# ON THE NUMBER OF GENERATORS OF A SEPARABLE ALGEBRA OVER A FINITE FIELD

URIYA FIRST, ZINOVY REICHSTEIN, AND SANTIAGO SALAZAR

Abstract. Let $F$ be a field and let $E$ be an étale algebra over $F$, that is, a finite product of finite separable field extensions, $E = F_1 \times \cdots \times F_r$. The classical primitive element theorem asserts that if $r = 1$, then $E$ is generated by one element as an $F$-algebra. The same is true for any $r \geqslant 1$, provided that $F$ is infinite. However, if $F$ is a finite field and $r \geqslant 2$, the primitive element theorem fails in general. In this paper we give a formula for the minimal number of generators of $E$ when $F$ is finite. We also obtain upper and lower bounds on the number of generators of a (not necessarily commutative) separable algebra over a finite field.

Contents



## 1. Introduction

The primitive element theorem asserts that a separable field extension $E/F$ of finite degree can be generated by one element; see, e.g., [La02, Theorem V.4.6]. It is natural to ask if the same is true for every étale algebra $E/F$. Recall that an étale algebra $E$ over a field $F$ is a finite product $E = F_1 \times \cdots \times F_r$, where each $F_i$ is a finite separable field extension of $F$. If $F$ is an infinite field, then the primitive element theorem continues to

2010 *Mathematics Subject Classification.* 12E20, 13E15, 16H05, 16P10.

*Key words and phrases.* Finite fields, étale algebras, Möbius inversion, separable algebras, number of generators.

Uriya First was supported, in part, by a postdoctoral research fellowship from the University of British Columbia.

Zinovy Reichstein was partially supported by National Sciences and Engineering Research Council of Canada (NSERC) grant No. 250217-2012.

Santiago Salazar's work on this project was conducted in the framework of NSERC's Undergraduate Summer Research Awards (USRA) program at the University of British Columbia.

hold: $E$ is generated by one element as an $F$-algebra; see, e.g., [FR17, Proposition 4.1]. On the other hand, if

$$E := \mathbb{F}_{q^{n_1}} \times \cdots \times \mathbb{F}_{q^{n_r}}. \tag{1}$$

is an étale algebra over a finite field $F = \mathbb{F}_q$ of $q$ elements, the primitive element theorem may fail. In this paper we will find the minimal number of generators for $E$ as an $\mathbb{F}_q$-algebra. We will denote this number by $\mathrm{gen}(E)$.

We will call an étale $\mathbb{F}_q$-algebra $E$ in (1) pure if $n_1 = \cdots = n_r$. Any étale algebra $E$ can be written as a product $E_1 \times \cdots \times E_t$, where each $E_i$ is pure, $E_i \cong (\mathbb{F}_{q^{n_i}})^{r_i}$, and $n_1, \ldots, n_t$ are distinct. In Section 2 we will show that $\mathrm{gen}(E) = \max\{\mathrm{gen}(E_1), \ldots, \mathrm{gen}(E_t)\}$; see Proposition 2.3. This reduces the problem of computing $\mathrm{gen}(E)$ to the case where $E$ is pure. In this case, we will prove the following formula for $\mathrm{gen}(E)$ in Section 3.

**Theorem 1.1.** *Let $E = \mathbb{F}_{q^n} \times \cdots \times \mathbb{F}_{q^n}$ ($r$ times). Then $\mathrm{gen}(E)$ is the minimal non-negative integer $g$ such that $r \leqslant \dfrac{1}{n}\sum_{d\,|\,n} \mu(d) q^{\frac{gn}{d}}$.*

Here the sum is taken over all positive divisors $d$ of $n$, and $\mu : \mathbb{N} \to \{-1, 0, 1\}$ denotes the Möbius function. In Section 4 we will prove the following consequence of this formula.

**Theorem 1.2.** *Let $E = \mathbb{F}_{q^n} \times \cdots \times \mathbb{F}_{q^n}$ ($r$ times). Then*

$$\lceil \frac{1}{n} \log_q(nr) \rceil \leqslant \mathrm{gen}(E) \leqslant \lceil \frac{1}{n} \log_q(nr) \rceil + 1 \ .$$

Here, as usual, $\lceil x \rceil$ denotes the smallest integer $n$ such that $x \leqslant n$. When $n = 1$, $\mathrm{gen}(E) = \lceil \log_q r \rceil$; see Corollary 3.4. For $n > 1$ both values for $\mathrm{gen}(E)$ allowed by Theorem 1.2 actually occur; see Theorem 1.4 below.

More generally, we will be interested in the minimal number of generators $\mathrm{gen}(A)$ of a (not necessarily commutative) separable algebra $A$. All algebras in this paper will be assumed to be associative with 1. Recall that an algebra $A$ over a field $F$ is called separable if $A$ is finite-dimensional, semisimple and its center is an étale $F$-algebra. If $F$ is an infinite field, then $\mathrm{gen}(A) = 1$ if $A$ is commutative and $\mathrm{gen}(A) = 2$ otherwise; see [FR17, Remark 4.4]. Thus, our question is only of interest if $F = \mathbb{F}_q$ is a finite field. In this case, by theorems of Wedderburn (see, e.g., [R88a, Theorem 2.1.8] and [R88b, Theorem 7.1.11]), $A$ is isomorphic to a product of matrix algebras over finite fields, i.e.,

$$A = \mathrm{M}_{m_1 \times m_1}(\mathbb{F}_{q^{n_1}}) \times \cdots \times \mathrm{M}_{m_t \times m_t}(\mathbb{F}_{q^{n_t}}) \, .$$

Note that if $m_1 = \ldots m_t = 1$, then $A$ is an étale algebra.

Once again, Proposition 2.3 reduces the problem of computing $\mathrm{gen}(A)$ to the case where $A$ is pure, i.e. $(m_1, n_1) = \cdots = (m_t, n_t)$. Our main result for pure algebras is as follows.

