Random Krylov spaces over finite fields *

Richard P. Brent[†], Shuhong Gao[‡] and Alan G.B. Lauder[§]

August 10, 2001

Abstract

Motivated by a connection with block iterative methods for solving linear systems over finite fields, we consider the probability that the Krylov space generated by a fixed linear mapping and a random set of elements in a vector space over a finite field equals the space itself. We obtain an exact formula for this probability, and from it we derive good lower bounds that approach 1 exponentially fast as the size of the set increases.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q[X]$ the ring of polynomials in one variable over $\mathbb{F}_q$. Let V be a vector space of dimension n over $\mathbb{F}_q$. Given a linear mapping T on V and a subset of vectors $S \subseteq V$ of size m the Krylov subspace generated by S under T is defined as

$$\mathrm{Kry}(T,S) := \left\{ \sum_{i=1}^{m} f_i(T)v_i : \, f_i(X) \in \mathbb{F}_q[X] \text{ and } v_i \in S \text{ for } 1 \le i \le m \right\}.$$

*The second author was supported in part by NSF under Grant DMS9970637, NSA under Grant MDA904-00-1-0048, ONR under Grant N00014-00-1-0565, and South Carolina Commission on Higher Education under a research initiative grant. The third author gratefully acknowledges the support of the EPSRC and St John's College, Oxford. The second author is also grateful to Oxford University Computing Lab for their warm hospitality during his visit in July 2001. *Mathematics Subject Classification 2000*: Primary 14Q10, 11Y99. *Key words and phrases*: finite field, Krylov subspace, matrix.

†Computing Laboratory, Oxford University, Oxford OX1 3QD, U.K. E-mail: richard.brent@comlab.ox.ac.uk

‡Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA. E-mail: sgao@math.clemson.edu.

§Computing Laboratory, Oxford University, Oxford OX1 3QD, U.K. E-mail: alan.lauder@comlab.ox.ac.uk.

This is just the space spanned by all vectors of the form $T^i v$ over all non-negative powers of T and vectors $v \in S$. Define

$$\kappa_m(T) = \frac{1}{q^{mn}} \cdot \#\{(v_1, \ldots, v_m) \in V^m : \mathrm{Kry}(T, \{v_1, \ldots, v_m\}) = V\},$$

that is, $\kappa_m(T)$ is the density of m-tuples of vectors in V that generate the whole space V under T. In other words, if one selects m vectors $v_1, \ldots, v_m$ uniformly at random and independently from V then $\kappa_m(T)$ is the probability that $\mathrm{Kry}(T, \{v_1, \ldots, v_m\}) = V$. Our main goal of this paper is to find good lower bounds on $\kappa_m(T)$.

To state our result, we need to define some parameter depending on T. Let ℓ be the minimal number of vectors required to generate V under T. This number ℓ is just the number of invariants in the Frobenius decomposition of V under T. We call ℓ *the Frobenius index* of T. Our main result is

Theorem. *Let T be a linear mapping on a vector space V of dimension n over $\mathbb{F}_q$. Suppose T has Frobenius index ℓ. Then for $m \geq \ell$*

$$\kappa_m(T) \geq \begin{cases} \frac{0.04}{1+\log_q(n-\ell+1)}, & \text{if } m = \ell \\ \frac{1}{8}, & \text{if } m = \ell + 1 \text{ and } q = 2 \\ 1 - \frac{3}{2^{m-\ell}} \geq \frac{1}{4}, & \text{if } m \geq \ell + 2 \text{ and } q = 2 \\ 1 - \frac{2}{q^{m-\ell}} \geq \frac{1}{3}, & \text{if } m \geq \ell + 1 \text{ and } q > 2. \end{cases}$$

When $m = \ell$ the lower bound is almost tight in the sense that there are infinite many values of n such that the probability approaches zero; see the remark following Corollary 10. Hence it is impossible to bound the probability away from zero in this case. When $m > \ell$, the probability grows exponentially fast to 1 as m increases.

There are two important special cases. One is when T is the identity map, so $\ell = n$. In this case, $\kappa_m(T)$ is equal to the probability that m random vectors in a vector space of dimension n over $\mathbb{F}_q$ span the whole space, and a much better lower bound can be proved (see Lemma 7). The other is when $\ell = 1$, which means that the minimal polynomial of T equals its characteristic polynomial, and better lower bounds are given in Theorem 9.

