

by Lemma 9 and since \(n > 1\). This completes the proof for the case where \(A\) is simple.

We now consider the general case. Recall that \(A = S \oplus J(A)\) where \(S = \prod_{i=1}^{r} S_i\) is semisimple. By Theorem 2, \(B\) is of type (T1), (T2) or (T3). We consider each of these possibilities.

Let \(B\) be of type (T1). That is, \(B \cong (B_j \times \prod_{i \neq j} S_i) \oplus J(A)\) for some \(j \in \{1, \ldots, r\}\) and maximal subalgebra \(B_j\) of \(S_j\). Then, using Lemma 5, we have

\[
\frac{|B^N|^2|A^x|}{|A^N|^2|N_{A^x}(B^x)|} \leq \frac{|B_j^N|^2|S_j^x|}{|S_j^N|^2|N_{S_j^x}(B_j^x)|} < \phi(1/2)^{-1}\left(\frac{|S_j|}{|B_j|}\right)^{-\frac{1}{2}} = \phi(1/2)^{-1}\left(\frac{|A|}{|B|}\right)^{-\frac{1}{2}}.
\]

Let \(B\) be of type (T2). That is, \(B \cong (\prod_{i \neq j_0} S_i) \oplus J(A)\) for some \(j_0 \in \{1, \ldots, r\}\). For simplicity, denote \(n_0 := n_{j_0}\), \(m_0 := m_{j_0}\) and \(t_0 := q_{m_0}\). So, \(S_{j_0} = M_{n_0}(t_0)\). Observe that \(N_{A^x}(B^x) = B^x T\), and so,

\[
|N_{A^x}(B^x)| = |Z(S_{j_0}^x)| = t_0 - 1.
\]

Then

\[
\frac{|B^N|^2|A^x|}{|A^N|^2|N_{A^x}(B^x)|} = \frac{|S_{j_0}^N|^{t_0 - 1}}{|S_{j_0}^N|t_0} = \frac{\prod_{i=0}^{n_0-1}(t_0^n - t_0^i)}{t_0^{2(n_0^2-n_0)}(t_0 - 1)} \leq 2t_0^{-n_0^2/4} = 2\left(\frac{|A|}{|B|}\right)^{-\frac{1}{2}}
\]

using (3) and since \(n_0 > 1\).

Finally, let \(B\) be of type (T3). That is, \(B \cong S \oplus H\) where \(H\) is a two-sided ideal of \(A\) that is maximal with respect to the condition \(H \subset J(A)\). Then

\[
\frac{|B^N|^2|A^x|}{|A^N|^2|N_{A^x}(B^x)|} \leq \frac{|H|}{|J(A)|} = \left(\frac{|A|}{|B|}\right)^{-1}
\]

by Lemma 5. This completes the proof of the lemma.

Let \(x, y \in A^N\) be chosen uniformly at random. If \((x, y) \neq A\), then \(x\) and \(y\) are both contained in a maximal subalgebra \(B\) of \(A\). For a given \(B\), the probability that this occurs is \(|B^N|^2/|A^N|^2\). Let \(\text{Max} A\) denote the set of maximal subalgebras of \(A\). Then

\[
1 - P_N(A) = P((x, y) \neq A) \leq \sum_{B \in \text{Max} A} |B^N|^2/|A^N|^2.
\]

(11)

Let \(B\) be the standard set of representatives of the conjugacy classes of maximal subalgebras of \(A\). For a given \(B \in B\), recall that there are \(|A^x|/|N_{A^x}(B^x)|\) conjugates of \(B\) in \(A\). Combining (11) with Lemma 16 gives us

\[
1 - P_N(A) < \phi(1/2)^{-1} \sum_{B \in B} (|A|/|B|)^{-1/4} = \phi(1/2)^{-1} \xi_A(1/4).
\]

(12)
If $A$ is simple then, by Corollary 4, $P_N(A) \to 1$ as $|A| \to \infty$. This completes the proof of Corollary 1.6.

Let $c \in \mathbb{R}$ such that $1 < c < q^{1/4}$ and let $\lambda > 0$. For the general case, we need the assumption that $A$ is bounded by $(c, \lambda)$. Then, by Theorem 3 (and its proof), $P_N(A) \to 1$ as $n \to \infty$, as $m \to \infty$ or as $q \to \infty$. This completes the proof of Theorem 1.5.

7 PROOF OF THEOREM 1.7

Let $A$ be a finite simple algebra that is not a field. That is, $A = M_n(q^m)$ where $n > 1$. For simplicity, denote $t := q^m$.

Let $f$ be a polynomial of degree $n$ over $\mathbb{F}_t$. Factorise $f = f_1^{\alpha_1} f_2^{\alpha_2} \ldots f_s^{\alpha_s}$ where the $f_i$’s are distinct and irreducible over $\mathbb{F}_t$. For each $i$, let $d_i$ be the degree of $f_i$. Without loss of generality, we assume that $f$ is monic.

Recall that $A_f$ refers to the set of elements of $A$ with characteristic polynomial $f$, and that $P_f(A)$ is the probability that two elements of $A_f$ chosen uniformly at random will generate $A$ as a $k$-algebra.

For positive integers $u, v$, recall the definition $F(u, v) = (1-u^{-1})(1-u^{-2}) \ldots (1-u^{-v})$ and $F(u, 0) = 1$. We will need [21, Theorem 2], which states that

$$|A_f| = t^{n^2-n} \frac{F(t, n)}{\prod_{i=1}^s F(t^{d_i}, \alpha_i)} = t^{-n} |A^x| \frac{1}{\prod_{i=1}^s F(t^{d_i}, \alpha_i)}.$$

**Lemma 17.** Let $B$ be a maximal subalgebra of $A$. There exists an absolute constant $C > 0$ such that

$$\frac{|B_f|^2|A^x|}{|A_f|^2|N_A(B^x)|} \leq C(\frac{|A|}{|B|})^{-\frac{1}{4}}.
$$

**Proof.** By Theorem 1, $B$ is of type (S1), (S2) or (S3). We consider individually each of these possibilities. If $B_f$ is empty, then we are done, so assume otherwise.