**Theorem 1.3.** *Let $A = \mathrm{M}_{m\times m}(\mathbb{F}_{q^n}) \times \cdots \times \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ ($r$ times). Then*

$$\lceil \frac{1}{nm^2} \log_q(C \cdot r) \rceil \leqslant \mathrm{gen}(A) \leqslant \lceil \frac{1}{nm^2} \log_q(C \cdot r) \rceil + 1 \ ,$$

*where $C := n \cdot |\mathrm{PGL}_m(\mathbb{F}_{q^n})| = \dfrac{n \prod_{i=0}^{m-1}(q^{nm} - q^{ni})}{q^n - 1}$.*

When $m = 1$, the constant $C$ is $n$ and Theorem 1.3 reduces to Theorem 1.2. Note, however, that our proof of Theorem 1.3 relies on Theorem 1.2.

In the case where $A$ is non-commutative, we do not have an explicit formula for the value of $\mathrm{gen}(A)$, analogous to Theorem 1.1; see Remark 5.3. However, our final result, proved in Section 7, estimates how frequently each of the two values for $\mathrm{gen}(A)$ allowed by Theorem 1.3 is assumed.

**Theorem 1.4.** *Fix positive integers $n$ and $m$, and a prime power $q$. Set*

$$A_r = \mathrm{M}_{m\times m}(\mathbb{F}_{q^n}) \times \cdots \times \mathrm{M}_{m\times m}(\mathbb{F}_{q^n}) \text{ (r times)}$$

*and let $C$ be as in Theorem 1.3. Let $I_0(g)$ denote the set of integers $r$ such that $\mathrm{gen}(A_r) = g = \lceil \frac{1}{nm^2}\log_q(C\cdot r)\rceil$ and let $I_1(g)$ denote the set of integers $r$ such that $\mathrm{gen}(A_r) = g = \lceil \frac{1}{nm^2}\log_q(C\cdot r)\rceil + 1$. Then:*

(a) $I_0(g) \sqcup I_1(g+1) = \mathbb{N} \cap (C^{-1}q^{(g-1)nm^2}, C^{-1}q^{gnm^2}]$
(b) $|I_0(g)| = C^{-1}(q^{gnm^2} - q^{(g-1)nm^2})(1 - O(q^{-g}))$ *as a function of $g$.*
(c) $|I_1(g)| \geqslant \lfloor C^{-1}q^{(g-1)m^2}\rfloor$, *if $n \geqslant 2$.*
(d) $|I_1(g)| \geqslant \lfloor C^{-1}q^{(g-1)n(m^2-m+1)}\rfloor$, *if $m \geqslant 2$.*

Here, as usual, $\lfloor x\rfloor$ denotes the largest integer $n$ such that $n \leqslant x$.

If $(n,m) = (1,1)$, then $I_1(g) = \emptyset$ for every $g$; see Corollary 3.4. If $(n,m) \neq (1,1)$, then Theorem 1.4 tells us that for any sufficiently large integer $g$, $I_0(g)$ and $I_1(g)$ are both non-empty. In other words, for each sufficiently large $g$, there exist integers $r_1$ and $r_2$ such that

$$\mathrm{gen}(A_{r_1}) = g = \lceil \frac{1}{nm^2}\log_q(C\cdot r_1)\rceil \quad \text{and} \quad \mathrm{gen}(A_{r_2}) = g = \lceil \frac{1}{nm^2}\log_q(C\cdot r_2)\rceil + 1.$$

On the other hand, if we let $r$ range over the interval $[1, R]$, then the probability that $\mathrm{gen}(A_r) = \lceil \frac{1}{nm^2}\log_q(C\cdot r)\rceil$ rapidly approaches 1 as $R$ increases.

## 2. Reduction to the case of pure algebras

We begin with the following well-known version of the Chinese Remainder Theorem. For lack of a suitable reference we include a proof of the implication (a) $\Longrightarrow$ (b).

**Proposition 2.1** (Chinese Remainder Theorem)**.** *Let $R$ be a (not necessarily commutative) ring and let $I_1, \ldots, I_t \subset R$ be two-sided ideals. Then the following conditions are equivalent:*

(a) *The natural homomorphism $f\colon R \to R/I_1 \times \cdots \times R/I_t$ is surjective. Here the $j$-th component of $f(r)$ is $r \pmod{I_j}$.*
(b) *$I_1, \ldots, I_t$ are pairwise coprime, i.e., $I_i + I_j = R$ for any $i \neq j$.*

*Proof.* (a) $\Longrightarrow$ (b): By symmetry, it suffices to show that $I_1 + I_2 = R$. Since $f$ is surjective, there exists an $r \in R$ such that $f(r) = (1, 0, \ldots, 0)$. In particular, $r \in I_2$ by the definition of $f$. Similarly, $f(1-r) = (0, 1, \ldots, 1)$, so $1 - r$ lies in $I_1$. Since $1 = (1-r) + r \in I_1 + I_2$, we conclude that $I_1 + I_2 = R$, as desired.

(b) $\Longrightarrow$ (a): See, e.g., [R88a, Proposition 2.2.1]. $\square$

In the sequel, $P_g := \mathbb{F}_q[x_1, \dots, x_g]$ and $R_g := \mathbb{F}_q\langle X_1, \dots, X_g\rangle$ will denote, respectively, the commutative polynomial algebra and the free associative algebra on $g$ generators over $\mathbb{F}_q$.

**Lemma 2.2.** (a) *A separable algebra $A = \mathrm{M}_{m_1\times m_1}(\mathbb{F}_{q^{n_1}}) \times \cdots \times \mathrm{M}_{m_r\times m_r}(\mathbb{F}_{q^{n_r}})$ can be generated by $g$ elements over $\mathbb{F}_q$ if and only if the free associative algebra $R_g$ has $r$ distinct two-sided ideals $I_1, \dots, I_r$ such that $R_g/I_i$ is isomorphic to $\mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}})$ as $\mathbb{F}_q$-algebras for every $i = 1, \dots, r$.*

(b) *An étale algebra $E = \mathbb{F}_{q^{n_1}} \times \cdots \times \mathbb{F}_{q^{n_r}}$ can be generated by $g$ elements over $\mathbb{F}_q$ if and only if the polynomial algebra $P_g$ has $r$ distinct ideals $J_1, \dots, J_r$ such that $P_g/J_i \cong \mathbb{F}_{q^{n_i}}$ as $\mathbb{F}_q$-algebras for every $i = 1, \dots, r$.*

*Proof.* (a) Suppose $a_1, \dots, a_g \in A$ generate $A$ over $\mathbb{F}_q$. Then the $\mathbb{F}_q$-algebra homomorphism $R_g \to A$ sending $X_j$ to $a_j$ ($j = 1, \dots, g$) is surjective. Let $I_i$ denote the kernel of the composition $R_g \to A \to \mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}})$. Then $R_g/I_i \cong \mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}})$. Moreover, the ideals $I_1, \dots, I_t$ are pairwise coprime (and in particular, distinct) by Lemma 2.1.

