On the distribution of rank of a random matrix over a finite field

C. Cooper*
School of Mathematical Sciences
University of North London
London N7 8DB, UK

September 12, 2005

Abstract

Let $M = (m_{ij})$ be a random $n \times n$ matrix over *GF(t)* in which each matrix entry m_{ij} is independently and identically distributed, with $\Pr(m_{ij} = 0) = 1 - p(n)$ and $\Pr(m_{ij} = r) = p(n)/(t-1)$, $r \neq 0$. If we choose $t \geq 3$, and condition on M having no zero rows or columns, then the probability that M is non-singular tends to $c_t \sim \prod_{j=1}^{\infty}(1 - t^{-j})$ provided $p \geq (\log n + d)/n$, where $d \to -\infty$ slowly.

1 Introduction

For convenience denote the elements of the finite field *GF(t)* by $0, 1, ..., t-1$. We consider a space of random $(m \times n)$-matrices over *GF(t)* which we denote by $\mathbf{M}(m, n, p; t)$. Let $M = (m_{ij})$ be a $(m \times n)$-matrix with entries in *GF(t)*, independently and identically distributed as:

$$\Pr(m_{ij} = r) = \begin{cases} 1 - p, & r = 0 \\ \dfrac{p}{t-1}, & r \in \{1, 2, ..., t-1\} \end{cases} \tag{1}$$

The simplest case is where $p = (t-1)/t$ and thus all matrices are equiprobable. Let $m = n$. If the first l columns of the matrix M are linearly independent, they span a

*Research supported by the STORM Research Group

vector space of dimension l and size t^l. The probability that the next column avoids this space is $\left(1 - t^l/t^n\right)$, and thus

$$Pr(M \text{ is non-singular }) = \prod_{l=1}^{n} \left(1 - \frac{1}{t^l}\right). \tag{2}$$

In the paper, *The Rank of Sparse Random Matrices Over Finite Fields*, J. Blömer, R. Karp and E. Welzl [BKW], posed a question on the existence of a threshold $p(n)$ for random $(n \times n)$-matrices over *GF(2)* to be linearly independent with constant probability c. Motivated by this paper, Cooper [CC] proved that we can choose $c = 0.28879$. This value of c is the limiting value of (2) when $t = 2$. This result holds provided $p(n)$ does not tend to either zero or one too rapidly. Specifically, let $p_0 = (\log n + d(n))/n$ where $d(n) \to \infty$ arbitrarily slowly. We require $p_0 \leq p \leq 1 - p_0$. The result is also true for $d(n) \geq -(\log\log n)$, conditional on no zero rows or columns and at most one *unity* (all 1's) row or column in the matrix.

For finite m, n the number $\eta(m, n, k, t)$ of $(m \times n)$-matrices of rank $n - k$ is given by a standard formula (13). Thus the probability of rank $n - k$ in the equiprobable model is $\eta(m, n, k, t)/t^{nm}$. The general asymptotics for $m = n - s$, s constant, in the equiprobable model, are obtained by the method of (14),(17) in Section 5 or by a recurrence argument [KLS],[Ko]. They are given by the following theorem.

Theorem 1 *Let $M \in \mathbf{M}(n - s, n, (t-1)/t; t)$. Let $p_n(k, t)$ be the probability that rank$(M) = n - s - k$, then*

$$\lim_{n\to\infty} p_n(k,t) = \pi_s(k,t) = \begin{cases} \prod_{j=s+1}^{\infty}\left(1 - \left(\frac{1}{t}\right)^j\right) & k = 0 \\ \dfrac{\prod_{j=s+k+1}^{\infty}\left(1-\left(\frac{1}{t}\right)^j\right)}{\prod_{j=1}^{k}\left(1-\left(\frac{1}{t}\right)^j\right)}\left(\frac{1}{t}\right)^{k(s+k)} & k \geq 1 \end{cases} \tag{3}$$

It is difficult to do justice to, or even to determine the full extent of the work on random matrices over finite structures produced by researchers in Russia and the Ukraine. We can point to the work (among others) of G. V. Balakin, V. F. Kolchin, I. N. Kovalenko, A. A. Levitskaya , V. I. Masol and M Savchuk. A survey of many results is given in [KL].

A remarkable early result of I. N. Kovalenko [K1] shows that the asymptotic distribution of rank of random matrices in $\mathbf{M}(n - s, n, p; 2)$ is invariant for constant p. That is, given $\delta > 0$, (3) holds for $\delta \leq p \leq 1 - \delta$.

Another noteable early result was that of Balakin [B], who studied random $(N \times n)$-matrices A over *GF(2)*, where $N/n = a + O(1/n)$ and $0 < a < 1$. Balakin proved that

if $p = (\log n + d)/n$, then

$$\Pr(\text{ Rank of } A \text{ is } N - k) \sim \frac{(ae^{-d})^k}{k!} e^{-ae^{-d}}.$$

See also Kolchin [Ko] for a full discussion of this case.

Many of the asymptotic results concerning the rank of random matrices $\mathbf{M}$ are given in the book *Selected Problems in Probabilistic Combinatorics* [KLS] by Kovalenko, Levitskya and Savchuk. For example, for *GF(2)* the invariant distribution of Theorem 1 holds for a generalization of $\mathbf{M}(m, n, p; 2)$ to the case where the elements of M although independent, are not identically distributed, but rather, $\Pr(m_{ij} = 0) = 1 - p_{ij}$ and it is only required that $\frac{\log(\omega_n n)}{n} \leq p_{ij} \leq 1 - \frac{\log(\omega_n n)}{n}$, where $\omega_n \to \infty$. This result also extends to *GF(t)*. The authors also prove results on random matrices, for the case where the matrix entries come from an *arbitrary finite ring*.

