APPEARED IN *Random Structures and Algorithms* **10(4)** (1997) 407-419.

The Rank of Sparse Random Matrices over Finite Fields

Johannes Blömer[*], Richard Karp[†], Emo Welzl[‡]

Abstract

Let M be a random matrix over GF$[q]$ such that for each entry M_{ij} in M and for each non-zero field element α the probability $\Pr[M_{ij} = \alpha]$ is $p/(q-1)$, where $p = (\log n - c)/n$ and c is an arbitrary but fixed positive constant. The probability for a matrix entry to be zero is $1-p$. It is shown that the expected rank of M is $n - \mathcal{O}(1)$. Furthermore, there is a constant A such that the probability that the rank is less than $n-k$ is less than A/q^k. It is also shown that if c grows depending on n and is unbounded as n goes to infinity then the expected difference between the rank of M and n is unbounded.

1 Introduction

In this paper we investigate the rank of random matrices over a fixed but arbitrary finite field GF$[q]$. Given some p, $0 \leq p \leq 1$, we choose the entries in the matrix M independently, so that 0 is attained with probability $1-p$, and each nonzero element in GF$[q]$ is attained with probability $p/(q-1)$. We want to get M as sparse as possible (i.e. choose p as small as possible), while maintaining the expected rank close to the dimension of the matrix. It turns out that if we want to achieve an expected rank of $n - \mathcal{O}(1)$ then $p = (\log n - c)/n$[1] is the crucial threshold. We also prove that with high probability the rank of a random matrix is not much less than its expected rank.

We achieve these results by establishing for an arbitrary matrix M a simple relationship between the quantity $n - \mathrm{rank}(M)$ and the number of linear dependencies of M, that is, the number of ways in which the all zero vector can be written as a linear combination of the rows of M. Then the main technical result of this paper shows that the expected number of linear dependencies is bounded by a constant iff $p \geq (\log n - c)/n$, where c is some arbitrary positive constant.

It is a well-known fact (see [8]), that a random $(n \times n)$-matrix over GF$[q]$, where each entry is chosen independently and uniformly at random from the elements of GF$[q]$, is

[*]Institut für Theoretische Informatik, Eidgenössische Technische Hochschule Zürich, ETH Zentrum, CH-8092 Zurich, Switzerland. Part of work done while a postdoc at the International Computer Science Institute, Berkeley, California. Research supported by Deutsche Forschungsgemeinschaft (DFG), Habilitationsstipendium Bl 314/4-1

[†]Department of Computer Science and Engineering, University of Washington, Seattle, Washington, WA 98105

[‡]Institut für Theoretische Informatik, Eidgenössische Technische Hochschule Zürich, ETH Zentrum, CH-8092 Zurich, Switzerland. Part of work done while at the Free University Berlin, Germany. Supported by a Leibniz Award from Deutsche Forschungsgemeinschaft (DFG), grant We 1265/5-1.

[1]log is the natural logarithm, $\log \mathrm{e} = 1$.

nonsingular with at least some constant probability[2]. Comparing this to the results of this paper naturally leads to the following question. How small can p be chosen such that a random $(n \times n)$-matrix over a finite field will be nonsingular with some constant probability? We show that if p is an arbitrary constant then random matrix is nonsingular with some constant probability[3]. However, the techniques and results of this paper do not seem to be sufficient to determine the exact threshold for p. Or show that p can be nonconstant while preserving the property that the random matrix based on p is nonsingular with some constant probability.

Our results are complementary to a recent result of Calkin [3] about linear dependencies over finite fields GF[q]. Calkin shows, that for any constant k there is another constant β_k (depending on q) such that if $\beta_k n$ n-dimensional vectors are chosen uniformly at random from the set of all vectors with k 1's, then the probability that these vectors are linearly dependent goes to 1 as n goes to infinity. Calkin's result generalizes and supersedes previous results by Kolchin and Khokhlov [6]. The results of our paper imply the following result. Assume that $c(n)$ is a function that is unbounded as n goes to infinity and assume that $p = (\log n - \mathcal{O}(1))/n$. If n vectors are chosen in $(\mathrm{GF}[2])^n$ such that each entry in a vector is 1 with probability p, then the probability that less than $n - c(n)$ of these vectors are linearly independent tends to 0 for $n \to \infty$.