Conversely, suppose $I_1, \dots, I_r$ are as above. Then $I_1, \dots, I_r$ are maximal and distinct, hence they are pairwise coprime. By Lemma 2.1, the homomorphism $R_g \to \prod_i R_g/I_i$ is surjective. Since $R_g/I_i \cong \mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}})$, we get an $\mathbb{F}_q$-algebra epimorphism $R_g \to \prod_i \mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}}) = A$. Hence, $E$ is generated by $g$ elements as an $\mathbb{F}_q$-algebra.

Part (b) is proved by the same argument as (a), with the free associative algebra $R_g$ replaced by the commutative polynomial algebra $P_g$. □

**Proposition 2.3.** *Suppose $A = A_1 \times \cdots \times A_t$, where each factor is a pure separable $\mathbb{F}_q$-algebra, $A_i = \mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}})^{r_i}$. Assume further that the pairs $(m_i, n_i)$ are distinct for $i = 1, \dots, t$. Then* $\mathrm{gen}(A) = \max\{\mathrm{gen}(A_1), \dots, \mathrm{gen}(A_t)\}$.

*Proof.* Let $g = \max\{\mathrm{gen}(A_i) \mid i = 1, \dots, t\}$. Clearly $\mathrm{gen}(A) \geqslant \mathrm{gen}(A_i)$ for each $i$, and thus $\mathrm{gen}(A) \geqslant g$.

To prove the opposite inequality, note that by Lemma 2.2 there exist $r_i$ distinct two-sided ideals $I_{i,1}, I_{i,2}, \dots, I_{i,r_i}$ such that

$$R_g/I_{i,j} \cong \mathrm{M}_{m_i\times m_i}(\mathbb{F}_{q^{n_i}}) \tag{2}$$

for each $j = 1, 2, \dots, r_i$. Letting $i$ vary from 1 to $t$, we obtain $r_1 + \cdots + r_t$ ideals, $I_{i,j}$. We claim that these ideals are distinct. If we can prove this claim, then Lemma 2.2 will tell us that $A$ is generated by $g$ elements, and the proof of Proposition 2.3 will be complete.

To prove the claim, suppose $I_{i,j} = I_{i',j'}$ for some $i, j, i', j'$. Then $i = i'$ by (2), and $j = j'$ because the ideals $I_{i,1}, I_{i,2}, \dots, I_{i,r_i}$ were chosen to be distinct. This proves the claim. □

## 3. Proof of Theorem 1.1

**Definition 3.1.** In the sequel, $N_{q,n}(g)$ will denote the number of maximal ideals $I$ in the polynomial ring $P_g := \mathbb{F}_q[x_1, \dots, x_g]$ such that $P_g/I \cong \mathbb{F}_{q^n}$.

We will often fix $q$ and $n$, and treat $N_{q,n}(g)$ as a function $g$. The symbol $N_{q,n}(g)$ emphasizes this point of view.

Let $E = (\mathbb{F}_{q^n})^r$ be a pure étale algebra over $\mathbb{F}_q$. By Lemma 2.2(b), $\mathrm{gen}(E)$ is the minimal integer $g$ such that $r \leqslant N_{q,n}(g)$. Thus in order to prove Theorem 1.1, it suffices to establish the following formula for $N_{q,n}(g)$.

**Proposition 3.2.** $N_{q,n}(g) = \dfrac{1}{n}\sum_{d|n} \mu(d) q^{\frac{gn}{d}}$.

Here $\mu$ denotes the Möbius function. Recall that $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as follows: $\mu(m) = (-1)^j$, if $m$ is the product of $j \geqslant 0$ distinct primes, and $\mu(m) = 0$, if $m$ is divisible by $p^2$ for some prime $p$.

When $g = 1$, ideals $I$ of $P_1 = \mathbb{F}_q[x]$ such that $\mathbb{F}_q[x]/I \cong \mathbb{F}_{q^n}$ are in bijection with monic irreducible polynomials of degree $n$ in $\mathbb{F}_q[x]$. In this case, Proposition 3.2 reduces to the well-known formula for the number of such polynomilas. The proof of this well-known formula relies on Möbius inversion; see, e.g., [LN97, Section 3.2] or [La02, p. 254]. Our proof of Proposition 3.2 proceeds along similar lines.

**Lemma 3.3.** *Let $P_g = \mathbb{F}_q[x_1, \ldots, x_g]$. The following three sets are in (pairwise) bijective correspondence. In particular, each of these sets has cardinality $N_{q,n}(g)$.*

(a) *The set of ideals $I \subset P_g$ such that $P_g/I \cong \mathbb{F}_{q^n}$,*
(b) *The set of orbits of $\mathbb{F}_q$-algebra epimorphisms $\phi : P_g \to \mathbb{F}_{q^n}$ under the action of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ given by $\sigma\colon \phi \mapsto \sigma \circ \phi$, for any $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.*
(c) *The set of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbits of order $n$ in $(\mathbb{F}_{q^n})^g$ or equivalently, the set of $g$-tuples $(a_1, \ldots, a_g) \in (\mathbb{F}_{q^n})^g$ such that $\mathbb{F}_q[a_1, \ldots, a_g] = \mathbb{F}_{q^n}$.*

*Proof.* The bijective correspondence between the sets (a) and (b) is given by sending the $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbit of $\phi : P_g \to \mathbb{F}_{q^n}$ to $\ker(\phi)$. In the other direction, send an ideal $I \subset P_g$ in (a) to the $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbit of the composition $\phi\colon P_g \to P_g/I \xrightarrow{\psi} \mathbb{F}_{q^n}$, where $\psi$ is an $\mathbb{F}_q$-algebra isomorphism $P_g/I \to \mathbb{F}_{q^n}$. (Here $\phi$ depends on the choice of the isomorphism $\psi$, but the $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbit of $\phi$ does not). One easily checks that these maps are mutually inverse.