Theorem 2 summarizes results for *GF(t)*, for the case of a random $((n-s) \times n)$-matrix, where $(n - s)/n \to 1$. As we have pointed out above, many of these are established results. The novel results, proved in this paper are (in (i)) the sharp threshold ($d(n)$ constant), and (in (ii)) for $d(n)$ constant or tending slowly to $-\infty$.

Theorem 2 *Let GF(t) be a finite field, $t \geq 3$ and $t = O(\log \log n)$. Let s be a nonnegative integer, $M \in \mathbf{M}((n-s), n, p; t)$ be a $(n - s \times n)$-matrix with entries independently and identically distributed according to (1). Let $c_t = \pi_s(0, t)$. Let $p = (\log n + d(n))/n$ where $d(n) \geq -\log(\log n/9t)$.*

(i)

$$\lim_{n\to\infty} \Pr(M \textit{ is non-singular }) = \begin{cases} 0 & d(n) \to -\infty \\ c_t e^{-2e^{-d}} & d \textit{ constant} \\ c_t & d(n) \to \infty \end{cases}$$

(ii) *Let $\mathcal{C}$ be the event that there are no zero rows or columns in M. For any finite non-negative integer k,*

$$\lim_{n\to\infty} \Pr(M \textit{ has rank } n - s - k \mid \mathcal{C}) = \pi_s(k, t),$$

and in particular

$$\lim_{n\to\infty} \Pr(M \textit{ is non-singular} \mid \mathcal{C}) = c_t.$$

If $s \to \infty$ the matrix M has rank $n - s$ **whp**[1] provided the condition $\mathcal{C}$ or the condition $d(n) \to \infty$ of Theorem 2 hold. This follows from Corollary 4 of Section 2.

[1] **whp.** with high probability. With probability tending to 1 as $n \to \infty$

If we condition on the event $\mathcal{C}$ of the matrix having no zero rows or columns, then the results of Theorem 2 can be shown to hold down to $p_L \sim (\frac{1}{2}\log n + \log\log n)/n$. Below p_L two or more columns with a single non-zero entry in the same row may occur. We do not persue the case $p \to 0$ here for limitations of space, see rather [CC1].

A major obstacle to proofs in this field has been the fact that the moments of the number of solutions of the associated system of homogeneous linear equations ($A\boldsymbol{x} = \mathbf{0}$) do not satisfy the Carlemann condition for unique reconstruction of the probability distribution. However, it was pointed out by a referee, that very recently, Alekseychuk [A1,A2], has proved that the distribution of rank (3) is uniquely determined by the aforementioned moments. This is indeed an interesting development, and should lead to an alternative proof of Theorem 2.

1.1 Basic definitions

The definitions and calculations of the type made in Sections 1,2 are common throughout the papers on this subject. However, the details vary and we repeat them here in order to give a full, as opposed to an indicative proof.

For simplicity we restrict our initial discussion to $(n\times n)$-matrices. Let $M \in \mathbf{M}(n,n,p;t)$. Let $D = (\boldsymbol{a}_1, ..., \boldsymbol{a}_m)$ be a matrix consisting of m columns of M and let $\boldsymbol{c} = (c_1, ..., c_m)$ a sequence of non-zero values from *GF(t)*. The matrix M is singular if and only if there exist $\boldsymbol{c}$ and D such that

$$c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_m\boldsymbol{a}_m = \mathbf{0}_n \qquad c_i \neq 0,\ i = 1, ..., m. \tag{4}$$

Because *GF(t)* is a field, for $j \neq 0$ and according to (1)

$$Pr(a_i j = k) = Pr(a_i = kj^{-1}) = Pr(a_i = k).$$

By a simple induction, for *fixed* non-zero $c_i,\ i = 1, ..., m$ the event given in (4) has the same probability as the *zero sum* event $\boldsymbol{a}_1 + \cdots + \boldsymbol{a}_m = 0$.

For $r \in$ *GF(t)*, the probability $\rho_m(r)$ that row j of D has sum $a_{j1} + \cdots + a_{jm} = r$ is

$$\rho_m(r) = \begin{cases} \frac{1}{t}\left(1 + (t-1)(1 - \frac{t}{t-1}p)^m\right) & r = 0 \\ \\ \frac{1}{t}\left(1 + (-1)(1 - \frac{t}{t-1}p)^m\right) & r \neq 0 \end{cases} \tag{5}$$

This result is derived from the recurrence relations

$$\rho_m(r) = \rho_{m-1}(r)(1-p) + \sum_{s\neq r} \frac{p}{t-1}\rho_{m-1}(s) \qquad (r, s \in GF(t)),$$

subject to the initial conditions given by (1).

Let $W_m(M)$ be the number of linearly dependent m-subsets of columns of M, then

$$\mathbf{E}W_m = \binom{n}{m}(t-1)^m \left(\rho_m(0)\right)^n.$$

For $r \in GF(t)$ let $N(r)$ be the set of indices i of $\boldsymbol{c}$ for which $c_i = r$, and let $|N(r)| = n_r$. The event (4) can be expressed as

$$\sum_{r=1,\ldots,t-1} \sum_{i \in N(r)} r\boldsymbol{a}_i = \mathbf{0}.$$

A solution $\boldsymbol{c}$ of the form given in (4), which we write as $D\boldsymbol{c} = \mathbf{0}_n$, extends naturally to a unique vector $\boldsymbol{y} \in (GF(t))^n$ satisfying $M\boldsymbol{y} = \mathbf{0}_n$. We simply put $y_i = 0$ if i does not index a column of the submatrix D of M and $y_i = c_j$ if $\boldsymbol{a}_j$ is column i of M. The expected number of such vectors $\boldsymbol{y}$ with partition $(n_0, n_1, ..., n_{t-1})$ is

$$\binom{n}{n_0}\binom{n-n_0}{n_1, ..., n_{t-1}} \left(\rho_{n-n_0}(0)\right)^n. \tag{6}$$