If the elements of an $r \times n$ random matrix are chosen uniformly at random from some finite field GF[q] more general statements than the ones obtained in this paper can be achieved. For these random matrices Kelly and Oxley study the matroid generated by columns of the matrix. They show for various matroid properties (like connectivity and existence of circuits of a certain size) that if n is large enough compared to r then it is very likely for a random matroid to have these properties.

Finally our results should be compared to the following result for $(0,1)$-matrices over the reals. Assume M is a random $(0,1)$-matrix, where each entry is 1 with probability $1/2$. Then there is a positive constant ϵ such that M is singular with probability less than $(1-\epsilon)^n$ (see [7]; for a simpler proof that this probability goes to 0 see [2].)

2 The results

In this section we state the main results of this paper.

We use $\mathrm{rank}(M)$ to denote the rank of an $(n \times n)$-matrix M, and $\mathrm{d}(M)$ to denote $n - \mathrm{rank}(M)$, called the *defect* of M. The following theorem is the main technical contribution of this paper.

Theorem 2.1 *Let M be a random $(n \times n)$-matrix over a fixed finite field* GF[q] *with $p = (\log n - c)/n$ and $n \geq \mathrm{e}^c$, for a* fixed *$c \geq 0$. Then the defect* $\mathrm{d}(M)$ *of M satisfies*

$$\mathrm{Exp}[q^{\mathrm{d}(M)}] = \mathcal{O}(1).$$

Moreover, if $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ *is considered as a function of the probability p, then* $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ *decreases monotonically in the range* $0 \leq p \leq \frac{q-1}{q}$.

[2][8] claims that this probability tends to 0 as n goes to infinity. However, it is easily seen that the proof of this claim is not correct.

[3]We thank an anonymous referee for pointing this out to us.

The theorem implies that for any $(\log n - \mathcal{O}(1))/n \leq p \leq (q-1)/q$ the expectation $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ is upper bounded by some constant. Because of the monotonicity of $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ in the sequel we will concentrate on probabilities p that are close to $\log n/n$.

The following lower bounds show that Theorem 2.1 is essentially optimal. Here, as opposed to the previous theorem, c is not considered fixed!

Theorem 2.2 *Let M be a random $(n \times n)$-matrix over the finite field* $\mathrm{GF}[q]$ *with $p = (\log n - c)/n$, for $c = c(n)$, $0 \leq c(n) < \log n - \log(q-1)$. Then the defect $\mathrm{d}(M)$ of M satisfies*

$$\mathrm{Exp}[q^{\mathrm{d}(M)}] = \Omega\left(\mathrm{e}^{\frac{q-1}{4}\mathrm{e}^{c}}\right).$$

The expected number of zero rows of M is $\Omega(\mathrm{e}^{c})$.

From these theorems we easily derive the following corollaries.

Corollary 2.3 *Let $c(n)$ be a function with $0 \leq c(n) < \log n$ for all n. Then* $\mathrm{Exp}[\mathrm{d}(M)] = \mathcal{O}(1)$ *for random $(n \times n)$ matrices with $p = (\log n - c(n))/n$, if and only if the function $c(n)$ is bounded.*

Proof: If $c(n)$ is bounded then by Theorem 2.1 $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ is bounded by some constant A. Jensen's inequality implies that $\mathrm{Exp}[\mathrm{d}(M)]$ is bounded by $\log_q A$.

If $c(n)$ is unbounded Theorem 2.2 shows that the expected number of zero rows is unbounded. This implies that $\mathrm{d}(M)$ is unbounded. □

Corollary 2.4 *For every $c \geq 0$ there exists a constant A_c such that a random $(n \times n)$ matrix M, $n > \mathrm{e}^c$, with $p = (\log n - c)/n$ satisfies*

$$\Pr[\mathrm{d}(M) \geq k] \leq \frac{A_c}{q^k}.$$

for all positive integers k.

Proof: By Markov's inequality

$$\Pr[\mathrm{d}(M) \geq k] = \Pr[q^{\mathrm{d}(M)} \geq q^k] \leq \frac{\mathrm{Exp}[q^{\mathrm{d}(M)}]}{q^k}.$$

The corollary follows from Theorem 2.1. □

3 Rank and linear dependencies

In order to prove Theorem 2.1 and Theorem 2.2 we relate the defect of a matrix over $\mathrm{GF}[q]$ to the number of linear dependencies.