Let $B$ be of type (S1). That is, $B \cong P_{l,n-l}(t)$ for some positive integer $l < n$. Let $\Lambda$ be the set of monic polynomials over $\mathbb{F}_t$ that divide $f$ and have degree $l$. We can assume that $\Lambda$ is non-empty (as otherwise $B_f$ is empty). Observe that $|\Lambda| \leq \binom{n}{l}$. Consider a generic element $f_0 \in \Lambda$. Factorise $f_0 = f_1^{\beta_1} f_2^{\beta_2} \ldots f_s^{\beta_s}$, where $0 \leq \beta_i \leq \alpha_i$ for each $i$. Then,

$$|B_f| \leq \sum_{f_0 \in \Lambda} |M_f(t) f_0| |M_{n-l}(t) f_{/f_0}| |J(B)|$$

$$= \sum_{f_0 \in \Lambda} t^{-l} |M_f(t)^x| t^{-(n-l)} |M_{n-l}(t)^x| |J(B)|$$

$$\leq |\Lambda| \left( \frac{3}{2} \right)^{n/2} t^{-n} |B^x| \frac{1}{\prod_{i=1}^s F(t^{d_i}, \alpha_i)}$$

$$\leq \left( \frac{n}{l} \right) \left( \frac{3}{2} \right)^{n/2} \frac{|B^x||A_f|}{|A^x|}
$$

using [21, Lemmas 5, 7 and Theorem 2].
For sufficiently large \( n \), say \( n \geq 200 \), observe that

\[
2l \log_2 n + n \log_2(3/2) \leq 3l(n - l)/4. \tag{13}
\]

Let \( C = 3 \cdot 199^{109} \left( \frac{3}{2} \right)^{199} \). Then, using (13) and Lemma 9, we have

\[
\frac{|B_f|^2 |A^\times|}{|A_f|^2 |N_{A^\times}(B^\times)|} \leq \left( \frac{3}{2} \right)^n \frac{|B^\times|}{|A^\times|} < 3n^{2l} \left( \frac{3}{2} \right)^n \frac{|B|}{|A|} = 3t^{2l \log_2 n + n \log_2(3/2) - l(n - l)} \leq Ct^{-l(n-l)/4} = C \left( \frac{|A|}{|B|} \right)^{1/4}.
\]

Let \( B \) be of type \((S2)\). That is, \( B \cong M_{n/a}(t^a) \) for some prime divisor \( a \) of \( n \). Let \( z \in B_f \). Recall that \( f \) is the characteristic polynomial of \( z \) as an \( n \times n \) matrix over \( \mathbb{F}_t \). Let \( g \) be the characteristic polynomial of \( z \) as an \( n/a \times n/a \) matrix over \( \mathbb{F}_{t^a} \). Let \( \Gamma_a := \text{Gal}(\mathbb{F}_{t^a}/\mathbb{F}_t) \cong \mathbb{Z}_a \).

Without loss of generality, we rearrange the factors of \( f \) such that, for some positive integer \( c \leq s \), \( f_i \) is reducible over \( \mathbb{F}_{t^a} \) if and only if \( i \leq c \).

Let \( i \in \{1, \ldots, s\} \). Let \( g_i \) be a \( \mathbb{F}_{t^a} \)-irreducible factor of \( f_i \). If \( i > c \), then \( f_i = g_i^\alpha \). If \( i \leq c \), then since \( a \) is prime, \( f_i = \prod_{\sigma \in \Gamma_a} g_i^\sigma \) where the \( \Gamma_a \)-conjugates of \( g_i \) are all distinct. So, the polynomials in the set \( \{g_i^\sigma \mid i = 1, \ldots, c; \sigma \in \Gamma_a\} \cup \{g_i \mid i = c + 1, \ldots, s\} \) are all \( \mathbb{F}_{t^a} \)-irreducible and distinct.

Let \( p_i \) be the greatest common divisor of \( f_i^{\alpha_i} \) and \( g_i \). Note that \( f = \prod_{\sigma \in \Gamma_a} g_i^\sigma \) by [17, Lemma 5.1]. So, if \( i > c \), then \( p_i = g_i^{\alpha_i/a} \) and if \( i \leq c \), then \( p_i = \prod_{\sigma \in \Gamma_a} (g_i^\sigma)^{\mathcal{Y}_i} \) where each \( \mathcal{Y}_i \) is a non-negative integer such that \( \sum_{\sigma \in \Gamma_a} \mathcal{Y}_i = \alpha_i \). Given that \( f \) is fixed, observe that there are at most \( a^s \) possibilities for \( g \) (by allowing \( \sum_{\sigma \in \Gamma_a} \mathcal{Y}_i = \alpha_i \) to range over all partitions for each \( i \leq c \)).

Applying [21, Theorem 2], we have

\[
|B_f| \leq a^n \frac{t^{-n}|B^\times|}{\prod_{i=1}^{c} \prod_{\sigma \in \Gamma_a} F(t^{d_i}, \mathcal{Y}_i) \prod_{i=c+1}^{s} F(t^{d_i}, \alpha_i/a)} < n^\alpha 2^{\alpha_1 + \cdots + \alpha_c} \frac{t^{-n}|B^\times|}{\prod_{i=1}^{c} F(t^{d_i}, \alpha_i)} \leq (2n)^{\alpha} \frac{|B^\times| |A_f|}{|A^\times|}.
\]

Observe that \( n \log_2(2n) \leq n^2/4 \) for \( n \geq 22 \). Then,

\[
\frac{|B_f|^2 |A^\times|}{|A_f|^2 |N_{A^\times}(B^\times)|} \leq (2n)^n \frac{|B^\times|}{|A^\times|} < 3(2n)^n \frac{|B|}{|A|}.
\]
\[
= 3t^n \log(2n) - n^2(1 - 1/a)
\leq C t^{-n^2(1 - 1/a)/2}
= C \left( \frac{|A|}{|B|} \right)^{-\frac{1}{2}}
\]

using Lemma 9 and since \(C \geq 3(2 \cdot 21)^{21}\).

Let \(B\) be of type (S3). That is, \(B \cong M_n(t^{1/b})\) for some prime divisor \(b\) of \(m\). Let \(\Gamma_b := \text{Gal}(\mathbb{F}_t/\mathbb{F}_{t^{1/b}}) \cong \mathbb{Z}_b\). We assume that the coefficients of \(f\) lie in \(\mathbb{F}_{t^{1/b}}\) (as otherwise \(B_f\) is empty). That is, \(f\) is \(\Gamma_b\)-stable.