Our work was motivated by a connection with block iterative methods for solving large sparse linear systems over finite fields, see [3, 4, 8, 11, 12]. It improves upon the result in the report [13] used in an analysis of the block Wiedemann algorithm. A more difficult and important question in the analysis of such algorithms is to bound the probability that certain "truncated" Krylov subspaces generate the whole space. More precisely, let

$$\mathrm{Kry}(T, S; t) = \{\sum_{i=1}^{m} f(T)v_i : f_i(X) \in \mathbb{F}_q[X], \deg f_i \leq t, \text{ and } v_i \in S\}.$$

For t approximately $n/|S|$, one requires a lower bound on the probability that the the above space is the whole space. For large finite fields, relative to the dimension n, Kaltofen [8] obtains such a bound using the Schwartz-Zippel Lemma. For some practical applications, such as integer and polynomial factorization [5, 6, 9, 10], it is desirable to have a good bound for small fields. Using a counting argument Coppersmith obtains a weak bound in [4, 13]; it would be of great interest to strengthen this bound.

We use a module theoretic approach, via a sequence of reductions using standard decomposition theorems and an argument from the theory of abelian groups communicated to us by Simon Blackburn. Using existing results on random elements in vector spaces over finite fields, we then obtain an exact formula (Theorem 5) for the probability depending only on certain properties of the mapping. Finally, good lower bounds for this expression will be derived.

2 Reductions

In this section we consider various reductions which allow us to characterise those sets of vectors which generate the whole space under T.

2.1 Module-theoretic interpretation

Let T be a linear mapping on a vector space V of dimension n over $\mathbb{F}_q$. Denote by V_T the $\mathbb{F}_q[X]$-module with underlying abelian group V and action of $\mathbb{F}_q[X]$ on V defined as

$$f(X) \cdot v := f(T)v$$

for any polynomial $f \in \mathbb{F}_q[X]$. (Any element $v \in V$ may be thought of as lying in V_T, and vice-versa. When necessary to distinguish we shall call elements in V "vectors" and those in V_T "module elements".)

Lemma 1 *For any set $S \subseteq V$ the Krylov space $Kry(T, S)$ equals V if and only if S generates V_T as a $\mathbb{F}_q[X]$-module.*

Proof: Let S be such that the Krylov space gennerated by S under T is V. Let $w \in V$. Thus the vector w equals a linear combination over $\mathbb{F}_q$ of vectors of the form $T^i v$ where $v \in V$. Hence the module element w is a linear combination over $\mathbb{F}_q$ of module elements of the form $X^i.v$ for $v \in S$. Thus S generates V_T as an $\mathbb{F}_q[X]$-module. The converse is similar.

□

Thus our main question is equivalent to the following: given a set of elements S chosen uniformly at random from the module V_T what is the probability they generate V_T?

2.2 Reduction to primary modules

Let the principal ideal (m_T) in $\mathbb{F}_q[X]$ be the annihilator of the module V_T, that is,

$$(m_T) = \{g \in \mathbb{F}_q[x] : g(T)v = 0 \text{ for all } v \in V\}.$$

(Thus m_T, which we take to be monic, is just the minimal polynomial of the linear mapping T.) Factorize m_T as

$$m_T = \prod_{i=1}^{a} g_i^{r_i}$$

where g_i are monic irreducible polynomials and each $r_i \geq 1$. Via the primary decomposition theorem [1, Theorem 3.7.12] the module V_T decomposes as

$$V_T = V_1 \oplus V_2 \oplus \ldots \oplus V_a \tag{1}$$

where the annihilator of V_i is $(g_i^{r_i})$.

For each $1 \leq i \leq a$, let π_i denote the projection of V_T onto its ith factor. For a subset S of elements in V_T write $\pi_i(S)$ for the image of the set S under this projection.

Lemma 2 *Let S be a set of elements in V_T. Then S generates V_T if and only if $\pi_i(S)$ generates V_i for $1 \leq i \leq a$.*

Proof: The forward implication is straightforward. For the reverse, assume that $\pi_i(S)$ generates V_i for $1 \leq i \leq a$. Let $v \in V_T$, so $\pi_i(v) \in V_i$. We can write $\pi_i(v) = \sum_{j=1}^{m} h_{ij}(X).v_j$ where $S = \{v_1, \ldots, v_m\}$. For each $1 \leq j \leq m$ using the Chinese Remainder Theorem we can find a polynomial $h_j(X)$ such that $h_j(X) \equiv h_{ij}(X) \bmod g_i(X)^{r_i}$ for each $1 \leq i \leq a$. Here we use the coprimality of the $g_i(X)$. Defining $w := \sum_{j=1}^{m} h_j(X).v_j$ we see that

$\pi_i(w) = \pi_i(v)$ for all $0 \leq i \leq a$, and hence $v = w$. Thus S generates V_T as we wished to show.

□

Thus it suffices to understand the number of generating sets of the primary modules V_i.

2.3 Reduction to irreducible exponent case

We now examine the primary parts V_i in the decomposition of the module V_T given in Equation (1). To this end, let W denote any $\mathbb{F}_q[X]$-module with annihilator the ideal generated by a power g^r of an irreducible polynomial g. We need to determine the probability that a set of randomly chosen elements in W generates the whole module.