A bijective correspondence between (b) and (c) is given by $\phi \mapsto (\phi(x_1), \ldots, \phi(x_g))$. Note that by the Galois correspondence $(a_1, \ldots, a_g) \in (\mathbb{F}_{q^n})^g$ has an orbit of order $n$ if and only if $\mathbb{F}_q[a_1, \ldots, a_g] = \mathbb{F}_{q^n}$. □

*Proof of Proposition 3.2.* Consider the natural (diagonal) action of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ on $(\mathbb{F}_{q^n})^g$. Let $d$ be a divisor of $n$. The group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of order $n$; its unique subgroup of index $d$ is $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})$. The elements of $(\mathbb{F}_{q^n})^g$ invariant under the action of this subgroup are precisely the elements of $(\mathbb{F}_{q^d})^g$. Thus by Lemma 3.3, there are $N_{g,d}(q)$ $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbits of size $d$ in $(\mathbb{F}_{q^n})^g$. Since the $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbits partition $(\mathbb{F}_{q^n})^g$, we have

$$q^{gn} = \sum_{d|n} dN_{q,d}(g).$$

The Möbius inversion formula (see, e.g., [LN97, Theorem 3.24]), now yields

$$nN_{q,n}(g) = \sum_{d|n} \mu(d) q^{\frac{gn}{d}},$$

as claimed. □

**Corollary 3.4.** *Let $E = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$ ($r$ times). Then* $\mathrm{gen}(E) = \lceil \log_q r \rceil$.

*Proof.* For $n = 1$, the sum in Theorem 1.1 reduces to just one term, $q^g$. That is, $\mathrm{gen}(E)$ is the smallest integer $g$ such that $r \leqslant q^g$. Equivalently, $\mathrm{gen}(E) = \lceil \log_q r \rceil$. □

## 4. Proof of Theorem 1.2

We shall need the following estimates on $N_{q,n}(g)$.

**Lemma 4.1.** (a) $N_{q,n}(g) \leqslant \frac{1}{n} q^{gn}$ *for any* $n, g \geqslant 1$.

(b) $N_{q,n}(g) \geqslant \frac{1}{n} q^{gn}(1 - \frac{1}{q})$ *for any* $n, g \geqslant 1$.

*Proof.* (a) is an immediate consequence of Lemma 3.3, since the number of orbits of order $n$ in $(\mathbb{F}_{q^n})^g$ cannot exceed $\frac{1}{n}|(\mathbb{F}_{q^n})|^g$. To prove (b) let us consider three cases.

*Case 1.* $n = 1$. By Proposition 3.2, $N_{q,n}(g) = \frac{1}{n} q^g$, and part (b) follows.

*Case 2.* $n = p^e$ is a prime power, where $e \geqslant 1$. By Proposition 3.2,

$$N_{q,n}(g) = \frac{1}{n}(q^{gp^e} - q^{gp^{e-1}}) = \frac{1}{n} q^{gn}(1 - q^{g(p^{e-1} - p^e)}) \,. \tag{3}$$

Since $p^{e-1} - p^e \leqslant -1$, part (b) follows.

*Case 3.* The prime decomposition of $n$ is $n = p_1^{e_1} \dots p_m^{e_m}$, where $m \geqslant 2$. In particular, $n \geqslant 6$. Let $\tau(n) = (e_1 + 1) \dots (e_m + 1)$ be the number of positive divisors of $n$. As $d$ ranges over these divisors, the function $\mu(d)$ attains each of the values 1 and $-1$ exactly $2^{m-1}$ times, and in all other cases $\mu(d) = 0$. We conclude that $\mu(d) = -1$ for at most $\tau(n)/2$ divisors $d$. In other words, in the expression for $N_{q,n}(g)$ given by Proposition 3.2, at most $\tau(n)/2$ terms $q^{gn/d}$ come with a negative sign. Since the absolute value of each of these terms is at most $q^{gn/2}$ and since $\tau(n) \leqslant 2\sqrt{n}$, we see that

$$N_{q,n}(g) \geqslant \frac{1}{n}\left(q^{gn} - \sqrt{n}\, q^{\frac{gn}{2}}\right) = \frac{1}{n} q^{gn}\left(1 - \sqrt{n}\, q^{-\frac{gn}{2}}\right) \,. \tag{4}$$

It is therefore enough to show that $\sqrt{n}\, q^{-gn/2} \leqslant \frac{1}{q}$, or equivalently, that $\sqrt{n}\, q^{1-gn/2} \leqslant 1$. Since $n \geqslant 6$, we have $1 - \frac{gn}{2} < 0$. Thus, if the inequality $\sqrt{n}\, q^{1-gn/2} \leqslant 1$ holds with $g = 1$ and $q = 2$, then it will hold for all $g$ and $q$. Substituting $g = 1$ and $q = 2$, we obtain $\sqrt{n}\, 2^{1-n/2} \leqslant 1$ or equivalently, $2^n \geqslant 4n$. An easy induction argument shows that this inequality is satisfied for every $n \geqslant 4$. □

*Proof of Theorem 1.2.* Set $E = (\mathbb{F}_{q^n})^r$ and $g = \mathrm{gen}(E)$. We need to show that

$$\frac{1}{n}\log_q(nr) \leqslant g < \frac{1}{n}\log_q(nr) + 2 \,. \tag{5}$$

If $g = 0$, then necessarily $r = n = 1$ and the theorem holds. If $g = 1$, then Lemmas 2.2 and 4.1(a) imply $r \leqslant N_{q,n}(1) \leqslant \frac{1}{n} q^n$. This yields $\lceil \frac{1}{n}\log_q(nr) \rceil \leqslant 1$, and once again, the inequalities (5) hold.