Since \(b\) is prime, each factor \(f_i\) of \(f\) is either over \(\mathbb{F}_{t^{1/b}}\) or \(\prod_{\sigma \in \Gamma_b} f_i^\sigma\) is \(\mathbb{F}_{t^{1/b}}\)-irreducible where the \(\Gamma_b\)-conjugates of \(f_i\) are all \(\mathbb{F}_t\)-irreducible and distinct. Let \(d := \{1 \leq i \leq s \mid f_i\) is over \(\mathbb{F}_{t^{1/b}}\}\}. Since \(f\) is \(\Gamma_b\)-stable, we can rearrange the factors of \(f\) such that \(f_i\) is over \(\mathbb{F}_{t^{1/b}}\) if and only if \(i \leq d\), \(b\) divides \(s - d\) and, for every \(i = 1, \ldots, (s - d)/b\), \(\prod_{j=0}^{b-1} f_{d+i+j(s-d)/b} = \prod_{\sigma \in \Gamma_b} f_{d+i}^\sigma\) and \(\alpha_{d+i} = \alpha_{d+i+(s-d)/b} = \ldots = \alpha_{d+i+(b-1)(s-d)/b}\).

For \(i \in \{1, \ldots, d + (s - d)/b\}\), define a polynomial \(h_i\) by \(h_i = f_i\) if \(i \leq d\) and \(h_i = \prod_{\sigma \in \Gamma_b} f_i^\sigma\) otherwise. Observe that the \(h_i\)'s are all distinct and \(\mathbb{F}_{t^{1/b}}\)-irreducible. Then,

\[
|B_f| = \left( \frac{t^{-n/b} |B^X|}{\prod_{i=1}^d F(t^{d_i/b}, \alpha_i) \prod_{i=d+1}^{d+(s-d)/b} F(t^{d_i}, \alpha_i)} \right) \leq \left( \frac{t^{-n/b} |B^X|}{\prod_{i=1}^d F(t^{d_i/b}, \alpha_i)} \right)
\]

by [21, Theorem 2] and Lemma 6. Recall that \(|N_{A^X}(B^X) : B^X| = (t - 1)/(t^{1/b} - 1)\). Then,

\[
\frac{|B_f|^2 |A^X|}{|A_f|^2 |N_{A^X}(B^X)|} = t^{-2n/b}(t^{1/b} - 1) \prod_{i=1}^s F(t^{d_i}, \alpha_i)^2 |B^X| \leq 6t^{(2n-1)(1-1/b)} \prod_{i=1}^s F(t^{d_i}, \alpha_i)^2 |B| \leq 3 \cdot 2^{2n+1} t^{2(n-1-n^2)(1-1/b)}
\]

\[
\leq \begin{cases} 96t^{-n^2(1-1/b)/4} & \text{if } n = 2 \\ 384t^{(6n-13-n^2)(1-1/b)} & \text{if } n > 2 \\ \leq 384 \left( \frac{|A|}{|B|} \right)^{-\frac{1}{2}} \end{cases}
\]

using (3) and Lemmas 6 and 9.

This proves the lemma, taking \(C = 3 \cdot 199^{199} \left( \frac{3}{2} \right)^{199}\).

Let \(x, y \in A_f\) be chosen uniformly at random. If \(\langle x, y \rangle \neq A\), then \(x\) and \(y\) are both contained in a maximal subalgebra \(B\) of \(A\). For a given \(B\), the probability that this occurs is \(|B_f|^2 / |A_f|^2\). Let \(\text{Max } A\) denote the set of maximal subalgebras of \(A\). Then,

\[
1 - P_f(A) = P(\langle x, y \rangle \neq A) \leq \sum_{B \in \text{Max } A} |B_f|^2 / |A_f|^2.
\]
Let $B$ be the standard set of representatives of the conjugacy classes of maximal subalgebras of $A$. For a given $B \in B$, recall that there are $|A^X|/|N_{A^X}(B^X)|$ conjugates of $B$ in $A$. Combining (14) with Lemma 17 gives us

$$1 - P_f(A) \leq C \sum_{B \in B} (|A|/|B|)^{-1/4} = C\zeta_A(1/4)$$

for some absolute constant $C > 0$. Hence, by Corollary 4, $P_f(A) \to 1$ as $|A| \to \infty$.

## 8 PROOF OF THEOREM 1.8 AND COROLLARY 1.9

Let $A$ be a finite simple algebra, say $A = M_n(q^m)$, where $n \geq 2$ and $m \geq 1$. Let $p$ be the smallest prime divisor of $n$. Let $\alpha := \alpha(n)$ be a positive integer such that $\alpha \leq n$.

Recall that $A_\alpha$ refers to the set of matrices in $A$ with rank $\alpha$, and that $P_\alpha(A)$ is the probability that two elements of $A_\alpha$ chosen uniformly at random will generate $A$ as a $k$-algebra.

For simplicity, denote $t := q^m$. It is a classical result, dating back to [10], that

$$|A_\alpha| = \prod_{i=0}^{\alpha-1} \frac{(tn - ti)^2}{t^\alpha - ti}.$$

We first prove part (i) of the theorem. In part (i), we consider $n$, and hence $\alpha$, to be fixed constants. Assume that $n \geq p\alpha$.

Let $B$ be a subalgebra of $A$ such that $B \cong M_{n/p}(t^p)$. Such a $B$ exists and is maximal by Theorem 1. We claim that

$$\frac{|B_\alpha|}{|A_\alpha|} \geq t^{-p\alpha^2}.$$

We first consider the case where $\alpha = 1$. Then, using (16), we have

$$\frac{|B_\alpha|}{|A_\alpha|} = \frac{t - 1}{t^p - 1} \geq t^{-p}.$$

So, indeed, (17) holds. Next, assume that $\alpha \neq 1$. Once again using (16) gives us

$$\frac{|B_\alpha|}{|A_\alpha|} = \prod_{i=0}^{\alpha-1} \frac{(tn - t^p i)^2(t^\alpha - ti)}{(tn - ti)^2(t^p \alpha - t^pi)} \geq \left(\frac{(tn - t^p(\alpha-1))^2(t^\alpha - t^{\alpha-1})}{t^{2n}(t^p \alpha - t^p(\alpha-1))}\right)^\alpha = \left(t^{-(p-1)\alpha}(1 - t^{-p})(1 - t^{-1})\right)^\alpha \geq t^{-p\alpha^2}.$$

So, we have established (17). Hence,

$$P_\alpha(A) \leq 1 - \frac{|B_\alpha|^2}{|A_\alpha|^2} \leq 1 - t^{-2p\alpha^2}.$$
We now move on to part (ii) of the theorem. We no longer consider $\alpha$ to be a constant, but rather an integer-valued function of $n$, which can vary. Assume that $n - \sqrt{n/3} \leq \alpha \leq n$.