Definition 3.1 *Let M be a $(n \times n)$-matrix over* GF$[q]$. *Denote by $M_1, \ldots, M_n$ the rows of M. A vector $(c_1, \ldots, c_n) \in (\mathrm{GF}[q])^n$ such that not all c_i are zero is called a linear dependency iff*

$$\sum_{i=1}^{n} c_i M_i = 0. \tag{1}$$

$l(M)$ denotes the number of linear dependencies of the rows of the matrix M.

Lemma 3.2 *Let M be an $(n \times n)$-matrix over* GF$[q]$ *then*

$$q^{d(M)} - 1 = l(M).$$

Proof: Let $d = d(M)$ be the defect of M. Since $k = n - d$ is the rank of M, any maximal subset of linearly independent rows of M has size k. Without loss of generality we may assume that the first k rows of M are such a maximal subset. This implies that the subspace generated by the last d rows of M is contained in the subspace generated by the first k rows. Hence any non-zero vector of length d in $(\mathrm{GF}[q])^d$ can be extended to a linear dependency. This extension is unique. Otherwise there is a linear dependency where the last d coordinates are zero, which contradicts the linear independence of the first k rows. Therefore the number of linear dependencies is given by $q^d - 1$. $\square$

Next we derive an explicit expression for the expected number of linear dependencies.

Theorem 3.3 *Let M be a random $(n \times n)$-matrix over* GF$[q]$, *based on some p, $0 \le p \le 1$. The expected number of linear dependencies of the rows of M is*

$$\sum_{k=1}^{n} \binom{n}{k} \frac{1}{q^{n-k}} \left(1 - \frac{1}{q}\right)^k \left[1 + (q-1)\left(1 - \frac{qp}{q-1}\right)^k\right]^n.$$

Proof: Fix some non-zero vector $c = (c_1, \ldots, c_n) \in (\mathrm{GF}[q])^n$, with exactly k non-zero coordinates. Without loss of generality assume that the first k coordinates of c are non-zero. Let P_k be the probability that $\sum_{i=1}^{k} c_i m_i = 0$, where each m_i is chosen according to the distribution for the matrix entries M_{ij}. Then the probability that c is a linear dependency is given by $P_k^{\,n}$.

Since the c_i's are fixed the following recursion holds for P_k.

$$P_0 = 1 \text{ and } P_k = P_{k-1}(1-p) + (1 - P_{k-1})p/(q-1). \tag{2}$$

Set $Q_k = P_k - \frac{1}{q}$. It follows from (2) that

$$Q_0 = \frac{q-1}{q} \text{ and } Q_k = Q_{k-1}\left(1 - \frac{qp}{q-1}\right). \tag{3}$$

Hence

$$Q_k = \frac{q-1}{q}\left(1 - \frac{qp}{q-1}\right)^k \text{ and } P_k = \frac{q-1}{q}\left(1 - \frac{qp}{q-1}\right)^k + \frac{1}{q}.$$

The number of vectors c with exactly k non-zero coordinates is given by $\binom{n}{k}(q-1)^k$. Hence

$$\mathrm{Exp}[l(M)] = \sum_{k=1}^{n} \binom{n}{k} (q-1)^k P_k^n = \frac{1}{q^n} \sum_{k=1}^{n} \binom{n}{k} (q-1)^k \left[1 + (q-1)\left(1 - \frac{qp}{q-1}\right)^k\right]^n$$

$$= \sum_{k=1}^{n} \binom{n}{k} \frac{1}{q^{n-k}} \left(1 - \frac{1}{q}\right)^k \left[1 + (q-1)\left(1 - \frac{qp}{q-1}\right)^k\right]^n .$$

$\square$

Observe that in the expression for the expected number of linear dependencies the terms $(1-1/q)^k/q^{n-k}$ are the probabilities for exactly k successes in a Bernoulli experiment with success probability $1-1/q$. This turns out to be very useful in the proof of Theorem 2.1.

4 The lower bound

In this section we prove

Theorem 2.2 *Let M be a random $(n \times n)$-matrix over the finite field* $\mathrm{GF}[q]$ *with $p = (\log n - c)/n$, for $c = c(n)$, $0 \le c(n) < \log n - \log(q-1)$. Then the defect* $\mathrm{d}(M)$ *of M satisfies*

$$\mathrm{Exp}[q^{\mathrm{d}(M)}] = \Omega\left(\mathrm{e}^{\frac{q-1}{4}\mathrm{e}^c}\right).$$

The expected number of zero rows of M is $\Omega(\mathrm{e}^c)$.