Let M be an $((n-s) \times n)$-matrix of rank $n-r$. Let $\mathcal{N} = \{\boldsymbol{x} : M\boldsymbol{x} = \mathbf{0}\}$ be the null space of M. We will refer to $\mathcal{N}$ as the row null space, as any $\boldsymbol{x} \in \mathcal{N}$ maps the rows of M to zero. By the matrix rank and nullity theorem (eg. [Ha] Chapter 5) $\text{Rank}(M) + \text{Dimension}(\mathcal{N}(M)) = n$. Similarly, the dimension of the column null space $\{\boldsymbol{y} : \boldsymbol{y}M = \mathbf{0}\}$ is $k = r - s$.

Let $\mathcal{C}$ be the subset of $\mathbf{M} = \mathbf{M}(n-s, n, p; t)$ consisting of those matrices with no zero rows or columns. Let $C \in \mathcal{C}$. To prove Theorem 2, we obtain the distribution of dimension of the row null space $\mathcal{Y}(C)$ of C. For lack of a better method, we are obliged to use a rather indirect approach.

We write $C = \begin{pmatrix} A \\ B \end{pmatrix}$ where A is an $(n-l) \times n$ matrix and $B = (\boldsymbol{b}_1 \cdots \boldsymbol{b}_{l-s})'$ is an $(l-s) \times n$ matrix. We will choose $l = \log\log n$.

The layout of the proof of Theorem 2 in this paper is as follows.

(i) In Section 2 we prove the matrix A is non-singular **whp.**

(ii) In Sections 2.3 and 3 we establish the relevant structure of $\mathcal{X}(A)$, the null space of the rows of A.

(iii) In Section 4 we calculate $\mathbf{E}(W)_k$, the expected number of linearly independent k-subsets of the null space $\mathcal{Y}(C)$ of C. This is obtained as the number of linearly independent k-subsets of $\mathcal{X}(A)$ which also lie within the null space of the rows of B.

(iv) In Section 5 we derive the distribution of the dimension of the row null space $\mathcal{Y}(C)$ of C. To find this distribution we use inclusion-exclusion type counting on $\mathbf{E}(W)_k$ over the lattice of vector subspaces of the null space of C.

It is easier to consider a subset $\mathcal{D}$ of $\mathbf{M}$, with elements C satisfying the condition that A has no zero rows or columns, but B may have zero rows. The probability of those matrices $D \in \mathcal{D} \setminus \mathcal{C}$ such that that B contains a zero row is $o\left(\frac{\log^2 n}{n}\right)$, and the probability of those matrices $C \in \mathcal{C} \setminus \mathcal{D}$ which have a submatrix A with zero columns which extend to non-zero columns of C is $o\left(\frac{\log^3 n}{n}\right)$. Thus $|\mathcal{C}| = (1 + o(1))|\mathcal{D}|$. All subsequent proofs refer to $\mathcal{D}$.

1.2 Joint probability of no zero rows or columns

Let $A \in \mathbf{M}(m, n, p; t)$ where $m = n - l$. We wish to condition on the event $\mathcal{E}$ that A has no zero rows or columns. We show that the probability of this event is given by

$$\Pr(\text{ No zero rows or columns in } A) \sim e^{-2e^{-d}}. \tag{7}$$

The number of zero rows is binomial $B(m, (1-p)^n)$, and thus

$$\Pr(\text{ No zero rows }) = (1 - (1-p)^n)^m \sim e^{-e^{-d}}.$$

If X is the number of zero columns, then for constant k

$$\begin{aligned} \mathbf{E}((X)_k \mid \text{ No zero rows }) &= \frac{(n)_k \left((1-p)^k(1-(1-p)^{n-k})\right)^m}{(1-(1-p)^n)^m} \\ &= (n)_k(1-p)^{nk}\left(1 + O(kpe^{-d})\right). \end{aligned}$$

Thus if $np = \log n + d$ where $d = o(\log\log n)$, then

$$\begin{aligned} \Pr(\text{ No zero columns } \mid \text{ No zero rows }) &= (1-(1-p)^n)^n \left(1 + O\left(\frac{\log^2 n}{n}\right)\right) \\ &= e^{-e^{-d}}\left(1 + O\left(\frac{\log^3 n}{n}\right)\right). \end{aligned}$$

Thus provided we can prove Theorem 2(ii), then for d constant, Theorem 2(i) follows.

2 Linear dependencies in the matrix A

Definition 3 *Let* $\mathcal{X}(A) = \{\boldsymbol{x} : A\boldsymbol{x} = \mathbf{0}\}$ *be the row null space of* A. *Let* $\boldsymbol{x} = (x_1, ..., x_n)$ *and let* n_i, $i = 0, 1, ..., t-1$ *be the number of entries* x_j, $j = 1...n$ *having value* i. *If for all* $\boldsymbol{x} \in \mathcal{X} \setminus \mathbf{0}$ *and for all* $i = 0, 1, ..., t-1$ *we have*

$$\frac{n}{t}\left(1 - 4\sqrt{\frac{t\log n}{n}}\right) \leq n_i \leq \frac{n}{t}\left(1 + 4\sqrt{\frac{t\log n}{n}}\right)$$

we will say the non-zero elements of $\mathcal{X}$ *are* nearly uniform *in the elements of GF(t).*

In this section we prove the following theorem.