Let $(K)$ be a property of elements of $A$. Let $E$ (resp. $E^K$) be the event that two elements of $A$ chosen uniformly at random generate $A$ (resp. both have property $(K)$). Let $P(E|E^K)$ denote the probability that two random elements of $A$ with property $(K)$ generate $A$.

**Lemma 18.** $P(E|E^K) \geq 1 - \frac{2(2n - 2 + \omega(m))q^{-mn/4}}{P(E^K)}$.

**Proof.** Using elementary probability theory, we have

$$P(E|E^K) = \frac{P(E \cap E^K)}{P(E^K)} \geq 1 - \frac{1 - P(E)}{P(E^K)}.$$ 

Then,

$$P(E|E^K) \geq 1 - \frac{2s_A(1/2)}{P(E^K)} \geq 1 - \frac{2(2n - 2 + \omega(m))q^{-mn/4}}{P(E^K)}$$

using (5) and the proof of Theorem 3.

Let $x \in A$ be chosen uniformly at random. Note that the probability that $x$ is invertible is at least $1/4$. Recall that $\alpha \leq n$. Then, using (3) and (16), we have

$$P(rk(x) = \alpha) = t^{-n^2}|A^\alpha| \geq t^{-n^2} \frac{|GL_n(t)|}{\prod_{j=\alpha}^{n-1}(t^n - t^j)} \prod_{i=0}^{\alpha-1} \frac{(t^n - t^i)^{\alpha - 1}}{t^{\alpha - i}} \geq \frac{1}{4t(n-\alpha)^2}.$$ 

We now apply Lemma 18 where we take $(K)$ to be the property that an element of $A$ has rank $\alpha$. This gives us

$$P_{\alpha}(A) \geq 1 - 32(2n - 2 + \omega(m))q^{-m(n/4 - 2(n - \alpha)^2)}.$$ 

Rearranging $n - \sqrt{n/3} \leq \alpha$ gives us $n/4 - 2(n - \alpha)^2 \geq n/36$, and hence $P_{\alpha}(A) \to 1$ as $|A| \to \infty$. This completes the proof of Theorem 1.8.

Recall that a matrix is invertible if and only if it has full rank. Then Corollary 1.9 follows from applying Theorem 1.8(ii) to the case where $\alpha = n$.

### 9 | THE MINIMAL NUMBER OF GENERATORS

Let $d(A)$ be the minimal number of generators of a finite algebra $A$. Recall our convention that subalgebras of $A$ contain the multiplicative identity of $A$. For an ideal $I$ of $A$, we define $d(I)$ to be the minimal number of generators of $I$ as a non-unital algebra.

We begin with the following elementary observation.

**Lemma 19.** Let $A$ be a finite algebra and let $I$ be an ideal of $A$. Then

$$d(A/I) \leq d(A) \leq d(A/I) + d(I).$$
Proof. Take the image/preimage of a generating set under the natural projection $A \to A/I$.

We now characterise when $d(A) \leqslant 1$. Recall that

$$\nu_q(x) := \frac{1}{x} \sum_{d \mid x} \mu(d) q^{x/d},$$

where $\mu$ is the Möbius function.

**Lemma 20.** Let $A$ be a finite algebra. Then the following hold.

(i) $d(A) = 0$ if and only if $A = k$.

(ii) If $d(A) = 1$, then $\dim A > 1$ and $A/J(A) = \prod_{i=1}^{r} (F_{q^{m_i}})^{\alpha_i}$ where $1 \leq m_1 < \ldots < m_r$ and $\alpha_i \leq \nu_q(m_i)$ for each $i$. If $A$ is semisimple, then the converse holds.

**Proof.**

(i) We have $d(A) = 0$ if and only if $A$ does not have a maximal subalgebra if and only if $A = k$.

(ii) We first consider the case where $A$ is simple, say $A = M_{n}(q^{m})$.

If $d(A) = 1$, then $A$ must be commutative, that is, it is a field. Conversely, let $A = F_{q^{m}}$ for $m > 1$. Any generator of the multiplicative group $A^\times$ then generates $A$ as an algebra.

Now consider the case where $A = S^\alpha$ for simple $S$.

Let $d(A) = 1$. Then $S$ is a field by Lemma 19 and the above arguments. Write $S = F_{q^{m}}$. Recall from the proof of Theorem 1.3 that the number of generators of $S$ as a $k$-algebra is $mn_{q}(m)$. By [9, Theorem 6.3], $A$ can be generated by 1 element if and only if $\alpha \leq \nu_q(m)$. The converse follows immediately.

Next consider the case where $A$ is semisimple, say $A = \prod_{i=1}^{r} S_{\alpha_i}^{\alpha_i}$ where the $S_{\alpha_i}$’s are pairwise non-isomorphic simple algebras. It follows from [9, Proposition 2.12] that $d(A) = \max_{i=1,\ldots,r} \{d(S_{\alpha_i}^{\alpha_i})\}$. The result then follows from Lemma 19 and the above arguments.

Finally, we consider the general case. If $d(A) = 1$, then $d(A/J(A)) \leq 1$ by Lemma 19. This completes the proof.

**Corollary 21.** Let $A$ be a finite simple algebra over $k$. Then

$$d(A) = \begin{cases} 2 & \text{if } A \text{ is not a field} \\ 1 & \text{if } A \text{ is a field and } A \neq k \\ 0 & \text{if } A = k \end{cases}$$

**Proof.** By [9, Theorem 6.4], $A$ is 2-generated. The result then follows immediately from Lemma 20.

Let $P(A, l)$ be the probability that $l$ elements of $A$ chosen uniformly at random will generate $A$ as a $k$-algebra. Note that $P(A, l) \geq P(A, l_0)$ for all $l \geq l_0$. Recall our previous notation $P(A) := P(A, 2)$.

**Proof of Theorem 1.10.**

Proof. We first consider the case where $r = 1$ and $J(A) = 0$. Write $A = S^\alpha$ where $S = M_{n}(q^{m})$. In this case, $f(A) = m^{-1}n^{-2} \log_q \alpha m$. 
If \( d(A) = 0 \), then \( A = k \) by Lemma 20 and the result is immediate. If \( d(A) = 1 \), then \( S \) is a field and \( \alpha \leq \nu_q(m) \) by Lemmas 19 and 20. Observe that \( P(S, 1) = m\nu_q(m)q^{-m} \leq 1 \) as in the proof of Theorem 1.3. So, \( f(A) = m^{-1}\log_q am \leq m^{-1}\log_q P(S, 1) + 1 \leq 1 \), and the result holds.