Let $\mathrm{Frat}(W)$ denote the Frattini submodule of W. This is defined to be the intersection of all maximal submodules. The following result is a special case of a module-theoretic analogue of a result in the theory of abelian groups, namely "a set of elements generates an abelian group if and only if its images in the quotient by the Frattini subgroup generate the quotient".

Lemma 3 *Let W be a primary $\mathbb{F}_q[X]$-module with annihilator (g^r), where g is irreducible in $\mathbb{F}_q[X]$. A set $S \subseteq W$ is a generating set if and only if $\bar{S} := \{s + \mathit{Frat}(W) \,|\, s \in S\}$ is a generating set in the quotient module $W/\mathit{Frat}(W)$.*

Proof: The forward implication is easy. For the reverse, by the cyclic decomposition theorem [1, Theorem 3.7.1] we can write

$$W = W_1 \oplus W_2 \oplus \ldots \oplus W_b$$

where each module W_i is cyclic with annihilator the ideal generated by the polynomial g^{r_i} for some power of g. We may take $r_i \geq r_{i+1}$ for $1 \leq i \leq b-1$, and so $r_1 = r$. Since each module in the decomposition is cyclic we have the $\mathbb{F}_q[X]$-module isomorphism

$$W_i \cong \mathbb{F}_q[X]/(g^{r_i})$$

and so

$$W \cong \oplus_{i=1}^{b} \mathbb{F}_q[X]/(g^{r_i}).$$

The intersection of all maximal submodules is just

$$\mathrm{Frat}(W) \cong \oplus_{i=1}^{b} g \cdot (\mathbb{F}_q[X]/(g^{r_i})).$$

which is just $g(X)W$. Hence

$$W/\mathrm{Frat}(W) \cong \mathbb{F}_q[X]/(g) \oplus \ldots \oplus \mathbb{F}_q[X]/(g)$$

where we have b terms in the sum. Now assume that the images of the elements of $S = \{v_i\}$ in the quotient generate $W/\mathrm{Frat}(W)$. Let $w \in W$. Via the isomorphisms described above we have $w = (w_1, \ldots, w_b)$ where each $w_i \in \mathbb{F}_q[X]/(g^{r_i})$. The image of w in the quotient $W/\mathrm{Frat}(W)$ is then $\bar{w} := (w_1 \bmod g, \ldots, w_b \bmod g)$. By assumption we can write $\bar{w} = \sum_{i=1}^{m} h_i(X).\bar{v}_i$. Then $w - \sum_{i=1}^{m} h_i(X).v_i = (gw'_1, \ldots, gw'_b)$. Defining $w' = (w'_1, \ldots, w'_b) \in W$ and repeating the process, we can express w as a combination of the elements v_i plus an "error vector" each coefficient of which is divisible by g^2. Continuing in this way the error vector eventually reduces to zero, since our module is annihilated by some power of g, and we have the desired combination.

□

As in the proof of the above lemma, for W a primary module with annihilator (g^r) the required quotient is just

$$W/\mathrm{Frat}(W) \cong \mathbb{F}_q[X]/(g) \oplus \ldots \oplus \mathbb{F}_q[X]/(g)$$

where we have b terms in the sum. Letting $d = \deg(g)$ we see that this is just the direct sum of b finite fields of order q^d, each viewed as an $\mathbb{F}_q[X]$-module. The action of $\mathbb{F}_q[X]$ on each finite field is just defined for α in the finite field by $X.\alpha = \beta\alpha$, where β is some element such that $g(\beta) = 0$ in the finite field. We have

$$W/\mathrm{Frat}(W) \cong (\mathbb{F}_{q^d})^b$$

as an $\mathbb{F}_q[X]$-module. The righthand-side also has the structure of a vector space over $\mathbb{F}_{q^d}$. A set of elements in $W/\mathrm{Frat}(W)$ is a generating set if and only if the corresponding elements on the righthand-side of above isomorphism generates the set $(\mathbb{F}_{q^d})^b$ as a $\mathbb{F}_{q^d}$-vector space. This follows from the description of the action of $\mathbb{F}_q[X]$ on each vector space in the summand, since $1, \beta, \ldots, \beta^{d-1}$ generates each finite field as a vector space over $\mathbb{F}_q$. Thus we have reduced our problem to the study of generating sets for vector spaces over finite fields.

2.4 Generating sets for vector spaces

For each positive integer n, define the real function $\pi(n, x)$ by

$$\pi(n, x) := (1 - x)(1 - x^2)\ldots(1 - x^n).$$

The following lemma, at least in the prime field case, may be derived from Theorem 1.1 in [2], (Alan: the original ref? include a proof?) taking "$\delta = 0$" and "$\Delta = m - n$" in their notation.

Lemma 4 *Let U be a vector space of dimension b over $\mathbb{F}_q$. Then the probability that $m \geq b$ elements of U chosen uniformly at random span U is*

$$\frac{\pi(m, 1/q)}{\pi(m-b, 1/q)}.$$

Equivalently, the above quantity is the probability that a random $m \times b$ matrix over $\mathbb{F}_q$ has rank b.