Theorem 4 *Let* $0 \leq l \leq \log\log n$. *Let* $\mathcal{E}$ *be the subspace of* $\mathbf{M}(n-l, n, p; t)$ *consisting of those matrices* A *with no zero rows or columns.*

Let $p = (\log n + d)/n$ *where* $d \geq -\log(\log n/9t)$. *Let* $m_2 = \frac{t-1}{t}n\left(1 - 4\sqrt{\frac{\log n}{n}}\right)$ *and let* $m_3 = \frac{t-1}{t}n\left(1 + 4\sqrt{\frac{\log n}{n}}\right)$. *Let* D *be a linearly dependent subset of the rows or columns of* A, *and let* $|D| = m$.

The following properties hold **whp.** *in* $\mathcal{E}$.

(i) There are no linear dependencies in A *of size outside the range* $m_2 < m < m_3$.

(ii) The expected number of linear dependencies of size $m_2 < m < m_3$ *among the rows of* A *is* $t^{-l}(1 + o(1))$ *and among the columns of* A *is* $t^l(1 + o(1))$.

(iii) The non-zero elements of $\mathcal{X}$ *are nearly uniform in the elements of GF(t).*

Thus we have the following corollary.

Corollary 5 *Let* $l \to \infty$, *then conditional on* $\mathcal{E}$, **whp.**

(i) The $((n-l) \times n)$*-matrix* A *is of rank* $n - l$.

(ii) The dimension of $\mathcal{X}(A)$ *is* l.

2.1 Expected number of linear dependencies of the matrix A

The calculations we make here are for rows. Similar calculations hold for columns.

Let $\rho_m(0) = \rho_m$, as given by (5). The probability a subset $D = (\boldsymbol{a}_1, ..., \boldsymbol{a}_m)$ of the rows of A satisfies $\boldsymbol{a}_1 + \cdots + \boldsymbol{a}_m = 0$ is ρ_m^n. The number, W_m, of linearly dependent m-subsets has expectation

$$\mathbf{E}W_m = \binom{n-l}{m}(t-1)^m \rho_m^n.$$

The main contribution to $\mathbf{E}W$ is from $|D| \sim (t-1)n/t$. When d is constant or $d \to -\infty$ linearly dependent sets of constant size are possible. However, for most values of m and d, the results of (eg) [CC] apply directly. We state these results in the lemma below.

Lemma 6 (CC) *Let the field be GF(t), where $t = o(\sqrt{\log n})$. Let $p = c/n$ where $c = \log n + d(n)$ and $d(n) > -(\log\log n)$*

(i) With high probability no linearly dependent set, D, of columns of M has $\log n \leq |D| \leq m_2 = n\frac{t-1}{t}\left(1 - 4\sqrt{\frac{\log n}{n}}\right)$ or $|A| \geq m_3 = n\frac{t-1}{t}\left(1 + 4\sqrt{\frac{\log n}{n}}\right)$

(ii) If $d(n) = \omega \to \infty$ then with high probability there are no linearly dependent sets of size $1 \leq |D| \leq \log n$.

Let $\mathbf{E}W_m^*$ denote the expected number of linearly dependent subsets conditional on the event $\mathcal{E}$ of no zero rows or columns. From (7),

$$\mathbf{E}W_m^* \leq 2\mathbf{E}W_m \times e^{2e^{-d}} = \mathbf{E}W_m O(n^{2/9t}).$$

Case of $1 \leq m \leq \log n$. Consider the column $(a_{k1}, ..., a_{km})$ of D. Suppose exactly j entries are non-zero. Let $P(j)$ be the conditional probability that the sum of these entries is zero, then $P(1) = 0$ and

$$P(j) = \frac{1}{t-1}(1 - P(j-1)), \qquad j \geq 2.$$

This has the solution

$$P(j) = \frac{1}{t-1}\left(1 - \frac{1}{t-1} + \cdots + \frac{(-1)^{j-2}}{(t-1)^{j-2}}\right).$$

Thus, we can write $\rho_m = \rho_m(0)$ as

$$\begin{aligned}\rho_m &= (1-p)^m + \binom{m}{2}p^2(1-p)^{m-2}P(2) + \cdots + \binom{m}{j}p^j(1-p)^{m-j}P(j) + \cdots \\ &= (1-p)^m + \binom{m}{2}\frac{p^2}{t-1}(1-p)^{m-2}(1+O(mp)).\end{aligned}$$

For $m \geq 2$ let f_m denote the probability that D is zero-sum and has no zero rows,

$$\begin{aligned}f_m &= (\rho_m)^n - \binom{m}{1}(1-p)^n f_{m-1} - \binom{m}{2}(1-p)^{2n} f_{m-2} - \cdots - (1-p)^{mn} \\ &\leq (1-p)^{mn}\left(\frac{\rho_m^n}{(1-p)^{mn}} - 1\right) \\ &= (1-p)^{mn}\left(n\binom{m}{2}\frac{p^2}{t-1}(1+O(mp))\right) \\ &\leq \binom{m}{2}\frac{e^{-md}}{n^m}\frac{(\log n + d)^2}{n}.\end{aligned}$$

The expected number of linearly dependent column subsets containing no zero rows is

$$\sum_{m=2}^{\log n}\binom{n-l}{m}(t-1)^m f_m \leq t^2\frac{(\log n + d)^2}{n}e^{-2d+(t-1)e^{-d}}.$$

Thus the conditional expectation is at most

$$\sum_{m=2}^{\log n}\mathbf{E}W_m^* = o(n^{-7/9}).$$

Case of $m_2 = n\frac{t-1}{t}\left(1 - 4\sqrt{\frac{\log n}{n}}\right) \leq m \leq m_3 = n\frac{t-1}{t}\left(1 + 4\sqrt{\frac{\log n}{n}}\right)$.