Proof: In order to simplify the notation we set $\gamma = 1 - 1/q$. By Theorem 3.3 the number of linear dependencies is

$$\sum_{k=1}^{n} \binom{n}{k} \gamma^k (1-\gamma)^{n-k} \left[1 + (q-1)(1-p/\gamma)^k\right]^n .$$

By the DeMoivre-Laplace Limit Theorem (see [4], p.186) $\sum_{1 \le k \le \gamma n} \binom{n}{k} (1-\gamma)^{n-k}\gamma^k$ is bounded from below by some constant. To prove the first part of the theorem it therefore suffices to show that for $k \le \gamma n$ the expression $\left[1 + (q-1)(1-p/\gamma)^k\right]^n$ is bounded from below by

$$\mathrm{e}^{\frac{q-1}{4}\mathrm{e}^c}.$$

We may assume that n is large enough so that $p/\gamma < 1$. Hence $\left[1 + (q-1)(1-p/\gamma)^k\right]^n$ decreases as k increases and it suffices to prove the lower bound on this expression for $k = \gamma n$, where, for the time being, we allow k to attain non-integral real values.

Since, for n large enough, $p/\gamma \le 1/2$, and since $1 - x \ge \mathrm{e}^{-x-x^2}$ for $0 \le x \le 1/2$, we have

$$\left[1 + (q-1)(1-p/\gamma)^k\right]^n \ge \left[1 + (q-1)\mathrm{e}^{-pk/\gamma - p^2k/\gamma^2}\right]^n .$$

Plugging in the values $p = (\log n - c)/n$ and $k = \gamma n$ we obtain

$$\mathrm{e}^{-pk/\gamma} = \frac{1}{n}\mathrm{e}^c.$$

For these values of p and k the term $\mathrm{e}^{-p^2k/\gamma^2} = \mathrm{e}^{-(\log n - c)^2/(\gamma n)}$ converges to 1 as n goes to infinity. In particular, for n large enough it is larger than $1/2$. Hence

$$\left[1 + (q-1)\mathrm{e}^{-pk/\gamma - p^2k/\gamma^2}\right]^n \ge \left[1 + (q-1)\mathrm{e}^{c(n)}/2n\right]^n .$$

By assumption, $c(n) \leq \log n - \log(q-1)$, and therefore $(q-1)\mathrm{e}^{c(n)}/2n \leq 1/2$. Applying $1+x \geq \mathrm{e}^{x/2}$ for $0 \leq x \leq 1/2$ shows

$$\left[1+(q-1)\mathrm{e}^{c(n)}/2n\right]^n \geq \mathrm{e}^{\frac{q-1}{4}\mathrm{e}^{c(n)}}.$$

The statement on the number of zero rows is proven similarly. ❑

5 The upper bound

In this section we prove

Theorem 2.1 *Let M be a random $(n \times n)$-matrix over the finite field* $\mathrm{GF}[q]$ *with $p = (\log n - c)/n$ and $n \geq \mathrm{e}^c$, for a* fixed *$c \geq 0$. Then the defect* $\mathrm{d}(M)$ *of M satisfies*

$$\mathrm{Exp}[q^{\mathrm{d}(M)}] = \mathcal{O}(1).$$

Moreover, if $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ *is considered as a function of the probability p, then* $\mathrm{Exp}[q^{\mathrm{d}(M)}]$ *decreases monotonically in the range $0 \leq p \leq \frac{q-1}{q}$.*

By Lemma 3.2 it suffices to prove the theorem for the expected number of linear dependencies. By Theorem 3.3 the expected number of dependencies is given by

$$\sum_{k=1}^{n} \binom{n}{k} \gamma^k (1-\gamma)^{n-k} \left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n ,$$

where we use γ short for $1-1/q$. The monotonicity of the expectation follows immediately from this formula. In order to prove the first and much more difficult part of the theorem the sum for the number of linear dependencies is split into five parts, which are analyzed separately in the following five lemmas.