Thus we may assume that $g \geqslant 2$. By Lemma 2.2, $g$ is the unique integer for which

$$N_{q,n}(g-1) < r \leqslant N_{q,n}(g) \,.$$

By Lemma 4.1(b), this implies $\frac{1}{n}q^{(g-1)n}(1-\frac{1}{q}) < r \leqslant \frac{1}{n}q^{gn}$ which, after rearranging, yields

$$\frac{1}{n}\log_q(rn) \leqslant g < \frac{1}{n}\log_q(rn) + 1 + \frac{1}{n}(1-\log_q(q-1)).$$

Since $q \geqslant 2$ and $n \geqslant 1$, the right hand side cannot exceed $\frac{1}{n}\log_q(nr) + 2$. □

The following corollary was stated in [FR17, Remark 4.3] without proof.

**Corollary 4.2.** *Let $E$ be an étale $\mathbb{F}_q$-algebra. If $d = \dim_{\mathbb{F}_q}(E)$, then* $\operatorname{gen}(E) \leqslant \lceil \log_q(d) \rceil$.

The bound in the corollary is tight, since $\operatorname{gen}(E) = \lceil \log_q(d) \rceil$ when $E = (\mathbb{F}_q)^d$ by Corollary 3.4.

*Proof.* By Proposition 2.3, we may assume without loss of generality that $E = (\mathbb{F}_{q^n})^r$ so that $d = \dim E = nr$. As we mentioned above, for $n = 1$, $\operatorname{gen}(E) = \lceil \log_q(d) \rceil$ by Corollary 3.4. We will thus assume that $n > 1$ from now on. By Theorem 1.2, $\operatorname{gen}(E) \leqslant \lceil \frac{1}{n}\log_q(rn) \rceil + 1 \leqslant \lceil \frac{1}{2}\log_q(d) \rceil + 1$. Thus $\operatorname{gen}(E) \leqslant \lceil \log_q(d) \rceil$ when $\log_q(d) > 1$.

It remains to consider the case, where $\log_q(d) \leqslant 1$, or equivalently, $nr \leqslant q$. We need to show that in this case $E$ can be generated by one element. By Lemma 2.2, it suffices to prove that $r \leqslant N_{q,n}(1)$. By Lemma 4.1(b), we have

$$N_{q,n}(1) \geqslant \frac{1}{n}q^n(1-\frac{1}{q}) \geqslant \frac{1}{n}q(q-1) \geqslant \frac{q}{n} \geqslant r\,,$$

since $n > 1$ and $q \geqslant nr$. This completes the proof of the corollary. □

## 5. The integers $N_{q,n,m}(g)$

Let $G(q,n,m)$ denote the group of $\mathbb{F}_q$-algebra automorphisms of $B := \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$. Let $\pi$ be the natural homomorphism $\pi\colon G(q,n,m) \to \operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ given by restricting an element of $G(q,n,m)$ to the center $\mathbb{F}_{q^n}$ of $B$. By the Skolem–Noether Theorem (see, e.g., [R88b, Theorem 7.1.10]), $\operatorname{Ker}(\pi)$ is the group of inner automorphisms of $B$. That is, $\operatorname{Ker}(\pi) \simeq \mathrm{PGL}_m(\mathbb{F}_{q^n}) := \mathrm{GL}_m(\mathbb{F}_{q^n})/\mathbb{F}_{q^n}^\times$. Using the resulting short exact sequence of finite groups

$$1 \to \mathrm{PGL}_m(\mathbb{F}_{q^n}) \to G(q,n,m) \to \operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to 1,$$

we see that

$$|G(q,n,m)| = n \cdot |\mathrm{PGL}_m(\mathbb{F}_{q^n})| = \frac{n\prod_{i=0}^{m-1}(q^{nm}-q^{ni})}{q^n-1}$$

is the number $C$ appearing in the statement of Theorem 1.3.

**Definition 5.1.** In the sequel, $N_{q,n,m}(g)$ will denote the number of two-sided ideals $I \subset R_g = \mathbb{F}_q\langle X_1,\dots,X_g\rangle$ for which $R_g/I \cong \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ as $\mathbb{F}_q$-algebras.

Let $A = \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})^r$. It is immediate from Lemma 2.2(a) that $\operatorname{gen}(A)$ is the smallest integer $g$ such that

$$r \leqslant N_{q,n,m}(g)\ .$$

The following lemma is a partial extension of Lemma 3.3 to the setting of separable algebras (not necessarily commutative).

**Lemma 5.2.** *Let $n, m$ be positive integers, $q$ be a prime power, $R_g = \mathbb{F}_q\langle X_1, \dots, X_g\rangle$ be the free associative algebra on $g$ generators over $\mathbb{F}_q$, and $S_g$ be the set of $g$-tuples $(a_1, \dots, a_g) \in \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})^g$ which generate $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ as an $\mathbb{F}_q$-algebra.*

*The following three sets are in (pairwise) bijective correspondence. In particular, each of these sets has $N_{q,n,m}(g)$ elements.*

(a) *ideals $I \subset R_g$ such that $R_g/I \cong \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$,*
(b) *orbits of $\mathbb{F}_q$-algebra epimorphisms $\phi : R_g \to \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ under the natural action of $G(q, n, m)$,*
(c) *$G(q, n, m)$-orbits in $S_g$.*

*Moreover, every $G(q, n, m)$-orbit in $S_g$ consists of $|G(q, n, m)|$ elements.*

*Proof.* The bijective correspondences between (a) and (b) and between (b) and (c) are constructed in exactly the same way as in the proof of Lemma 3.3, with the commutative polynomial ring $P_g$ replaced by the free associative algebra $R_g$. To prove the last assertion, note that if $a_1, \dots, a_g$ generate $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ as an $\mathbb{F}_q$-algebra, then the stabilizer of $(a_1, \dots, a_g)$ in $G(q, m, n)$ is necessarily trivial. □