Let $X = \sum_{i=1}^{n-l} X_i$ where X_i is an indicator for the event that row $\boldsymbol{a}_i$ of A is zero, that D is linearly dependent and that A contains no zero columns. Let $\mathbf{E}(X)_s$ denote the s-factorial moment of X.

$$\begin{aligned}\frac{\mathbf{E}(X)_s}{s!} &= \sum_{j=0}^{s}\binom{n-l-m}{s-j}\binom{m}{j}(1-p)^{ns} \\ &\times \left[\left(\frac{1}{t}\left(1 + (t-1)(1 - \frac{t}{t-1}p)^{m-j}\right)\right) - (1-p)^{n-l-s}\right]^n \\ &= \frac{e^{-sd}}{s!}\frac{1}{t^n}e^{-e^{-d}}\left(1 + O\left(\frac{\log^{3/2} n}{\sqrt{n}}\right)\right).\end{aligned}$$

Thus, we can use standard inclusion-exclusion followed by (7) to deduce

$$Pr(D \text{ is linearly dependent } \mid \text{no zero rows or columns}) \sim \frac{1}{t^n}.$$

and

$$\begin{aligned}\sum_{m_2}^{m_3} \mathbf{E}W_m^* &= (1+o(1)) \sum_{m=m_2}^{m_3} \binom{n-l}{m} \frac{(t-1)^m}{t^n} \\ &= (1+o(1)) \times \frac{1}{t^l}.\end{aligned}$$

We note that a similar calculation for the columns of A gives $\sum_{m_2}^{m_3} \mathbf{E}W_m^* = t^l(1+o(1))$.

2.2 The structure of solutions of $A\boldsymbol{x} = \mathbf{0}$

Let $A\boldsymbol{x} = \mathbf{0}$, and let $n_i = |\{j : x_j = i, j = 1..n\}|$, be the number of entries in $\boldsymbol{x}$ with value i. We prove that **whp.** all values $n_i,\ i = 0, 1, ..., t-1$ are concentrated within $O(\sqrt{n \log n})$ of the expected number n/t.

We know that **whp.** any dependencies among the columns of A are of size $m_2 \le m \le m_3$. Applying (6), the expected number of vectors $\boldsymbol{x}$ satisfying $A\boldsymbol{x} = \mathbf{0}$ with partition $(n_0, n_1, ..., n_{t-1})$ is for any $A \in \mathbf{M}$

$$\begin{aligned}\binom{n}{m}\binom{m}{n_1, ..., n_{t-1}} & \left(\frac{1}{t}\left(1 + (t-1)\left(1 - \frac{t}{t-1}p\right)^m\right)\right)^{n-l} \\ &= O(1)e^{(t-1)e^{-d}} t^l \binom{n}{m} \frac{(t-1)^m}{t^n} \\ &\times \binom{m}{n_1, ..., n_{t-1}} \left(\frac{1}{t-1}\right)^{n_1} \cdots \left(\frac{1}{t-1}\right)^{n_{t-1}}.\end{aligned}$$

The variables n_i of a multinomial distribution on m objects in $t-1$ classes with probabilities $1/(t-1)$ are sharply concentrated around $m/(t-1)$. The probability we see a deviation of at least $\frac{m}{t-1}(1 \pm \epsilon)$ where $\epsilon = 4\sqrt{\frac{t \log n}{n}}$ in any variable n_i is $o(1/n^2)$ by the Hoeffding inequality.

From Corollary 4, $|\mathcal{X}| \sim t^l$, and $l \le \log\log n$. Thus the conditional expectation of partitions not satisfying the near-uniformity conditions of Theorem 4(iii) is bounded by

$$t^l e^{(t-1)e^{-d}}(e^{2e^{-d}})(t^{l+1})/n^2 = o(1/n).$$

3 Properties of the null space $\mathcal{X}$ of the rows of A

The fact that all elements of $\mathcal{X} \setminus \mathbf{0}$ have about n/t entries of each r in $GF(t)$, combines with the vector space structure of $\mathcal{X}$ to induce a structure on the linearly independent k-subsets of $\mathcal{X}$. We now describe a partition approach introduced in [KLS].

Denote by $V(k) = \{\boldsymbol{u}_i : i = 1, ..., t^k\}$ the space of k-vectors over *GF(t)*. Let $\boldsymbol{z}_i,\ i = 1, ..., k$ be arbitrary n-vectors and let $\boldsymbol{y}$ be the $k \times n$ matrix,

$$\boldsymbol{y} = \begin{pmatrix} \boldsymbol{z}_1 \\ \vdots \\ \boldsymbol{z}_k \end{pmatrix} = \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ \vdots & & & \vdots \\ z_{k1} & z_{k2} & \cdots & z_{kn} \end{pmatrix} = (\,\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n\,).$$

Each column of $\boldsymbol{y}$ is an element of $V(k)$, so we can partition the columns of $\boldsymbol{y}$ in terms of the elements $\boldsymbol{u}$ of $V(k)$. This also partitions $[n]$ by

$$S(\boldsymbol{u}) = \{j \in [n] : \begin{pmatrix} z_{1j} \\ \vdots \\ z_{kj} \end{pmatrix} = \boldsymbol{u}\}.$$

Theorem 7 *Let $l \leq \log\log n / \log t$. Let the non-zero elements of $\mathcal{X}$ be nearly uniform in the elements of GF(t).*

The following property holds for all linearly independent subsets $\{\boldsymbol{z}_1, ..., \boldsymbol{z}_k\}$ of $\mathcal{X}$, for all $\boldsymbol{u} \in V(k)$ and for all $k = 1, 2, .., l$.