Lemma 5.1

$$\sum_{k=\gamma n(1-1/\log n)}^{n} \binom{n}{k} \gamma^k (1-\gamma)^{n-k} \left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n \leq \mathrm{e}^{(q-1)\mathrm{e}^{c+1}}.$$

Proof: It will be shown that for $k = \gamma n(1-1/\log n)$

$$\left[1+(q-1)(1-p/\gamma)^k\right]^n \leq \mathrm{e}^{(q-1)\mathrm{e}^{c+1}}.$$

Since $\left[1+(q-1)(1-p/\gamma)^k\right]^n$ decreases as k increases and since $\sum_{k=1}^{n} \binom{n}{k} \gamma^k (1-\gamma)^{n-k} \leq 1$ this will prove the lemma. Using $1+x \leq \mathrm{e}^x$ we get

$$\left[1+(q-1)(1-p/\gamma)^k\right]^n \leq \left[1+(q-1)\mathrm{e}^{-pk/\gamma}\right]^n \leq \mathrm{e}^{n(q-1)\mathrm{e}^{-pk/\gamma}}. \tag{4}$$

Plugging in the values $p = (\log n - c)/n$ and $k = \gamma n(1-1/\log n)$ yields

$$\mathrm{e}^{n(q-1)\mathrm{e}^{-pk/\gamma}} \leq \mathrm{e}^{n(q-1)\mathrm{e}^{-\log n + c + 1}} \leq \mathrm{e}^{(q-1)\mathrm{e}^{c+1}}.$$

❑

Lemma 5.2

$$\sum_{k=\frac{2n\log\log n}{\log n}}^{\gamma n(1-1/\log n)} \binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n \to 0 \quad as \quad n\to\infty.$$

Proof: Consider

$$\sum_{k=\frac{2n\log\log n}{\log n}}^{\gamma n(1-1/\log n)} \binom{n}{k}\gamma^k(1-\gamma)^{n-k}$$

By Chernoff bounds (see [1], Theorem A.13.) this is upper-bounded by

$$\mathrm{e}^{-\frac{\gamma n}{2\log^2 n}}.$$

Using (4) and the fact that $\left[1+(1-p/\gamma)^k\right]^n$ is monotonically decreasing as a function of k we obtain

$$\sum_{k=\frac{2n\log\log n}{\log n}}^{\gamma n(1-1/\log n)} \binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n$$

$$\leq \mathrm{e}^{-\frac{\gamma n}{2\log^2 n}}\mathrm{e}^{n(q-1)\mathrm{e}^{-2pn\log\log n/(\gamma\log n)}} = \mathrm{e}^{-\frac{\gamma n}{2\log^2 n}}\mathrm{e}^{n(q-1)\mathrm{e}^{-2(1-c/\log n)\log\log n/\gamma}}.$$

For n large enough

$$\mathrm{e}^{-2(1-c/\log n)\log\log n/\gamma} \leq \frac{1}{\log^\delta(n)},$$

for some δ that is strictly larger than 2. Hence

$$\mathrm{e}^{-\frac{\gamma n}{2\log^2 n}}\mathrm{e}^{\frac{n(q-1)}{\log^\delta(n)}}$$

tends to 0 as n tends to infinity and the lemma follows. ◻

Lemma 5.3 *Let μ be a positive constant satisfying*

$$\gamma(1-\mu)^2 > \frac{2}{q^3}.$$

Then

$$\sum_{k=5\gamma(\log q)n/\log n}^{\mu\gamma n} \binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n \to 0 \quad as \quad n\to\infty.$$

Proof: Observe that since $2/(q^3\gamma)\leq 1$ a constant μ as required by the lemma exists. By Chernoff bounds ([1], Theorem A.13.) and the assumption for μ

$$\sum_{k=5\gamma(\log q)n/\log n}^{\mu\gamma n} \binom{n}{k}\gamma^k(1-\gamma)^{n-k} \leq \mathrm{e}^{-(1-\mu)^2\gamma n/2} \leq \mathrm{e}^{-\frac{n}{q^3}}.$$

Using (4) it follows that for $k\geq 5\gamma(\log q)n/\log n$

$$\left[1+(q-1)(1-p/\gamma)^k\right]^n \leq \left[1+(q-1)\mathrm{e}^{-5(\log q)}\mathrm{e}^{5c(\log q)/\log n}\right]^n.$$