3 An exact formula

We now piece the results proved in Section 2 together to obtain an exact formula for the required probability. Let the minimal polynomial of the linear mapping T be denoted m_T and the characteristic polynomial c_T. Let ℓ be the Frobenius index of T. We consider a cyclic decomposition [1, Theorem 3.7.1] of the module V_T as

$$V_T = U_1 \oplus U_2 \oplus \ldots \oplus U_\ell$$

where each U_i is a cyclic module with annihilator the ideal generated by a monic polynomial h_i satisfying $h_{i+1} | h_i$ for $1 \leq i \leq \ell - 1$. Thus $m_T = h_1$ and $c_T = h_1 h_2 \ldots h_\ell$. As before, let g_j, $1 \leq j \leq a$, be the irreducible factors of m_T. Let d_j be the degree of g_j and ℓ_j the number of polynomials $h_1, \ldots, h_l$ divisible by g_j, $1 \leq j \leq a$. Thus $1 \leq \ell_j \leq \ell$ and the cyclic decomposition of the module V_i in the primary decomposition of V_T (see Equation (1)) has exactly ℓ_i factors.

Theorem 5 *Let T be a linear mapping on a vector space V of dimension n over $\mathbb{F}_q$. Suppose T has Frobenius index ℓ and $m \geq \ell$. With the notation defined above, we have*

$$\kappa_m(T) = \prod_{j=1}^{a} \frac{\pi(m, q^{-d_j})}{\pi(m - \ell_j, q^{-d_j})}$$

where $\pi(m, x) = (1-x)(1-x^2)\ldots(1-x^m)$.

Proof: By Lemma 1 one may equivalently find the probability that a uniform at random sequence of elements S in V_T generates V_T as an $\mathbb{F}_q[X]$-module. By Lemma 2 such a set will generate V_T if and only if the set $\pi_j(S)$ generates each primary summand V_j for $1 \leq j \leq a$. Now for any choice of subsets $S_j \subseteq V_j$ of size m, $1 \leq j \leq a$, there exists exactly one set S in V_T such that $\pi_j(S) = S_j$ for each $1 \leq j \leq a$. Conversely, all sets S arise in this way. Thus it suffices to compute the probabilities of generating each primary module V_i by m elements separately, and to take the product.

We claim that the jth term in the product in the statement of the theorem is the probability that a sequence of m elements chosen uniformly at random in V_j will generate V_j. Once this claim is proved the result follows. By Lemma 3 a set of elements S_j in V_j is a generating set if and only if its image in the quotient by the Frattini submodule of V_j generates this quotient. If S_j is chosen uniformly at random in V_j, the corresponding set of elements $\bar{S}_j$ in the quotient will be uniform at random (exactly $|\mathrm{Frat}(V_j)|$ elements of V_j map onto each element in the quotient). Thus we need to find the probability that m elements chosen uniformly at random in the quotient generate it. But the quotient has the structure of a vector space of dimension ℓ_j over $\mathbb{F}_{q^{d_j}}$. From the comments at the end of Section 2.3 this probability is equal to the probability that m elements chosen uniformly at random from a vector space of dimension ℓ_j over $\mathbb{F}_{q^{d_j}}$ span the space. The result now follows from Lemma 4.

□

4 Lower bounds

The formula in Theorem 5 is nice, but it is hard to see the magnitude of the probability $\kappa_m(T)$. In this section we shall derive various simple explicit lower bounds for $\kappa_m(T)$.

We shall repeatedly use the following equality and inequality:

$$\frac{1}{q^k} + \frac{1}{q^{k+1}} + \cdots + \frac{1}{q^m} + \cdots = \frac{1}{q^{k-1}(q-1)},$$
$$(1 - x_1)^{a_1}(1 - x_2)^{a_2} \cdots (1 - x_m)^{a_m} \geq 1 - (a_1x_1 + a_2x_2 + \cdots + a_mx_m),$$

for any real $a_i \geq 1$, $1 \geq x_i \geq 0$, $q > 1$, and any integer $k \geq 0$. The next lemma is an extremely crude estimation, but already useful for large q.