Let $\boldsymbol{y}$ be the $(k \times n)$-matrix $\boldsymbol{y} = (\boldsymbol{z}_1, ..., \boldsymbol{z}_k)'$. The number $|S(\boldsymbol{u})|$ of occurrences of $\boldsymbol{u}$ in the columns of $\boldsymbol{y}$ satisfies $|S(\boldsymbol{u})| = n/t^k \left(1 + O\left(\sqrt{\frac{\log n}{nt}}\right)\right)$.

Proof Let $J = V(k) \setminus \mathbf{0}$, and let $\boldsymbol{a} \in J,\ \boldsymbol{a} = (a_1, ..., a_k)$. If $\boldsymbol{z}_1, ..., \boldsymbol{z}_k \in \mathcal{X}$ are linearly independent, then $\boldsymbol{ay} = a_1\boldsymbol{z}_1 + \cdots + a_k\boldsymbol{z}_k \in \mathcal{X} \setminus \mathbf{0}$. Let $N(s)$ be the set of indices $j \in [n]$ which satisfy $\boldsymbol{a} \cdot \boldsymbol{y}_j = a_1 z_{1j} + \cdots + a_k z_{kj} = s$. By the near-uniform property of Definition 3, $N(s) = n/t(1 + O(\sqrt{t \log n/n}))$.

For $\boldsymbol{w} \in V(k)$, let $T = \{\boldsymbol{a} \in V(k) : \boldsymbol{a} \cdot \boldsymbol{w} = 0\}$, then T is a subgroup of $(V(k), +)$. If $\boldsymbol{w} \neq \mathbf{0}$ then $|T| = t^{k-1}$ as T has exactly t cosets, for,

$$\boldsymbol{a} \cdot \boldsymbol{w} = j \text{ and } \boldsymbol{b} \cdot \boldsymbol{w} = j \Longrightarrow (\boldsymbol{a} - \boldsymbol{b}) \cdot \boldsymbol{w} = 0.$$

For fixed $\boldsymbol{u}, \boldsymbol{v},\ \boldsymbol{u} \neq \boldsymbol{v}$, how many times λ does $\boldsymbol{a} \cdot \boldsymbol{u} = \boldsymbol{a} \cdot \boldsymbol{v},\ \boldsymbol{a} \in J$?

$$\begin{aligned} \{\boldsymbol{a} \in J : \boldsymbol{a} \cdot \boldsymbol{u} = \boldsymbol{a} \cdot \boldsymbol{v}\} &= \{\boldsymbol{a} \in V : \boldsymbol{a} \cdot (\boldsymbol{u} - \boldsymbol{v}) = 0\} \cap J \\ &\Longrightarrow \lambda = |T| - 1 = t^{k-1} - 1. \end{aligned}$$

We consider a table with rows $\boldsymbol{a} \in J$, columns $i \in [n]$ and entries $\boldsymbol{a} \cdot \boldsymbol{y}_i = s$. Let

$$\eta(\boldsymbol{u}) = \sum_{\boldsymbol{a} \in J} |\{i \in [n] : \boldsymbol{a} \cdot \boldsymbol{y}_i = \boldsymbol{a} \cdot \boldsymbol{u}\}|,$$

then

$$\eta(\boldsymbol{u}) = (n - |S(\boldsymbol{u})|)(t^{k-1} - 1) + |S(\boldsymbol{u})|(t^k - 1).$$

Any columns i of the table which are in $S(\boldsymbol{u})$ are counted $|J| = t^k - 1$ times. Any column $j \notin S(\boldsymbol{u})$ is in $S(\boldsymbol{v})$ for some $\boldsymbol{v}$ and coincides with $\boldsymbol{u}$ on $\lambda = t^{k-1} - 1$ occasions. In row $\boldsymbol{a}$ of the table where $\boldsymbol{a} \cdot \boldsymbol{u} = s$ say, the contribution to $\eta(\boldsymbol{u})$ is $n/t(1 + O(\sqrt{t \log n/n}))$ so that $|S(\boldsymbol{u})| = n/t^k \left(1 + O\left(\sqrt{\frac{\log n}{nt}}\right)\right)$ as required. □

4 Estimating the moments of the null space of C

We will first consider the $(n \times n)$-matrix $C = \begin{pmatrix} A \\ B \end{pmatrix}$, $C \in \mathcal{D}$ where $\mathcal{D}$ is defined in Section 1.1. The matrix A has null space $\mathcal{X}$ and the matrix B is a random $(l \times n)$-matrix. Let $\mathcal{Y} = \{\boldsymbol{x} : C\boldsymbol{x} = \boldsymbol{0}\}$. Let $(W)_k$ be the number of linearly independent k-tuples in $\mathcal{Y}$. Now,

$$\begin{aligned} C\boldsymbol{x} = \boldsymbol{0} &\iff A\boldsymbol{x} = \boldsymbol{0} \text{ and } B\boldsymbol{x} = \boldsymbol{0} \\ &\iff \boldsymbol{x} \in \mathcal{X} \text{ and } B\boldsymbol{x} = \boldsymbol{0} \\ &\iff (\boldsymbol{b}_1\boldsymbol{x} = \boldsymbol{0}) \wedge (\boldsymbol{b}_2\boldsymbol{x} = \boldsymbol{0}) \wedge \cdots \wedge (\boldsymbol{b}_l\boldsymbol{x} = \boldsymbol{0}). \end{aligned}$$

We consider k-tuples $\boldsymbol{y} = (\boldsymbol{z}_1, ..., \boldsymbol{z}_k)$ of linearly independent vectors from $\mathcal{X}$ such that

$$B\boldsymbol{z}_1 = ... = B\boldsymbol{z}_k = \boldsymbol{0}_l. \tag{8}$$

If we write $B = (\,\boldsymbol{b}_1, ..., \boldsymbol{b}_l\,)'$ then (8) is true iff $\boldsymbol{b}_i\boldsymbol{z}_j = \boldsymbol{0}$ for all $i = 1, ..., l;\ j = 1, ..., k$.