By [9, Theorem 6.3], \( A \) can be generated by \( l \) elements if and only if

\[
\alpha \leq \frac{q^{lmn^2}P(S, l)}{m|PGL_n(q^m)|}.
\]  

(18)

If \( d(A) = 2 \), then plugging \( l = 2 \) into (18) and using Lemma 8 gives us

\[
f(A) \leq m^{-1}n^{-2}\log_q(q^{mn^2}(q^m - 1)F(q^m, n)^{-1}) < m^{-1}n^{-2}(mn^2 + m + 2) \leq 4.
\]

So, again, the result holds.

Now assume that \( d(A) \geq 3 \). Plugging \( l = d(A) - 1 \) into (18), rearranging and using Lemma 8 and Theorem 1.3 gives us

\[
q^{(d(A)-2)mn^2} < \frac{\alpha m F(q^m, n)}{P(S, d(A) - 1)(q^m - 1)} < \frac{8\alpha m}{3(q^m - 1)}.
\]

Consequently,

\[
d(A) \leq \left\lceil m^{-1}n^{-2}\log_q \frac{8\alpha m}{3(q^m - 1)} \right\rceil + 1 < m^{-1}n^{-2}\log_q \alpha m + 3.42.
\]

For the lower bound, combining (18) with Lemma 8 gives us

\[
d(A) > m^{-1}n^{-2}\log_q \frac{\phi(1/2)\alpha m}{q^m - 1} + 1 > m^{-1}n^{-2}\log_q \alpha m - 2.33.
\]

Next consider the case where \( A \) is semisimple. That is, \( A = \prod_{i=1}^r S_i^{\alpha_i} \) where the \( S_i \)'s are simple and pairwise non-isomorphic. It follows from [9, Proposition 2.12] that \( d(A) = \max_{i=1,...,r} \{d(S_i^{\alpha_i})\} \). The result follows immediately.

Finally, we consider the general case. That is, \( A = S \oplus J(A) \) where \( S \) is semisimple. The lower bound is immediate from Lemma 19 and the semisimple case. For the upper bound, let

\[
0 = H_0 \leq H_1 \leq ... \leq H_\mu = J(A)
\]

be an unrefinable chain of minimal length of \( S \)-submodules of \( J(A) \). For each \( i = 1, ..., \mu \), let \( x_i \in H_i \setminus H_{i-1} \). Let \( X \) be a generating set for \( S \) of minimal cardinality. Using Theorem 2, we see that \( X \cup \{x_1, ..., x_\mu\} \) is a set of generators for \( A \). That is, \( d(A) \leq d(S) + \mu \). This completes the proof of the theorem.

10 | POSITIVELY FINITELY GENERATED ALGEBRAS

In this section, we investigate PFG profinite algebras.
Let $A$ be a profinite algebra. Recall the following definitions. For $d \geq 1$, $P(A, d)$ is the probability that $d$ randomly chosen elements of $A$ generate $A$. Let $m_n(A)$ be the number of index $n$ (open) maximal subalgebras of $A$.

In order to prove Theorems 1.11 and 1.12, we need some preparations.

**Lemma 22.** With the above notation, we have $1 - P(A, d) \leq \sum_{n \geq 2} m_n(A) n^{-d}$.

**Proof.** If randomly chosen $a_1, \ldots, a_d \in A$ do not generate $A$ (topologically), then they all lie in some (open) maximal subalgebra $B$ of $A$. Therefore, $1 - P(A, d) \leq \sum_{B \in \text{Max} A \mid A : B} \leq \sum_{n \geq 2} m_n(A) n^{-d}$ yielding the result.

Given the algebra $A$ and a subalgebra $B < A$, define the core $B_A$ of $B$ in $A$ to be the maximal two-sided ideal $C$ of $A$ such that $C \subseteq B$. It exists (as the sum of all ideals of $A$ which are contained in $B$) and is unique.

**Lemma 23.** Let $A$ be a profinite algebra. Then, for all $n \geq 2$, $A$ has at most $6.93n$ maximal subalgebras of index $n$ with trivial core.

**Proof.** By our assumptions, $A = S \oplus J(A)$ where $S = \prod_{i \in I} S_i$ is a semisimple subalgebra of $A$ such that each $S_i$ is simple. Let $B$ be a maximal subalgebra of $A$ of finite index $n \geq 2$, and let $C = B_A$.

It is straightforward to generalise Theorem 2 to profinite algebras, so $B$ is of type (T1), (T2) or (T3). If $B$ is of type (T1), then $C = (\prod_{i \neq j} S_i) \oplus J(A)$ for some $j \in I$. If $B$ is of type (T2), then $C = (\prod_{i \neq j_1, j_2} S_i) \oplus J(A)$ where $j_1, j_2 \in I$ are distinct and $S_{j_1} \cong S_{j_2}$. If $B$ is of type (T3), then $C = (\prod_{i \neq j_1, j_2} S_i) \oplus J(B)$ for some (not necessarily distinct) $j_1, j_2 \in I$.

Henceforth assume that $B$ has trivial core, namely $C = 0$.

Suppose that $B$ is of type (T1). Then $|I| = 1$ and $J(A)$ is trivial. That is, $A$ is finite and simple. It follows from Theorem 1 that $A$ has at most two conjugacy classes of maximal subalgebras of index $n$. Lemma 9 shows that, given $B$ as above, $A$ has at most $\frac{|A^x|}{|B^x|} < \phi(1/2)^{-1} \frac{|A|}{|B|} = \phi(1/2)^{-1} n$ subalgebras which are conjugate to $B$. Note that $2\phi(1/2)^{-1} \approx 6.925$.

Now let $B$ be of type (T2). Then $|I| = 2$ and $J(A)$ is trivial. That is, $A = S_1 \times S_2$ where $S_1, S_2$ are isomorphic finite simple algebras, and $B$ is a diagonal subalgebra of $A$, so $n = |S_1| = |S_2|$. The number of choices for $B$ is therefore bounded above by the number of isomorphisms from $S_1$ to $S_2$, which, in turn, is bounded above by $n$.

Finally, suppose that $B$ is of type (T3). Then $|I| = 1$ or $2$ and $J(A)$ is a simple $S$-bimodule with $|J(A)| = n$. By the Wedderburn–Malcev principal theorem, $B = S^{1+z}$ for some $z \in J(A)$. So, there are precisely $n$ choices for $B$.

Altogether we see that the number of maximal subalgebras of $A$ of index $n$ with trivial core is at most $6.93n$.