Since $e^{5c\log q/\log n}$ goes to 1 as n goes to infinity, for n large enough the last expression can be bounded by

$$\left(1+\frac{3}{2q^4}\right)^n \leq e^{\frac{3n}{2q^4}}.$$

The lemma follows. $\square$

Lemma 5.4

$$\sum_{k=\gamma n/\log n}^{5\gamma(\log q)n/\log n} \binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n \to 0 \quad as \quad n\to\infty.$$

Proof: Using for k the value $\gamma n/\log n$ we get that in the range covered by the lemma

$$\left[1+(q-1)(1-p/\gamma)^k\right]^n \leq \left[1+\frac{(q-1)e^{c/\log n}}{e}\right]^n.$$

Since $e^{c/\log n}$ goes to 1 as n goes to infinity, for n large enough this expression is less than $(2q/e)^n$.

We may assume that $5\gamma(\log q)n/\log n \leq n/2$. Therefore in the range under consideration $\binom{n}{k}$ is upper-bounded by the term for $k = 5\gamma(\log q)n/\log n$. Using $\binom{n}{k} \leq (en/k)^k$ we obtain

$$\binom{n}{5\gamma(\log q)n/\log n} \leq (2\log n)^{5\gamma(\log q)n/\log n}.$$

This implies that for $\gamma n/\log n \leq k \leq 5\gamma(\log q)n/\log n$

$$\binom{n}{k}\gamma^k(1-\gamma)^{n-k} = \binom{n}{k}\frac{1}{q^n}(q-1)^k \leq \frac{1}{q^n}(2(q-1)\log n)^{5\gamma(\log q)n/\log n}.$$

This expression can be bounded by

$$\frac{1}{q^n}e^{an\log\log n/\log n},$$

for some positive constant a. Combining this with the previous estimate for $[1+(q-1)(1-p/\gamma)^k]^n$ shows

$$\binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n$$
$$\leq \frac{1}{q^n}e^{an\log\log n/\log n}\left(\frac{2q}{e}\right)^n = e^{-\Omega(n)}.$$

This proves the lemma. $\square$

Lemma 5.5

$$\sum_{k=1}^{\gamma n/\log n} \binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n = \mathcal{O}(1).$$

Proof: By the binomial formula

$$\left[1+(q-1)(1-p/\gamma)^k\right]^n \leq \left[1+(q-1)\left(1-pk/\gamma+p^2k^2/(2\gamma^2)\right)\right]^n$$

provided

$$\binom{k}{i-1}(p/\gamma)^{i-1} \geq \binom{k}{i}(p/\gamma)^i. \tag{5}$$

This condition is equivalent to

$$\frac{\gamma}{p} \geq \binom{k}{i}\Big/\binom{k}{i-1} = \frac{k-i+1}{i}.$$

$(k-i+1)/i \leq k/3$ for $i \geq 3$, and

$$\frac{\gamma}{p} = \frac{\gamma n}{(1-c/\log n)\log n} \geq \frac{\gamma n}{\log n}.$$

Since $k \leq \gamma n/\log n$ this shows that (5) is satisfied.

Next

$$\left[1+(q-1)\left(1-pk/\gamma+p^2k^2/(2\gamma^2)\right)\right]^n = q^n\left[1-pk+p^2k^2/(2\gamma)\right]^n$$

$$\leq q^n \mathrm{e}^{-pkn}\mathrm{e}^{p^2k^2n} = q^n\mathrm{e}^{-(1-c/\log n)k\log n}\mathrm{e}^{(1-c/\log n)^2k^2\log^2 n/n} \leq q^n\frac{1}{n^k}\mathrm{e}^{ck}\mathrm{e}^{k^2\log^2 n/n}.$$

Using $\binom{n}{k} \leq n^k/k!$ yields

$$\binom{n}{k}\gamma^k(1-\gamma)^{n-k}\left[1+(q-1)\left(1-p/\gamma\right)^k\right]^n = \binom{n}{k}\frac{1}{q^n}(q-1)^k\left[1+(q-1)(1-p/\gamma)^k\right]^n$$

$$\leq \frac{1}{k!}(q-1)^k\mathrm{e}^{k^2\log^2 n/n}\mathrm{e}^{ck} = \frac{1}{k!}\mathrm{e}^{k^2\log^2 n/n}\mathrm{e}^{ak},$$

with $a = c + \log(q-1)$.