Thus $(W)_k$ is the number of linearly independent k-tuples in $\mathcal{X}$ such that (8) holds.

Theorem 8 *Let $\mathcal{D} \subseteq \mathbf{M}(n, n, t; p)$ and $k \leq \log(\log n/3 \log\log n)/\log t$, then $\mathbf{E}(W)_k \sim 1$.*

Proof Let $\boldsymbol{b} = (\beta_1, ...\beta_n)$ be a fixed row of B and let $\boldsymbol{z}_i \in \mathcal{X},\ i = 1..k$ be linearly independent. Let the $(n \times k)$-matrix $\boldsymbol{y} = (\boldsymbol{z}_1, ..., \boldsymbol{z}_k)$ be written as $\boldsymbol{y} = (\boldsymbol{y}_1, ..., \boldsymbol{y}_n)$. We partition the columns of $\boldsymbol{y}$ according to the vectors of $V(k) = (GF(t))^k$ which we

write as $V(k) = \{\boldsymbol{u}_i : i = 1, ..., t^k\}$. Let $m = t^k - 1$. For convenience we assume that $\boldsymbol{u}_{m+1} = \mathbf{0}_k$.

$$\begin{aligned} \boldsymbol{by} = \mathbf{0}_k &\iff \beta_1 \boldsymbol{y}_1 + \cdots + \beta_n \boldsymbol{y}_n = \mathbf{0} \\ &\iff x_1 \boldsymbol{u}_1 + \cdots + x_{m+1} \boldsymbol{u}_{m+1} = \mathbf{0} \\ &\iff x_1 \boldsymbol{u}_1 + \cdots + x_m \boldsymbol{u}_m = \mathbf{0}. \end{aligned} \tag{9}$$

Here $x_i = \sum_{j \in S(\boldsymbol{u}_i)} \beta_j$ and $S(\boldsymbol{u}_i) = \{j \in [n] : \boldsymbol{y}_j = \boldsymbol{u}_i\}$. By Theorem 4 we know that $|S(\boldsymbol{u}_i)| \sim n/t^k$.

Let $G = (\{(x_1, ..., x_m)\}, +)$ be the finite Abelian group of addition of m-vectors with entries in *GF(t)*. Thus $|G| = t^m$. Let the solutions of (9) be

$$T = \{(x_1, ..., x_m) \in G : x_1 \boldsymbol{u}_1 + \cdots + x_m \boldsymbol{u}_m = \mathbf{0}_k\}$$

then T is a subgroup of G. Let $\boldsymbol{c} = (c_1, \cdots, c_k)'$. The cosets of T in G are the sets

$$H(\boldsymbol{c}) = \{(y_1, ..., y_m) : y_1 \boldsymbol{u}_1 + \cdots + y_m \boldsymbol{u}_m = \boldsymbol{c}\}.$$

Thus there are $|\{\boldsymbol{c}\}| = t^k$ cosets and

$$|T| = \frac{t^m}{t^k} = t^{t^k - k - 1}.$$

From (5)

$$\begin{aligned} \pi(\boldsymbol{y}) &= \Pr(\ \boldsymbol{by} = \mathbf{0}\ ) \\ &= \sum_{(x_1,...,x_m) \in T} \prod_{j=1}^{m} \frac{1}{t} \left(1 + \lambda(x_j)(1 - \frac{t}{t-1} p)^{|S(\boldsymbol{u}_j)|}\right) \\ &= \frac{|T|}{t^m} \exp\left(\alpha \exp - \left[\frac{t}{t-1} \frac{n}{t^k} p(1 + o(1))\right]\right) \end{aligned}$$

where $\lambda(x_j) = [(t-1)1_{\{x_j = 0\}} + (-1)1_{\{x_j \neq 0\}}]$ and $(-1) \leq \alpha \leq (t-1)$.

The set $\Omega = \{\boldsymbol{y}\}$ of ordered k-tuples of linearly independent vectors in $\mathcal{X}$ has size

$$|\Omega| = \nu(k, l) = (t^l - 1)(t^l - t) \cdots (t^l - t^{k-1}).$$

Thus

$$\begin{aligned} \mathbf{E}(W)_k &= \sum_{\boldsymbol{y} \in \Omega} (\pi(\boldsymbol{y}))^l \qquad (10) \\ &= \nu(k, l) \frac{1}{t^{kl}} \exp\left(l\alpha \left(\frac{e^{-d}}{n}\right)^{\frac{(1+o(1))}{(t-1)t^{k-1}}}\right) \\ &= \exp\left\{+O\left(t^{k-l}\right) + O\left(lt \left(\frac{\log n}{n}\right)^{\frac{1}{t^k}}\right)\right\} \\ &= 1 + o\left(\frac{1}{\log n}\right). \qquad (11) \end{aligned}$$

□

Corollary 9 *Let* $\mathcal{D} \subseteq \mathbf{M}(n-s, n, t; p)$ *and let* $k \leq \log(\log n/3 \log\log n)/\log t$, *then* $\mathbf{E}(W)_k \sim t^{sk}$.