**Remark 5.3.** In the commutative setting of Lemma 3.3 (i.e., for $m = 1$), the set $S_g$ consists precisely of the $g$-tuples $(a_1, \dots, a_g)$ whose $G(q, n, m)$-orbit has exactly $|G(q, n, m)|$ elements. For $m \geqslant 2$, this is not so in general. In other words, a $g$-tuple $(a_1, \dots, a_g) \in \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})^g$ with trivial stabilizer in $G(q, n, m)$ may not generate $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$. For example, when $m = 2$, $n = 1$, and $g = 3$,

$$(a_1, a_2, a_3) = \left( \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

has trivial stabilizer in $G(q, 1, 2) = \mathrm{PGL}_2(\mathbb{F}_q)$. On the other hand, since $a_1$, $a_2$ and $a_3$ are upper-triangular matrices, they do not generate $\mathrm{M}_{2\times 2}(\mathbb{F}_q)$. For this reason, Lemma 5.2 does not allow us to obtain a formula for $N_{q,n,m}(g)$ when $m \geqslant 2$, analogous to the formula in Proposition 3.2. However, it does lead to useful estimates on $N_{q,n,m}(g)$.

**Corollary 5.4.** (a) $N_{q,n,1}(g) = N_{q,n}(g)$.
(b) $N_{q,n,m}(g) = C^{-1}|S_g| \leqslant C^{-1}q^{gnm^2}$.
(c) *Suppose $B$ is a proper $\mathbb{F}_q$-subalgebra of $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$. Then $N_{q,n,m}(g) = C^{-1}|S_g| \leqslant C^{-1}(q^{gnm^2} - |B|^g)$.*

*Proof.* (a) The set of $N_{q,n}(g)$ elements described in Lemma 3.3(c) is the same as the set of $N_{q,n,1}(g)$ elements described in Lemma 5.2(c).

(b) Follows from $S_g \subset \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ and $|\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})| = q^{gnm^2}$.

(c) Clearly, if $a_1, \dots, a_g \in B^g$, then $(a_1, \dots, a_g) \notin S_g$. From this we see that $S_g \subset \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})^g \setminus B^g$, and thus $|S_g| \leqslant (q^{gnm^2} - |B|^g)$. □

## 6. Proof of Theorem 1.3

**Lemma 6.1.** *$N_{q,n,m}(g) \geqslant |G(q, n, m)|^{-1}q^{(g-1)nm^2}$ for every $g, m \geqslant 2$ and $n \geqslant 1$.*

*Proof.* By Corollary 5.4(b), we need to establish the inequality $|S_g| \geqslant 2q^{(g-1)nm^2}$. Since $S_2 \times \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})^{g-2} \subseteq S_g$, it suffices to show that

$$|S_2| \geqslant q^{nm^2}. \tag{6}$$

To prove (6), fix a nonzero generator $u$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and consider pairs of matrices

$$A = \alpha_1 E_{1,2} + \alpha_3 E_{2,3} + \cdots + \alpha_{m-1} E_{m-1,m} \qquad \text{and} \qquad B = \sum_{i,j=1,\dots,m} \beta_{ij} E_{i,j} \tag{7}$$

where $\alpha_i$ and $\beta_{ij}$ are arbitrary elements of $\mathbb{F}_{q^n}$, subject to

$$\alpha_1 \dots \alpha_{m-1} \beta_{m1} = u\,. \tag{8}$$

Here, as usual, $E_{i,j}$ denotes the $(i,j)$-elementary matrix, i.e., an $m \times m$-matrix with 1 in the $(i,j)$-position and zeroes elsewhere. Note that $\alpha_1, \dots, \alpha_{m-1}$ can be arbitrary non-zero elements of $\mathbb{F}_{q^n}$. Once they are chosen, $\beta_{m1}$ is uniquely determined by (8). Thus the number of pairs $(A, B)$ of the above form is $(q^n - 1)^{m-1}(q^n)^{m^2-1}$.

*Claim.* Any pair of matrices $(A, B)$ defined by (7) and (8) generates $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ as an $\mathbb{F}_q$-algebra.

The claim implies that the pair $(A + \gamma I_m, B)$ generates $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ for every $\gamma \in \mathbb{F}_q$. This gives us $(q^n - 1)^{m-1}(q^n)^{m^2-1} q = (q^n - 1)^{m-1} q^{n(m^2-1)+1}$ pairs of generators. Thus, once the claim is established, we can conclude that

$$|S_2| \geqslant (q^n - 1)^{m-1} q^{n(m^2-1)+1} \geq (q^n - 1) q^{n(m^2-1)+1} = (q - q^{1-n}) q^{nm^2} \geq q^{nm^2}\,.$$

This would complete the proof of (6) and thus of part (b).

We now turn to the proof of the claim. Denote by $\Lambda$ the $\mathbb{F}_q$-subalgebra of $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ generated by $A$ and $B$. Our goal is to show that $\Lambda = \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$. We will do this in several steps.

*Step 1.* For every $c \in \mathbb{F}_{q^n}$, $\Lambda$ contains a matrix of the form $cE_{1,1} + c_2 E_{1,2} + \cdots + c_m E_{1,m}$ for some $c_2, \dots, c_m \in \mathbb{F}_{q^n}$.

*Proof.* Since $A^{m-1} = \alpha_1 \dots \alpha_{m-1} E_{1,m}$, the matrix $A^{m-1}B$ has the form $uE_{1,1} + t_2 E_{1,2} + \cdots + t_m E_{1,m}$ for some $t_2, \dots, t_m \in \mathbb{F}_{q^n}$. In particular, $A^{m-1}B$ is an upper-triangular matrix with diagonal entries $u, 0, \dots, 0$. If $p(x)$ is a polynomial with coefficients in $\mathbb{F}_q$, then $p(A^{m-1}B) = p(u)E_{1,1} + w_2 E_{1,2} + \cdots + w_m E_{1,m} \in \Lambda$ for some $w_2, \dots, w_m \in \mathbb{F}_{q^n}$. The desired conclusion now follows from the fact that $u$ is a generator for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

*Step 2.* For every $c \in \mathbb{F}_{q^n}$ and every $j = 1, 2, \dots, m$, $\Lambda$ contains an element of the form $cE_{1,j} + s_{j+1} E_{1,j+1} + \cdots + s_m E_{1,m}$ for some $s_{j+1}, \dots, s_m \in \mathbb{F}_{q^n}$.