To illustrate Lemma 23, consider the case where $A = M_2(q)$. It is easy to check that $m_n(A) \leq n + 1$ for all $n > 1$.

Analogous to the Haar measure for locally compact groups, every profinite algebra admits a unique left (additive) translation invariant probability measure.

**Lemma 24.** Let $B_1, B_2$ be maximal subalgebras of $A$ with cores $C_1, C_2$, respectively. Suppose $C_1 \neq C_2$ and let $d$ be a positive integer. Then the events $B_1^d, B_2^d$ in $A^d$ are independent.
Proof. Replacing $A$ with $A/(C_1 \cap C_2)$, we may assume that $\dim A < \infty$. Clearly $B_1^d, B_2^d$ are independent if and only if $B_1, B_2$ are, namely if and only if $[A : B_1 \cap B_2] = [A : B_1][A : B_2]$ if and only if $\dim A = \dim B_1 + \dim B_2 - \dim(B_1 \cap B_2)$ if and only if $\dim A = \dim(B_1 + B_2)$ if and only if $B_1 + B_2 = A$.

Suppose $C_1 \neq C_2$. Without loss of generality, $C_2 \not\subset C_1$. Then $C_2$ is an ideal of $A$ which is not contained in the maximal subalgebra $B_1$. Hence, $B_1 + C_2$ is a subalgebra of $A$ which properly contains $B_1$. It follows that $B_1 + C_2 = A$, which implies $B_1 + B_2 = A$. We conclude that $B_1, B_2$ are independent.

Recall that $A$ is PFG if $P(A, d) > 0$ for some $d$. Also recall that $A$ has PMSG if the number $m_n(A)$ of index $n$ maximal subalgebras of $A$ is bounded by $n^c$ for some fixed constant $c$.

Proof of Theorem 1.11.

Proof. PMSG easily implies PFG. Indeed, if $m_n(A) \leq n^b$ for some positive integer $b$ and all $n \geq 2$, then

$$1 - P(A, b + 2) \leq \sum_{n \geq 2} m_n(A)n^{-(b+2)} \leq \sum_{n \geq 2} n^{-2} = \pi^2/6 - 1 < 1,$$

so $P(A, b + 2) > 0$.

Now, suppose that $A$ is PFG, and let $d \in N$ such that $P(A, d) > 0$. We shall show that $A$ has PMSG.

Let $C_i$ be a list of the distinct cores of maximal subalgebras of $A$. For each $i$, choose a maximal subalgebra $B_i$ of $A$ with core $C_i$. For each $n \geq 2$, let $c_n(A)$ denote the number of maximal subalgebras of index $n$ obtained in this way.

Consider $X = A^d$ as a probability space and the events $X_i = B_i^d < X$. By Lemma 24, the events $X_i$ are pairwise independent. Let $p_i = [A : B_i]^{-d}$, the probability of the event $X_i$.

By the Borel–Cantelli lemma, if $\sum_i p_i = \infty$, then, with probability 1, infinitely many events $X_i$ occur. This implies that a random $d$-tuple in $A^d$ generates $A$ with probability 0, a contradiction to $P(A, d) > 0$. We conclude that $\sum_i p_i$ converges. Moreover, by the effective version of the Borel–Cantelli lemma, we have

$$\sum_i p_i \leq P(A, d)^{-1}.$$

We deduce that

$$\sum_{n \geq 2} c_n(A)n^{-d} = \sum_i [A : B_i]^{-d} \leq P(A, d)^{-1},$$

so $c_n(A)n^{-d} \leq P(A, d)^{-1}$, which yields

$$c_n(A) \leq P(A, d)^{-1}n^d$$

for all $n \geq 2$.

Now, by Lemma 23, there are at most $6.93n$ maximal subgroups of $A$ of index $n$ with a given core $C_i$. This yields

$$m_n(A) \leq 6.93nc_n(A) \leq 6.93P(A, d)^{-1}n^{d+1}. \quad (19)$$

In particular, $A$ has PMSG as required.
Finally, assume that $A$ is infinite and recall that $d_0(A) := \min\{d \geq 1 \mid P(A, d) > 0\}$. It then follows from Equation (19) that

$$M^*(A) = \limsup_{n>1} \frac{m_n(A)}{\log n} \leq d_0(A) + 1,$$

establishing the second statement of Theorem 1.11.

We now move on to the proof of Theorem 1.12.

**Proposition 25.** Let $A$ be a finite algebra, say $A = S \oplus J(A)$ where $S = \prod_{i=1}^{r} S_i$ and $S_i = M_n(q^{m_i})$ for each $i$. Then, for all $n > 1$, we have

$$m_n(A) \leq n \left(6.93 r + r(r - 1)/2 + r^2 n^{d(A)}\right).$$

**Proof.** Let $B < A$ be a maximal subalgebra of index $n$ and let $C = B_A$ be its core.

If $B$ is of type (T1), then $C = (\prod_{i \neq j_1, j_2} S_i) \oplus J(A)$ for some $1 \leq j_1 < j_2 \leq r$, so there are $r^2$ possibilities for $C$. As follows from the proof of Lemma 23, there are at most $6.93n$ possibilities for $B/C$, hence for $B$ given $C$. We conclude that there are at most $6.93rn$ possibilities for $B$ of type (T1).

Suppose that $B$ is of type (T2). Then $C = (\prod_{i \neq j_1, j_2} S_i) \oplus H$ for some (not necessarily distinct) integers $1 \leq j_1 \leq j_2 \leq r$ and some two-sided ideal $H$ of $A$ that is maximal with respect to being contained in $J(A)$. We first want to count the possibilities for $H$.

Observe that $B^X$ is a maximal subgroup of $A^X$. Then $A^X$ acts primitively by left multiplication on the set of left cosets $A^X/B^X$ (see, e.g. 1.7(b) of [2]). In other words, $A^X/B^X$ is a primitive (left) $A^X$-space. Applying 1.3 of [2] then tells us that the conjugacy class of $B^X$ in $A^X$, and hence $H$, is uniquely determined by the isomorphism class of $A^X/B^X$ as an $A^X$-space.

Consider the (non-unital) quotient algebra $V := J(A)/H$. We equip $V$ with the structure of an $A$-bimodule under the action $v \mapsto ava'$ for $a, a' \in A$ and $v \in V$. Note that $V$ is a simple $A$-bimodule since $B$ is a maximal subalgebra of $A$, and hence, $J(A)$ acts trivially on $V$ (on both the left and the right) by Nakayama’s lemma. So, $V^2 = 0$.