Lemma 6 *Let T be any linear map on a vector space of dimension n over $\mathbb{F}_q$. Let ℓ be the Frobenius index of T. Then, for $m \geq \ell$,*

$$\kappa_m(T) \geq 1 - \frac{n}{q-1}.$$

Proof: With the notation in Theorem 5, as $n \geq a$, $m \geq \ell_j$ and $d_j \geq 1$, we have

$$\begin{aligned} \kappa_m(T) &= \prod_{j=1}^{a} \prod_{i=1}^{\ell_j} \left(1 - \left(\frac{1}{q^{d_j}}\right)^{m-\ell_j+i}\right) \\ &\geq \prod_{j=1}^{n} \prod_{i=1}^{\infty} \left(1 - \left(\frac{1}{q}\right)^{i}\right) \\ &\geq \left(1 - \sum_{i=1}^{\infty} \frac{1}{q^i}\right)^n \geq \left(1 - \frac{1}{q-1}\right)^n \geq 1 - \frac{n}{q-1}. \end{aligned}$$

□

The bound in Lemma 6 is good if q is large, but says nothing if $q \leq n+1$. To get a good lower bound of $\kappa_m(T)$ for small q, we need a more careful estimation. We start with a simple case when T is the identity map on V.

Lemma 7 *Let V be a vector space of dimension n over $\mathbb{F}_q$ and let $m \geq n$. Then the probability that m random vectors in V span the whole space V is*

$$\prod_{i=1}^{n}(1 - \frac{1}{q^{m-n+i}}) \geq \begin{cases} 0.288, & \text{if } m = n \text{ and } q = 2 \\ 1 - \frac{1}{q^{m-n}(q-1)}, & \text{otherwise.} \end{cases}$$

Equivalently, this also bounds the probability that a random $m \times n$ matrix over $\mathbb{F}_q$ has rank n.

Proof: By Lemma 4, the probability is

$$\begin{aligned} \frac{\pi(m, 1/q)}{\pi(m-n, 1/q)} &= (1 - \frac{1}{q^{m-n+1}})(1 - \frac{1}{q^{m-n+2}}) \cdots (1 - \frac{1}{q^m}) \\ &\geq 1 - (\frac{1}{q^{m-n+1}} + \frac{1}{q^{m-n+2}} + \cdots + \frac{1}{q^m}) \\ &\geq 1 - \frac{1}{q^{m-n+1}}(1 + \frac{1}{q} + \cdots + \frac{1}{q^{n-1}} + \cdots) \\ &\geq 1 - \frac{1}{q^{m-n+1}} \frac{1}{1 - 1/q} \geq 1 - \frac{1}{q^{m-n}(q-1)}. \end{aligned}$$

For $m = n$ and $q = 2$, the above bound is zero, so we need a more careful analysis:

$$
\begin{aligned}
&(1-\frac{1}{2})(1-\frac{1}{2^2})\cdots(1-\frac{1}{2^m}) \\
&> (1-\frac{1}{2})(1-\frac{1}{2^2})(1-\frac{1}{2^3})(1-\frac{1}{2^4})(1-\frac{1}{2^5})\cdots(1-\frac{1}{2^m})\cdots \\
&> (1-\frac{1}{2})(1-\frac{1}{2^2})(1-\frac{1}{2^3})(1-\frac{1}{2^4})(1-(\frac{1}{2^5}+\cdots+\frac{1}{2^m}+\cdots)) \\
&= (1-\frac{1}{2})(1-\frac{1}{2^2})(1-\frac{1}{2^3})(1-\frac{1}{2^4})(1-\frac{1}{2^4}) \\
&> 0.288.
\end{aligned}
$$

This completes the proof.

□

To deal with the general case we need the following result, which reduces the problem for a general polynomial to that of a polynomial with irreducible factors of small degrees only.

Lemma 8 *For $k \geq 1$, let I_k be the number of irreducible polynomials in $\mathbb{F}_q[X]$ of degree k. Let $f \in \mathbb{F}_q[X]$ of degree n and let $u = \lfloor \log_q n \rfloor$. Then for any integer $q_1 > 1$*

$$\prod_{g|f,\, g \text{ irred}} \left(1 - \frac{1}{q_1^{\deg g}}\right) \geq \prod_{k=1}^{u+1} \left(1 - \frac{1}{q_1^k}\right)^{I_k}.$$

Proof: This result is proved in [7] (i.e., the formula (6) on page 144, with q replaced by q_1).

□

We consider the important case when V is cyclic as a $\mathbb{F}_q[X]$-module under T, hence $\ell = 1$ and $\ell_j = 1$ in Theorem 5. In this case, the minimal polynomial of T is equal to its characteristic polynomial, and T is called *nonderogatory.*

Theorem 9 *Let T be a nonderogatory linear map on a vector space V of dimension n over $\mathbb{F}_q$. Then*

$$\kappa_m(T) \geq \begin{cases} \frac{0.218}{1+\log_q n}, & \text{if } m = 1, \\ 0.42, & \text{if } m = 2 \text{ and } q = 2, \\ 1 - \frac{1.5}{q^{m-1}} \geq \frac{1}{2}, & \text{otherwise} \end{cases}$$

Proof: Let f be the minimal polynomial of T. Then f has degree n and all $\ell_i = 1$ in Theorem 5. Hence

$$\kappa_m(T) = \prod_{g|f,\, g\,\mathrm{irred}} \left(1 - \frac{1}{q^{m\deg g}}\right).$$

First assume $m = 1$. Then $\kappa_1(T)$ is the density of polynomials in $\mathbb{F}_q[X]$ of degrees $< n$ that are relatively prime to f. In this case, by Theorem 2.1 in [7], we have

$$\kappa_1(T) \geq (1 - \frac{1}{q}) \cdot \frac{1}{e^{0.83}(1 + \log_q n)} > \frac{0.218}{1 + \log_q n},$$

where the factor $1 - 1/q$ counts for the irreducible factor X that is excluded there.