It follows that for any constant C_1 there is a constant C_2 such that for all $k \leq C_1$

$$\binom{n}{k}\frac{1}{q^n}(q-1)^k\left[1+(q-1)(1-p/\gamma)^k\right]^n \leq C_2.$$

Therefore the lemma follows if

$$\sum_{k=C}^{\gamma n/\log n}\binom{n}{k}\frac{1}{q^n}(q-1)^k\left[1+(q-1)(1-p/\gamma)^k\right]^n = \mathcal{O}(1) \tag{6}$$

for some constant C.

To prove (6) it will be shown that for n large enough

$$\frac{1}{(k-2)!}\mathrm{e}^{k^2\log^2 n/n}\mathrm{e}^{ak} \leq 1. \tag{7}$$

(7) then implies

$$\sum_{k=C}^{\gamma n/\log n} \binom{n}{k} \frac{1}{q^n}(q-1)^k \left[1+(q-1)(1-p/\gamma)^k\right]^n \leq \sum_{k=C}^{\gamma n/\log n} \frac{1}{k(k-1)}.$$

Since $\sum_{k=1}^{\infty} 1/k^2$ is constant this proves Equation (6) and the lemma.

In order to prove (7), first Stirling's formula (see [4]) is used to bound $(k-2)!$ from below.

$$(k-2)! \geq (k-2)^{k-2}\mathrm{e}^{-(k-2)} = \mathrm{e}^{(k-2)\log(k-2)-(k-2)} \geq \mathrm{e}^{(k-2)(\log(k)-2)}.$$

(7) follows if there exists a constant C such that for all k between C and $\gamma n/\log n$

$$\frac{k-2}{k^2}(\log(k)-2) - \frac{a}{k} \geq \frac{\log^2 n}{n}. \tag{8}$$

Taking the derivative it can be shown that there is a constant C such that in the range $k \geq C$ the left-hand side of (8) is monotonically decreasing. It therefore suffices to prove Equation (8) for $k = \gamma n/\log n$. For this value of k (8) becomes

$$\frac{\log n}{\gamma n}[\log n - \log\log n - 3] - \frac{2\gamma^2 \log^2 n}{n^2}[\log n - \log\log n - 3] - \frac{a\log n}{\gamma n} \geq \frac{\log^2 n}{n}.$$

For n large enough this is correct since the dominating term on the left-hand side is $\log^2 n/\gamma n$ and $1/\gamma$ is strictly larger than 1. This finishes the proof of Lemma 5.4. $\square$

Theorem 2.1 now follows easily from the five preceding lemmas. If n is large enough such that $2n(\log\log n)/\log n$ is less than $\mu\gamma n$ then the lemmas cover the whole range of $1 \leq k \leq n$.

6 Generalizations and open problems

The analysis given in the previous section can be generalized to show the next theorem.

Theorem 6.1 *Let M be a random $(n \times n)$-matrix over the finite field* $\mathrm{GF}[q]$ *with $p = (\log n - c(n))/n$, where $c(n)$ is some function satisfying $0 \leq c(n) \leq a\log n$ and $0 \leq a < 1$ is some arbitrary but fixed constant. Then the defect* $\mathrm{d}(M)$ *satisfies*

$$\mathrm{Exp}[q^{\mathrm{d}(M)}] \leq \mathrm{e}^{\mathrm{e}^{\mathcal{O}(c(n)+1)}}.$$

Combining this with Jensen's inequality, Lemma 3.2, and Theorem 2.2 gives the following corollary.

Corollary 6.2 *Let M be a random matrix as in the previous theorem. Then*

$$\mathrm{Exp}[\mathrm{d}(M)] = \mathrm{e}^{\Theta(c(n)+1)}.$$

In other words, the defect of M increases exponentially with $c(n)$. We conjecture that this is true for an arbitrary function c satisfying $0 \leq c(n) < \log n$. However, the estimates used in Section 5 don't seem to be strong enough to prove this conjecture.

It is a well-known result (see for example [8]) that a random $(n \times n)$-matrix over GF$[q]$, where each entry is chosen independently and uniformly at random from the elements of GF$[q]$, is nonsingular with at least some constant probability. For example, over GF[2] the probability tends to approximately 0.29 (and the probability that the defect exceeds 2 is always less than 0.06). On the other hand, Corollary 2.4 shows that for $p = (\log n - c)/n$ the random matrix M has constant defect with high probability.