Next consider the quotient algebra $A/C =: \overline{A}$ and the natural projection $\rho : A \rightarrow \overline{A}$. Let $\overline{S}$ be a maximal semisimple subalgebra of $A$. Since our field $k$ is perfect, $\overline{A}/J(\overline{A}) \cong \overline{S}$ is separable. Observe that $V$ is isomorphic to $J(\overline{A})$ as a (non-unital) algebra. Then applying [19, Proposition 11.7] (a version of Wedderburn’s principal theorem) gives us a semidirect product of algebras $\overline{A} = V \rtimes \overline{S}$ (i.e. $(u, s)(v', s') = (uv's' + s'uv, ss')$ for all $u, v, s, s' \in \overline{S}$, and $(0,1)$ is the unity element). The core of $\overline{A}$ is trivial, and so, $\overline{S}$ is isomorphic to either $S_{j_1}$ (if $j_1 = j_2$) or to $S_{j_1} \times S_{j_2}$ (if $j_1 \neq j_2$). One can interpret $V$ as the natural left $S_{j_1} \otimes (S_{j_2})^{op}$-module (refer to §10.1 of [19]). It follows that there are at most $n^2$ possibilities for the isomorphism class of $\overline{A}$.

Taking the respective groups of units of $\overline{A} = V \rtimes \overline{S}$ gives us a semidirect product of groups $\overline{A}^X = V \rtimes \overline{S}^X$ (considering $V$ to be its additive group). The natural projection $\rho : A \rightarrow \overline{A}$ induces a (left) action of $A^X$ by permutations on $V$ as follows. Let $v \in V$ and $a \in A^X$, say $\rho(a) = (u', s)$ for $v' \in V$ and $s \in \overline{S}$, and define $a \cdot v := vsu^{-1} + v's^{-1}$. It is then easy to see that the map $V \rightarrow A^X/B^X$ given by $x + H \mapsto (x + 1)B^X$ for $x \in J(A)$ is an isomorphism of $A^X$-spaces.
The isomorphism class of $V$ as an $A^\times$-space is uniquely determined by the isomorphism class of $\overline{A}^\times$ along with a 1-cocycle $A^\times \to V$, which arises from a derivation $\delta : A \to V$. Certainly $\overline{A}^\times$ is determined up to isomorphism by $A$ and $\delta : A \to V$ is determined by its values on the generators of $A$. By assumption, $|V| = n$. In summary, the number of possibilities for $H$ is bounded above by $r^2 n^{d(A)}$.

For a given $H$, by Malcev’s contribution to the principal theorem and since $B \cap J(A) = J(B) = H$, there are at most $|J(A)/H| = n$ possibilities for $B$. So, there are at most $r^2 n^{d(A)+1}$ possibilities for $B$ of type $(T3)$. This completes the proof.

Let $x = (x_d)_{d \in \mathbb{N}}$ be a sequence of elements of $A$ that are chosen randomly, uniformly and independently. Define a random variable $\tau_A$ by

$$\tau_A = \min\{d \geq 1 \mid \langle x_1, ..., x_d \rangle = A\} \in \mathbb{N} \cup \{+\infty\}.$$ 

Recall that $E(A)$ is the expected number of random elements of $A$ chosen uniformly and independently which generate $A$. Observe that

$$E(A) = \sum_{d \geq 1} d P(\tau_A = d) = \sum_{d \geq 1} \left( \sum_{c \geq d} P(\tau_A = c) \right) = \sum_{d \geq 0} (1 - P(A, d)). \tag{20}$$

Recall the definitions

$$M(A) = \sup_{n > 1} \log m_n(A)/\log n$$

and, for any real number $\eta \geq 1$,

$$V_\eta(A) = \min\{d \geq 1 : P(A, d) \geq \eta^{-1}\}.$$ 

Let $\zeta$ denote the Riemann zeta function.

**Proof of Theorem 1.12.**

Proof. We first prove $(i)$. Observe that $m_n(A) = 0$ for $n < q$ (or indeed if $n < m(A)$). We claim that

$$m_n(A) \leq 2r^2 n^{d(A)+1}. \tag{21}$$

Assuming that (21) holds, we obtain

$$M(A) = \max_{n > 1} \log m_n(A)/\log n$$

$$\leq \max_{n \geq q} \log(2r^2 n^{d(A)+1})/\log n$$

$$\leq 2 \log_q r + d(A) + 2.$$ 

It remains to show that the inequality (21) holds.

Recall from Proposition 25 that

$$m_n(A) \leq n \left( 6.93 r + r(r - 1)/2 + r^2 n^{d(A)} \right).$$
It follows immediately that (21) holds, unless (possibly) if \( d(A) \leq 1 \), or if \( d(A) = 2, n = q = 2 \) and \( r = 1 \).

If \( d(A) = 0 \), then \( A \cong k \) and \( m_n(A) = 0 \), and, of course, (21) holds.

Next assume that \( d(A) = 1 \). Let \( i \in \{1, \ldots, r\} \). Since \( d(A) = 1 \), Lemma 20(ii) tells us that \( S_i \) is a field. It then follows from Theorem 1 that any maximal subalgebra of \( S_i \) is of type (S3), and hence, for any given \( n \), there is at most one index \( n \) maximal subalgebra of \( S_i \). That is, \( m_n(S_i) \leq 1 \). We can use this to refine the proof of Proposition 25, and obtain the sharpened inequality

\[
m_n(A) \leq r + n(r - 1)/2 + r^2n.
\]

It follows that (21) holds.

Finally, assume that \( d(A) = 2, n = q = 2 \) and \( r = 1 \). Since \( n = q \), the invariant \( m_n(A) \) is counting the codimension 1 subalgebras of \( A \). Note that \( S \) is simple since \( r = 1 \), and so, \( A \) has no maximal subalgebras of type (T2).

Assume for the moment that \( S \cong k \). Then, \( A \) has no maximal subalgebras of type (T1). By the proof of Proposition 25, \( A \) has at most eight maximal subalgebras of type (T3). Hence, \( m_n(A) \leq 8 \) by Theorem 2, so certainly (21) holds.

Now assume that \( S \not\cong k \). Then any maximal subalgebra of type (T3) of \( A \) has codimension strictly greater than 1. Codimension 1 subalgebras of type (T1) of \( A \) are in bijection with codimension 1 subalgebras of \( S \), of which there are none unless \( S \cong M_2(q) \) (in which case there are 3 of them) or \( S \cong F_q^2 \) (in which case there is 1 of them). So, \( m_n(A) \leq 3 \) by Theorem 2, and again, (21) holds.