Now assume $m > 1$. Let $u = \lfloor \log_q n \rfloor$ and I_k as in Lemma 8. Note that $I_1 = q$ and

$$I_k \leq \frac{q^k - 1}{k} \leq \frac{q^k}{2}, \quad k \geq 2.$$

By Lemma 8, we have

$$\begin{aligned}
\kappa_m(T) &\geq \prod_{k=1}^{u+1} \left(1 - \frac{1}{q^{mk}}\right)^{I_k} \\
&\geq \left(1 - \frac{1}{q^m}\right)^q \prod_{k=2}^{\infty} \left(1 - \frac{1}{q^{mk}}\right)^{\frac{q^k-1}{k}} \\
&\geq \left(1 - \frac{1}{q^m}\right)^q \left(1 - \sum_{k=2}^{\infty} \frac{q^k - 1}{kq^{mk}}\right) \\
&\geq \left(1 - \frac{1}{q^m}\right)^q \left(1 - \sum_{k=2}^{\infty} \frac{1}{2q^{(m-1)k}}\right) \\
&\geq \left(1 - \frac{1}{q^m}\right)^q \left(1 - \frac{1}{2q^{m-1}(q^{m-1} - 1)}\right)
\end{aligned}$$

which is at least 0.42 when $m = 2$ and $q = 2$, and generally at least

$$\left(1 - \frac{1}{q^{m-1}}\right)\left(1 - \frac{1}{2q^{m-1}(q^{m-1} - 1)}\right) > 1 - \frac{1}{q^{m-1}} - \frac{1}{2q^{m-1}(q^{m-1} - 1)} \geq 1 - \frac{1.5}{q^{m-1}}$$

for all q and m.

□

Theorem 9 can be interpreted for the following situation. Let $f \in \mathbb{F}_q[X]$ be any polynomial of degree n. Define $\kappa_m(f)$ to be the probability that

$$\gcd(f, g_1, \ldots, , g_m) = 1$$

for m random polynomials $g_1, \ldots, g_m \in \mathbb{F}_q[x]$ of degrees $< n$. Note that $\kappa_1(f)$ is the Euler function for the polynomial f. Then for any nonderogatory linear map T on a vector space of dimension n over $\mathbb{F}_q$ that has f as its minimal polynomial, we have

$$\kappa_m(f) = \kappa_m(T) = \prod_{g|f,\, g \,\mathrm{irred}} \left(1 - \frac{1}{q^{m \deg g}}\right).$$

Hence the lower bounds in Theorem 9 applies to $\kappa_m(f)$ automatically.

Corollary 10 *Let $f \in \mathbb{F}_q[x]$ of degree n. Then*

$$\kappa_m(f) \geq \begin{cases} \frac{0.218}{1+\log_q n}, & \text{if } m = 1, \\ 0.42, & \text{if } m = 2 \text{ and } q = 2, \\ 1 - \frac{1.5}{q^{m-1}} \geq \frac{1}{2}, & \text{otherwise} \end{cases}$$

Remark. By Theorem 3.4 in [7], there are infinitely many values of n such that

$$\kappa_1(x^n - 1) \leq \frac{c}{\sqrt{1 + \log_q n}}$$

for some constant $c > 0$ depending only on q. This means that the probability may be arbitrarily close to zero and our lower bound is quite tight to the upper bound. This also applies to the lower bound in Thereom 11 below for $m = \ell$.

Now we turn to the general case where we obtain slightly weaker bounds. The next result is the main theorem stated in the introduction.

Theorem 11 *Let T be any linear map on a vector space of dimension n over $\mathbb{F}_q$. Let ℓ be the Frobenius index of T and let $m \geq \ell$. Then*

$$\kappa_m(T) \geq \begin{cases} \frac{0.04}{1+\log_q(n-\ell+1)}, & \text{if } m = \ell \\ \frac{1}{8}, & \text{if } m = \ell + 1 \text{ and } q = 2 \\ 1 - \frac{3}{2^{m-\ell}} \geq \frac{1}{4}, & \text{if } m \geq \ell + 2 \text{ and } q = 2 \\ 1 - \frac{2}{q^{m-\ell}} \geq \frac{1}{3}, & \text{if } m \geq \ell + 1 \text{ and } q > 2. \end{cases}$$