*Proof.* We argue by induction on $j$. The base case, where $j = 1$, is given by Step 1. For the induction step, assume that $j \geqslant 2$ and for every $c' \in \mathbb{F}_{q^n}$, there exist $s_j, \dots, s_m \in \mathbb{F}_{q^n}$ such that

$$L := c' E_{1,j-1} + s_j E_{1,j} + \cdots + s_m E_{1,m} \in \Lambda\,.$$

Now observe that $LA \in \Lambda$ is of the form $c'\alpha_{j-1} E_{1,j} + t_{j+1} E_{1,j+1} + \cdots + t_m E_{1,m}$ for some $t_{j+1}, \dots, t_m \in \mathbb{F}_{q^n}$. Since $\alpha_{j-1} \neq 0$ by (8), we see that the coefficient $c'\alpha_{j-1}$ of $E_{1,j}$ can assume an arbitrary value in $\mathbb{F}_{q^n}$.

*Step 3.* $\Lambda$ contains $\mathbb{F}_{q^n} E_{1,j}$ for every $j = 1, \dots, m$.

*Proof.* The elements given in Step 2 span $\mathbb{F}_{q^n} E_{1,1} \oplus \mathbb{F}_{q^n} E_{1,2} \oplus \cdots \oplus \mathbb{F}_{q^n} E_{1,m}$ as an $\mathbb{F}_q$-vector space.

*Step 4.* $\Lambda$ contains $\mathbb{F}_{q^n} E_{k,j}$ for every $k = 1, \dots, m-1$ and $j = 1, \dots, m$.

*Proof.* We argue by induction on $k$. The base case, $k=1$, is given by Step 3. If $1<k<m$, assume that $\mathbb{F}_{q^n}E_{k',j}\subset\Lambda$ for every $k'=1,\dots,k-1$ and every $j=1,\dots,m$. Subtracting a linear combination of $E_{1,2},\dots,E_{k-1,k}$ from $A$, we see that

$$A_k := \alpha_k E_{k,k+1}+\cdots+\alpha_{m-1}E_{m-1,m}\in\Lambda$$

and hence, so is $A_k^{m-k}=\alpha E_{k,m}$, where $\alpha=\alpha_k\cdots\alpha_{m-1}$. By Step 3, $tE_{1,j}\in\Lambda$ for every $t\in\mathbb{F}_{q^n}$ and every $j=1,\dots,m$. Consequently, so is $(\alpha E_{k,m})B(tE_{1,j})=(t\alpha\beta_{m1})E_{k,j}$. Since $\alpha\beta_{m1}\neq 0$, this shows that $\mathbb{F}_{q^n}E_{k,j}\subset\Lambda$, as required.

*Step 5.* $\Lambda$ contains $\mathbb{F}_{q^n}E_{m,j}$ for every $j=1,\dots,m$.

*Proof.* By Step 4, $\Lambda$ contains $E_{k,k}$ for $k=1,\dots,m-1$. Since it also contains the identity element $I_m=E_{1,1}+\cdots+E_{m,m}$, we see that $E_{m,m}=I_m-E_{1,1}-\cdots-E_{m-1,m-1}\in\Lambda$. To show that $\mathbb{F}_{q^n}E_{m,j}\subset\Lambda$ for every $j=1,\dots,m$, we will use the same method as in Step 4. By Step 3, $tE_{1,j}\in\Lambda$ for every $t\in\mathbb{F}_{q^n}$. Thus,

$$E_{m,m}B(tE_{1,j})=t\beta_{m1}E_{m,j}\in\Lambda\,.$$

Since $\beta_{m1}\neq 0$, this shows that $\mathbb{F}_{q^n}E_{m,j}\subset\Lambda$, as claimed.

Taken together, Steps 4 and 5 show that $\Lambda$ contains $\mathbb{F}_{q^n}E_{k,j}$ for every $k,j=1,\dots,m$. As a result, $\Lambda=\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$, which completes the proof of the claim, and thus of the lemma. □

*Proof of Theorem 1.3.* Let $A=\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})\times\cdots\times\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ ($r$ times) and $C=|G(q,n,m)|$, as in the statement of the theorem. When $m=1$, Theorem 1.3 reduces to Theorem 1.2. Thus, we may assume that $m>1$.

By Lemma 2.2, $\mathrm{gen}(A)$ is the unique integer $g$ satisfying

$$N_{q,n,m}(g-1)<r\leqslant N_{q,n,m}(g)\ . \tag{9}$$

Our goal is to show that

$$\frac{1}{nm^2}\log_q(C\cdot r)\leqslant g<\frac{1}{nm^2}\log_q(C\cdot r)+2\ . \tag{10}$$

Suppose $g\geqslant 3$. By Lemma 6.1 and Corollary 5.4(b), (9) implies

$$C^{-1}q^{(g-2)nm^2}<r\leqslant q^{gnm^2}C^{-1}\ .$$

Multiplying through by $C$ and taking $\log_q$, we obtain (10).

Since $A$ is non-commutative, $g\leqslant 1$ is impossible. Thus, it remains to consider the case $g=2$. In this case, Corollary 5.4(b) yields $r\leqslant N_{q,n,m}(g)\leqslant C^{-1}q^{gnm^2}$, and thus $\frac{1}{nm^2}\log_q(r\cdot C)\leqslant g$. On the other hand, the upper bound on $g$ from (10) also remains valid, since $g=2<\frac{1}{nm^2}\log_q(C\cdot r)+2$. □

## 7. Proof of Theorem 1.4

We begin with further estimates on $N_{q,n,m}(g)$. We will denote $|G(q,n,m)|$ by $C$ throughout, as in the statement of Theorem 1.3.