This raises the following question. Assume that a random $(n \times n)$-matrix M over GF[2] is chosen such that each entry M_{ij} is 0 with probability $1 - p$ and is 1 with probability p. What is the smallest p such that the probability that M is nonsingular is bounded from below by some constant c? The next theorem shows that if p is an arbitrarily small constant then M is nonsingular with some constant probability c[4].

Theorem 6.3 *Let $0 < p < 1$ and let M be a random $(n \times n)$-matrix over some finite field* GF$[q]$, *where each matrix entry is chosen independently at random and* 0 *is attained with probability $1-p$ and each non-zero field element is attained with probability $p/(q-1)$. Then M is nonsingular with probability at least $\prod_{i=1}^{n}\left(1-\pi^i\right)$, where $\pi = \max\{p/(q-1), 1-p\}$.*

Proof: Assume that the first $i-1$ rows $M_1, \ldots, M_{i-1}$ that have been chosen are linearly independent. We will bound from below the probability p_i that the i^{th} row M_i is independent of the these rows. Then the probability that M is nonsingular is at least $\prod_{i=1}^{n} p_i$.

M_i is independent from the previous rows iff it is not contained in the (vector-)subspace spanned by the first $i-1$ rows. Consider the matrix formed by the rows $M_1, \ldots, M_{i-1}$. Since these rows are linearly independent, by elementary row operations we can transform the matrix into a matrix that contains the $i-1 \times i-1$ identity matrix. Without loss of generality, we may assume that the first $i-1$ columns form the identity matrix. The rows of this matrix generate the same subspace as the rows $M_1, \ldots, M_{i-1}$.

The vectors contained in this subspace can be easily described. The first $i-1$ coordinates can be arbitrary, but the remaining $n-i+1$ coordinates are uniquely determined by the first $i-1$ coordinates. This implies that the probability that the vector M_i is not contained in the subspace generated by the rows $M_1, \ldots, M_{i-1}$ is at least $1 - \pi^{n-i+1}$.

Hence M is nonsingular with probability at least

$$\prod_{i=1}^{n}(1-\pi^{n-i+1}) = \prod_{i=1}^{n}(1-\pi^{i}).$$

$\square$

$\prod_{i=1}^{n}\left(1-\pi^i\right)$ is bounded from below by $\prod_{i=1}^{\infty}\left(1-\pi^i\right)$. If $p < 1$ is some constant the last expression converges to some positive value c. This proves the above stated claim that a random $(n \times n)$ matrix based on some constant p is nonsingular with some constant probability c. Hence the simplest (and main) open problem the results of this paper raise is as follows. Is there a function $p(n)$ that tends to 0 as n goes to infinity and a constant

[4]We like to thank an anonymous referee for pointing this out to us.

$c > 0$ such that the following holds: A random $(n \times n)$-matrix over GF[2], where each matrix entry is 0 with probability $1 - p(n)$ and 1 with probability $p(n)$, is nonsingular with probability at least c?

References

[1] N. Alon, J. H. Spencer, *The probabilistic method*, John Wiley & Sons, Inc., New York, 1992.

[2] B. Bollobás, *Random Graphs*, Academic Press, New York, 1985.

[3] N. J. Calkin, Dependent sets of constant weight vectors in GF[q], *Random Structures and Algorithms*, Vol. 9, No. 1, pp. 49-53, 1996.

[4] W. Feller, *An introduction to probability theory and its applications*, John Wiley & Sons, Inc., New York, 1968.

[5] D. J. Kelly, J. G. Oxley, On random representable matroids, *Studies in Applied Mathematics*, Vol. 71, pp. 181-205, 1984.

[6] V. F. Kolchin, V. I. Khokhlov, A threshold effect for systems of random equations of a special form, *Discrete Mathematics and its Applications*, Vol. 5, No. 5, pp. 425-436, 1995.

[7] J. Kahn, J. Komlós, E. Szemerédi, On the probability that a random ± 1-matrix is singular, *Journal of the American Mathematical Society*, Vol. 8, No. 1, pp. 223-240, 1995.

[8] A. Mukhopadhyay, The probability that the determinant of an $(n \times n)$ matrix over a finite field vanishes, *Discrete Mathematics*, Vol. 51, pp. 311-315, 1984.

[8] R. P. Stanley, *Enumerative Combinatorics*, Wadsworth, 1986.