Proof: Let f be the minimal polynomial of T. Then $\deg f \le n-\ell+1$ as at one irreducible factor of f appears ℓ times in the characteristic polynomial of T, which has degree n and is divisible by f. Let $u = \lfloor \log_q(n-\ell+1) \rfloor$. By Theorem 5 and Lemma 8, we have

$$\begin{aligned}
\kappa_m(T) &= \prod_{j=1}^{a}\prod_{i=1}^{\ell_i}\left(1-\left(\frac{1}{q^{d_j}}\right)^{m-\ell+i}\right) \\
&\ge \prod_{j=1}^{a}\prod_{i=1}^{\ell}\left(1-\left(\frac{1}{q^{d_j}}\right)^{m-\ell+i}\right) \\
&= \prod_{i=1}^{\ell}\prod_{g|f,\, g\,\mathrm{irred}}\left(1-\left(\frac{1}{q^{\deg g}}\right)^{m-\ell+i}\right) \\
&\ge \prod_{i=1}^{\ell}\prod_{k=1}^{u+1}\left(1-\left(\frac{1}{q^{k}}\right)^{m-\ell+i}\right)^{I_k}. \qquad (2)
\end{aligned}$$

Assume first that $m=\ell$. Then

$$\begin{aligned}
\kappa_m(T) &\ge \prod_{i=1}^{\ell}\prod_{k=1}^{u+1}\left(1-\left(\frac{1}{q^{k}}\right)^{i}\right)^{I_k} \\
&\ge \prod_{i=1}^{\ell}\left(1-\frac{1}{q^i}\right)\prod_{i=1}^{\ell}\prod_{k=1}^{u+1}\left(1-\frac{1}{q^{ki}}\right)^{\frac{q^k-1}{k}} \\
&\ge \prod_{i=1}^{\ell}\left(1-\frac{1}{q^i}\right)\prod_{k=1}^{u+1}\left(1-\frac{1}{q^{k}}\right)^{\frac{q^k-1}{k}}\prod_{k=1}^{\infty}\prod_{i=2}^{\infty}\left(1-\frac{1}{q^{ki}}\right)^{\frac{q^k-1}{k}}.
\end{aligned}$$

By Lemma 7, we know the first product is at least 0.288. For the second product, the proof of Theorem 2.1 in [7] implies

$$\prod_{k=1}^{u+1}\left(1-\frac{1}{q^{k}}\right)^{\frac{q^k-1}{k}} \ge \frac{1}{e^{0.83}(1+u)} \ge \frac{1}{e^{0.83}(1+\log_q(n-\ell+1))}.$$

To estimate the third product, we recall the fact that

$$\ln(1-x) \ge -(x+x^2), \quad 0 \le x \le 0.6.$$

Then

$$\prod_{k=1}^{\infty}\prod_{i=2}^{\infty}\left(1-\frac{1}{q^{ki}}\right)^{\frac{q^k-1}{k}} \ \ge\ \exp\left(\sum_{k=1}^{\infty}\sum_{i=2}^{\infty}\frac{q^k-1}{k}\ln(1-\frac{1}{q^{ki}})\right)$$

$$
\begin{aligned}
&\geq \exp\left(-\sum_{k=1}^{\infty}\sum_{i=2}^{\infty}\frac{q^k-1}{k}(\frac{1}{q^{ki}}+\frac{1}{q^{2ki}})\right)\\
&\geq \exp\left(-\sum_{k=1}^{\infty}\frac{q^k-1}{k}(\frac{1}{q^k(q^k-1)}+\frac{1}{q^{2k}(q^{2k}-1)})\right)\\
&\geq \exp\left(-\sum_{k=1}^{\infty}(\frac{1}{q^k}+\frac{1}{q^{3k}})\right)\\
&\geq \exp\left(-(\frac{1}{q-1}+\frac{1}{q^3-1})\right)\\
&\geq \exp\left(-(1+\frac{1}{7})\right) > 0.3189.
\end{aligned}
$$

Therefore, when $m = \ell$,

$$
\kappa_m(T) > \frac{0.288 \cdot 0.3189}{e^{0.83}} \cdot \frac{1}{1+\log_q(n-\ell+1)} > \frac{0.04}{1+\log_q(n-\ell+1)}.
$$

Finally assume $m > \ell$. Then from Equation (2)

$$
\kappa_m(T) \geq \prod_{i=1}^{\infty}\left(1-\frac{1}{q^{m-\ell+i}}\right)^q \prod_{k=2}^{\infty}\prod_{i=1}^{\infty}\left(1-\frac{1}{q^{k(m-\ell+i)}}\right)^{\frac{q^k-1}{k}}.
$$