This completes the proof of part (i).

(ii) Let \( d = \lceil M(A) + 2.02 \rceil \). It is immediate from the definition that \( m_n(A) \leq n^{M(A)} \) for all \( n \geq 2 \). Then, we have

\[
1 - P(A, d) \leq \sum_{n \geq 2} m_n(A)n^{-d} \leq \sum_{n \geq 2} n^{-2.02} = \zeta(2.02) - 1 < 1 - e^{-1}.
\]

Hence, \( P(A, d) > e^{-1} \), so \( V(A) \leq d \), as required. This gives us the upper bound.

Now let \( d = V(A) \). Then \( P(A, d) \geq e^{-1} \), and it follows from Equation (19) that

\[
m_n(A) \leq 6.93e \cdot n^{V(A)+1}.
\]

This implies that

\[
M(A) = \sup_{n>1} \log m_n(A)/\log n \leq \log(6.93e) + V(A) + 1 < V(A) + 5.24.
\]

Since \( V(A) \) is an integer, we have \( V(A) \geq \lceil M(A) - 5.24 \rceil \).

(iii) Let \( \eta \geq 1 \) be a real number and set \( d = V(A) \). By the same argument as in the proof of (ii), we see that

\[
m_n(A) \leq 6.93\eta \cdot n^{V(A)+1}.
\]

This implies

\[
M(A) = \sup_{n>1} \log m_n(A)/\log n < V(A) + \log \eta + 3.80.
\]
Now consider the case where $\eta = 2^i$ for some positive integer $i$. Then

$$M(A) < V_2(A) + i + 3.80$$

by Equation (22). Denote $\alpha := \lceil M(A) - 4.80 \rceil$. In particular, if $d = \alpha - i$, then $P(A,d) < 2^{-i}$.

Combining this with Equation (20) gives us

$$E(A) \geq \sum_{d=0}^{\alpha-1} (1 - P(A,d)) > \sum_{d=0}^{\alpha-1} (1 - 2^{d-\alpha}) \geq \alpha - 1.$$

This establishes the lower bound of $E(A)$. It remains to prove the upper bound.

Denote $l := \lceil M(A) \rceil$. Since $m_n(A) \leq n^i$, we have

$$1 - P(A,d) \leq \sum_{n \geq 2} m_n(A)n^{-d} \leq \sum_{n \geq 2} n^{l-d}.$$

Denote $\beta := d - l$. Combining this with (20) gives us

$$E(A) \leq l + 2 + \sum_{d \geq l+2} (1 - P(A,d))$$

$$\leq l + 2 + \sum_{\beta \geq 2} \left( \sum_{n \geq 2} n^{-\beta} \right)$$

$$\leq l + 2 + \sum_{n \geq 2} (\zeta(n) - 1)$$

$$= l + 3.$$

This completes the proof of $(iii)$.

**ACKNOWLEDGEMENTS**

DS was supported by a Post-Doctoral Fellowship from ISF grant 686/17 of AS. AS was partially supported by ISF grant 686/17 and the Vinik Chair of mathematics which he holds.

Open access funding enabled and organized by Projekt DEAL.

**JOURNAL INFORMATION**

The *Journal of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

**REFERENCES**

1. A. Borovik, L. Pyber, and A. Shalev, *Maximal subgroups in finite and profinite groups*, Trans. Amer. Math. Soc. 348 (1996), 3745–3761.

2. P.J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.
3. E. Detomi, A. Lucchini, and F. Morini, *How many elements are needed to generate a finite group with good probability?*, Israel J. Math. **132** (2002), 29–44.

4. A. G. Elashvili and V. G. Kac, *Classification of good gradings of simple lie algebras*, Amer. Math. Soc. Transl. **213** (2005), 85–104.

5. N. J. Fine and I. N. Herstein, *The probability that a matrix be nilpotent*, Illinois J. Math. **2** (1958), 499–504.

6. G. Gasper and M. Rahman, *Basic hypergeometric series*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 96, Cambridge University Press, Cambridge, 2004.

7. M. C. Iovanov and A. H. Sistko, *Maximal subalgebras of finite-dimensional algebras*, Forum Math. **31** (2019), 1283–1304.

8. A. Jaikin-Zapirain and L. Pyber, *Random generation of finite and profinite groups and group enumeration*, Ann. Math. **173** (2011), 769–814.

9. R. Kravchenko, M. Mazur, and B. V. Petrenko, *On the smallest number of generators and the probability of generating an algebra*, Algebra Number Theory **6** (2012), 243–291.

10. G. Landsberg, *Ueber eine anzahlbestimmung und eine damit zusammenhängende reihe*, J. Reine Angew. Math. **111** (1893), 87–88.

11. M. W. Liebeck, *Probabilistic and asymptotic aspects of finite simple groups*, Probabilistic group theory, combinatorics and computing (eds. A. Detinko et al.), Springer Lecture Notes in Math., vol. 2070, Springer, London, 2013, pp. 1–34.

12. M. W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of kantor and lubotzky*, J. Algebra **184** (1996), 31–57.

13. A. Lubotzky, *The expected number of random elements to generate a finite group*, J. Algebra **257** (2002), 452–459.

14. A. Lucchini and M. Moscatiello, *Generation of finite groups and maximal subgroup growth*, Adv. Group Theory Appl. **9** (2020), 39–49.

15. A. Mann and A. Shalev, *Simple groups, maximal subgroups, and probabilistic aspects of profinite groups*, Israel J. Math. **96** (1996), 449–468.

16. N. E. Menezes, M. Quick, and M. C. Roney-Dougal, *The probability of generating a finite simple group*, Israel J. Math. **198** (2013), 371–392.

17. P. M. Neumann and C. E. Praeger, *Cyclic matrices over finite fields*, J. London Math. Soc. **52** (1995), 263–284.

18. I. Pak, On the probability of generating a finite group, 1999.

19. R. S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer, New York, 1982.

20. C. Pomerance, *The expected number of random elements to generate a finite abelian group*, Period. Math. Hungar. **43** (2001), 191–198.

21. I. Reiner, *On the number of matrices with given characteristic polynomial*, Illinois J. Math. **5** (1961), 324–329.

22. L. H. Rowen, *Ring theory*, Student Edition, Academic Press, San Diego, CA, 1991.

23. A. Shalev, *Probabilistic group theory*, Groups St Andrews 1997 in Bath, II, London Mathematical Society Lecture Note Series vol. 261, pp. 648–678, Cambridge University Press, Cambridge, 1999.