**Lemma 7.1.** *Let $V$ be a $d$-dimensional vector space over $\mathbb{F}_q$ and let $T_g\subset V^g$ be the set of $g$-tuples $(v_1,\dots,v_g)$ which span $V$. Then $|T_g|=q^{gd}(1-O(q^{-g}))$.*

*Proof.* The cardinality of $T_g$ is the equal to the number of matrices in $\mathrm{M}_{d\times g}(\mathbb{F}_q)$ of rank $d$. When $g \geqslant d$ this is the set of $d \times g$ matrices over $\mathbb{F}_q$ whose rows are linearly independent. The cardinality of this set is well-known to be $\prod_{i=0}^{d-1}(q^g - q^i) = q^{dg}\prod_{i=0}^{d-1}(1-q^{i-g}) \geqslant q^{dg}(1-\sum_{i=0}^{d-1} q^{i-g})$. Since $|T_g| \leqslant q^{dg}$, the lemma follows. □

**Lemma 7.2.** (a) $N_{q,n,m}(g) = C^{-1}q^{gnm^2}(1-O(q^{-g}))$.

(b) *If* $n \geqslant 2$, *then* $N_{q,n,m}(g) \leqslant C^{-1}(q^{gnm^2} - q^{gm^2})$.

(c) *If* $m \geqslant 2$, *then* $N_{q,n,m}(g) \leqslant C^{-1}(q^{gnm^2} - q^{gn(m^2-m+1)})$.

*Proof.* (a) As before, let $S_g$ be the set of $g$-tuples in $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})^g$ which generate $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ as an $\mathbb{F}_q$-algebra. By Corollary 5.4(b), $N_{q,n,m}(g) = C^{-1}|S_g|$. We now apply Lemma 7.1 with $V = \mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ and $d = nm^2$. Clearly every $g$-tuple that spans $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ as an $\mathbb{F}_q$-vector space also generates it as an $\mathbb{F}_q$-algebra. Thus, $|S_g| \geqslant |T_g| = q^{gnm^2}(1-O(q^{-g}))$, and so $N_{q,n,m}(g) \geqslant C^{-1}q^{gnm^2}(1-O(q^{-g}))$. On the other hand, $N_{q,n,m}(g) \leqslant C^{-1}q^{gnm^2}$ by Corollary 5.4(b).

(b) follows from Corollary 5.4(c) with $B = \mathrm{M}_{m\times m}(\mathbb{F}_q)$.

(c) Let $B$ be the subalgebra of $\mathrm{M}_{m\times m}(\mathbb{F}_{q^n})$ consisting of matrices with zeroes in positions $(2,1),\dots,(m,1)$, and apply Corollary 5.4(c). Note that $|B| = q^{n(m^2-m+1)}$. □

*Proof of Theorem 1.4.* We first claim that

$$I_0(g) = \mathbb{N} \cap (C^{-1}q^{(g-1)nm^2}, N_{q,n,m}(g)] \tag{11}$$

and

$$I_1(g) = \mathbb{N} \cap (N_{q,n,m}(g-1), C^{-1}q^{(g-1)nm^2}]. \tag{12}$$

Indeed, by Lemma 2.2, $\mathrm{gen}(A_r) = g$ if and only $N_{q,n,m}(g-1) < r \leqslant N_{q,n,m}(g)$. On the other hand, by Theorem 1.3, $\mathrm{gen}(A_r) = g$ if and only if $r \in I_0(g) \sqcup I_1(g)$. Thus,

$$I_0(g) \sqcup I_1(g) = (N_{q,n,m}(g-1), N_{q,n,m}(g)]\,,$$

and (12) follows from (11). To establish (11), note that $r > C^{-1}q^{(g-1)nm^2}$ is equivalent to $g < \dfrac{1}{nm^2}\log_q(C\cdot r) + 1$. This proves the claim.

We now turn to the proof of itself. Equations (11) and (12) tell us that $I_0(g) = \mathbb{N} \cap (C^{-1}q^{(g-1)nm^2}, N_{q,n,m}(g)]$ and $I_1(g+1) = \mathbb{N} \cap (N_{q,n,m}(g), C^{-1}q^{nm^2}]$. These intervals are, by definition, disjoint, and part (a) follows.

To prove part (b), we combine (11) with Lemma 7.2(a):

$$\begin{aligned}|I_0(g)| &= N_{q,n,m}(g) - C^{-1}q^{(g-1)nm^2} - 1 + O(1)\\ &= C^{-1}q^{gnm^2}(1-O(q^{-g})) - C^{-1}q^{(g-1)nm^2} - 1 + O(1)\\ &= C^{-1}(q^{gnm^2} - q^{(g-1)nm^2})(1-O(q^{-g}))\ .\end{aligned}$$

To prove (c), we combine (12) with Lemma 7.2(b):

$$|I_1(g)| \geqslant \lfloor C^{-1}q^{(g-1)nm^2} - N_{q,n,m}(g-1)\rfloor \geqslant \lfloor C^{-1}q^{gm^2}\rfloor\ .$$

Similarly, to prove (d), we combine (12) with Lemma 7.2(c):

$$|I_1(g)| \geqslant \lfloor C^{-1}q^{(g-1)nm^2} - N_{q,n,m}(g-1)\rfloor \geqslant \lfloor C^{-1}q^{gn(m^2-m+1)}\rfloor\ .$$ □

## References

[FR17] U. A. First and Z. Reichstein, On the number of generators of an algebra, C. R. Math. Acad. Sci. Paris **355** (2017), no. 1, 5–9. MR3590278

[La02] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002. MR1878556

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, second edition, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997. MR1429394

[R88a] L. H. Rowen, Ring Theory, Vol. I, Pure and Applied Mathematics, 127, Academic Press, Inc., Boston MA, 1988. MR0940245.

[R88b] L. H. Rowen, Ring Theory, Vol. II, Pure and Applied Mathematics, 128, Academic Press, Inc., Boston MA, 1988. MR0945718.

*E-mail address*: `uriya.first@gmail.com`

Department of Mathematics, University of Haifa, Mount Carmel, Haifa, Israel 31905

*E-mail address*: `reichst@math.ubc.ca`

*E-mail address*: `santiago.salazar@zoho.com`

Department of Mathematics, University of British Columbia, BC, Canada V6T 1Z2