For the first product, we have

$$
\begin{aligned}
\prod_{i=1}^{\infty}\left(1-\frac{1}{q^{m-\ell+i}}\right)^q &\geq \left(1-\frac{q}{q^{m-\ell+1}}\right)\left(1-\sum_{i=2}^{\infty}\frac{q}{q^{m-\ell+i}}\right)\\
&\geq \left(1-\frac{1}{q^{m-\ell}}\right)\left(1-\frac{1}{q^{m-\ell}(q-1)}\right)
\end{aligned}
$$

which is $1/4$ for $m = \ell + 1$ and $q = 2$. For the second product, we have

$$
\begin{aligned}
\prod_{k=2}^{\infty}\prod_{i=1}^{\infty}\left(1-\frac{1}{q^{k(m-\ell+i)}}\right)^{\frac{q^k-1}{k}} &\geq 1-\sum_{k=2}^{\infty}\sum_{i=1}^{\infty}\frac{q^k-1}{kq^{k(m-\ell+i)}}\\
&\geq 1-\sum_{k=2}^{\infty}\sum_{i=1}^{\infty}\frac{1}{kq^{k(m-\ell+i-1)}}\\
&\geq 1-\sum_{k=2}^{\infty}\frac{1}{kq^{k(m-\ell-1)}(q^k-1)}
\end{aligned}
$$

$$\geq \; 1 - \sum_{k=2}^{\infty} \frac{1}{q^{k(m-\ell)}}$$
$$\geq \; 1 - \frac{1}{q^{m-\ell}(q^{m-\ell}-1)}$$

which is 1/2 for $m = \ell + 1$ and $q = 2$. Therefore $\kappa_m(T)$ is at least $\frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$ for $m = \ell + 1$ and $q = 2$. In general when $m > \ell$ it is at least

$$\left(1 - \frac{1}{q^{m-\ell}}\right)\left(1 - \frac{1}{q^{m-\ell}(q-1)}\right)\left(1 - \frac{1}{q^{m-\ell}(q^{m-\ell}-1)}\right)$$
$$\geq 1 - \frac{1}{q^{m-\ell}} - \frac{1}{q^{m-\ell}(q-1)} - \frac{1}{q^{m-\ell}(q^{m-\ell}-1)}$$
$$\geq 1 - \frac{q+1}{q-1}\frac{1}{q^{m-\ell}} \geq 1 - \frac{3}{q^{m-\ell}}.$$

For $q = 2$ and $m \geq \ell + 2$ this is $1 - \frac{3}{2^{m-\ell}} \geq \frac{1}{4}$, and for $q \geq 3$ and $m \geq \ell + 1$ at least $1 - \frac{2}{q^{m-1}} \geq \frac{1}{3}$.

□

References

[1] W. A. Adkins and S. H. Weintraub, *Algebra: an approach via module theory*, Graduate Texts in Mathematics 136, Springer-Verlag, 1992.

[2] R. P. Brent and B. D. McKay, "Determinants and ranks of random matrices over $\mathbb{Z}_m$", *Discrete Mathematics* **66** (1987), 35-49.

[3] D. Coppersmith, "Solving linear equations over $GF(2)$: block Lanczos algorithm", *Linear Algebra and Its Applications*, **192** (1993), 33–60.

[4] D. Coppersmith, "Solving homogeneous linear equations over $GF(2)$ via block Wiedemann algorithm", *Math. Comp.* **62** (1994), no. 205, 333-350.

[5] S. Gao, "Factoring multivariate polynomials via partial differential equations", to appear in Mathematics of Computation. (28 pages).

[6] S. Gao and J. von zur Gathen, "Berlekamp's and Niederreiter's polynomial factorization algorithms", *Proc. 2nd International Conference on Finite Fields: Theory, Applications, and Algorithms*, Las Vegas, 1993. *Contemporary Mathematics*, vol. 168, 1994, 101–116.

[7] S. Gao and D. Panario, "Density of normal elements in finite fields", *Finite Fields and Their Applications*, **3** (1997), 141–150.

[8] E. Kaltofen, "Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems", *Math. Comp.*, **64** (1995), 777–806.

[9] E. Kaltofen and A. Lobo, "Factoring high-degree polynomials by the black box Berlekamp algorithm," in *ISSAC'94*, 90-98.

[10] A. K. Lenstra and H. W. Lenstra, Jr., editors, *The Development of the Number Field Sieve*, Lecture Notes in Mathematics, no. 1554, Springer-Verlag, 1993.

[11] P. L. Montgomery, "A block Lanczos Algorithm for finding dependencies over $GF(2)$", *Advances in cryptology—EUROCRYPT '95* (Saint-Malo, 1995), LNCS 921, Springer, Berlin, 1995, 106–120.

[12] G. Villard, "Further analysis of Coppersmith's block Wiedemann algorithm for the solution of sparse linear systems," in *International Symposium on Symbolic and Algebraic Computation*, Maui, Hawaii, USA. ACM Press, July 1997.

[13] G. Villard, "A study of Coppersmith's block Wiedemann algorithm using matrix polynomials", LMC-IMAG, report # 975 IM, April 1997. (38 pages)