Proof As B is now an $((l-s) \times n)$-matrix, in (10) we have

$$\begin{aligned} \mathbf{E}(W)_k &= \sum_{\boldsymbol{y} \in \Omega} (\pi(\boldsymbol{y}))^{l-s} \\ &= t^{sk}(1 + o(1/\log n)). \end{aligned}$$

□

5 Limiting probability distribution of matrix rank

The initial discussion concerns the distribution $(\pi_s(k,t),\ k \geq 0)$ given in (3). The t-nomial theorem (see [vLW] (p291)) states that, for $r \geq 1$,

$$(1+x)(1+tx)\cdots(1+t^{r-1}x) = \sum_{k=0}^{r} \left[\begin{array}{c} r \\ k \end{array} \right]_t t^{\binom{k}{2}} x^k, \tag{12}$$

where the Gaussian coefficients are defined, for $t > 0$ by $\left[\begin{array}{c} r \\ 0 \end{array} \right]_t = 1$ and

$$\left[\begin{array}{c} r \\ k \end{array} \right]_t = \frac{(t^r-1)(t^{r-1}-1)\cdots(t^{r-k+1}-1)}{(t^k-1)(t^{k-1}-1)\cdots(t-1)}.$$

The number of $(m \times n)$-matrices over *GF(t)* with rank $n-r$ is (see [vLW] (p303)),

$$\eta(m,n,r,t) = \left[\begin{array}{c} m \\ r \end{array} \right]_t \sum_{l=0}^{n-r} (-1)^l \left[\begin{array}{c} n-r \\ l \end{array} \right]_t t^{n(n-(r+l))+\binom{l}{2}}. \tag{13}$$

When $p = (t-1)/t$ and all matrices of the space $\mathbf{M}(m,n,p;\ t)$ are equiprobable, we have $Pr(\text{ Rank} = n-r) = \eta(m,n,r,t)/t^{nm}$. It can easily be shown that

$$\pi_0(r,t) = \lim_{n\to\infty} \frac{\eta(n,n,r,t)}{t^{n^2}} = \sum_{l \geq 0} c(r,l), \tag{14}$$

where, using the convention that $\prod_{j=1}^{0}(t^j-1) = 1$, we have defined $c(r,l)$ by

$$c(r,l) = (-1)^l \frac{t^{-\binom{r}{2}}}{\prod_{j=1}^{r}(t^j-1)} \frac{t^{-rl}}{\prod_{j=1}^{l}(t^j-1)} = (-1)^l a(r) b(r,l). \tag{15}$$

If we define

$$\left[\begin{array}{c} \infty \\ k \end{array} \right]_z = \frac{1}{(1-z^k)\cdots(1-z)} \qquad |z|<1, \qquad k \geq 1,$$

then

$$\prod_{k=0}^{\infty}(1+z^k x) = \sum_{k=0}^{\infty} \left[\begin{array}{c} \infty \\ k \end{array} \right]_z z^{\binom{k}{2}} x^k. \tag{16}$$

We note that if $t>1$ then

$$\frac{1}{\prod_{j=1}^{k}(t^j-1)} = \left[\begin{array}{c} \infty \\ k \end{array} \right]_{\left(\frac{1}{t}\right)} \left(\frac{1}{t}\right)^{\binom{k}{2}} \left(\frac{1}{t}\right)^k.$$

Thus from (15), (16) and (3),

$$\begin{aligned} \sum_{l\geq 0} c(r,l)t^{s(r+l)} &= \frac{t^{-\binom{r}{2}}t^{rs}}{\prod_{j=1}^{r}(t^j-1)} \sum_{l\geq 0} \left[\begin{array}{c} \infty \\ l \end{array} \right]_{\left(\frac{1}{t}\right)} \left(\frac{1}{t}\right)^{\binom{l}{2}} \left(\frac{-t^s}{t^{r+1}}\right)^l \qquad (17) \\ &= \frac{t^{-\binom{r}{2}}t^{rs}}{\prod_{j=1}^{r}(t^j-1)} \prod_{l\geq 0}\left(1+\left(\frac{1}{t}\right)^l\left(\frac{-t^s}{t^{r+1}}\right)\right) \\ &= \left\{ \begin{array}{ll} 0 & r<s \\ \pi_s(r-s,t) & r\geq s \end{array} \right. . \end{aligned}$$

We now prove the following lemma which completes the proof of Theorem 2.

Lemma 10 *Let r,s be constant, $r \geq s$ and let $\pi_s(r,t)$ be given by (3). Let $\{C\}$ be a space of random $((n-s)\times n)$-matrices for which $\mathbf{E}(W)_k = t^{sk}(1+o(1))$, for $k \leq k^* = \log(\log n/3\log\log n)/\log t$. Let $\mathcal{Y}(C)$ be the row null space of C, then*

$$\lim_{n\to\infty} Pr\,(\textit{dimension of } \mathcal{Y}(C) = r) = \pi_s(r-s,t).$$

Proof

Let C be a random matrix over *GF(t)* with row null space $\mathcal{Y}(C)$. We note that the dimension of the vector space $\mathcal{Y}$ must be at least s. Let $(\boldsymbol{z}_1,...,\boldsymbol{z}_k)$ be a k-tuple of linearly independent vectors from $\mathcal{Y}$. Let $N_{k,r}$ be the number of linearly independent k-tuples if the dimension $\mathcal{Y}$ is r. Thus $N_{k,r}=0$ if $r<k$, $N_{0,r}=1$ and for $1\leq k\leq r$,

$$N_{k,r} = (t^r-1)(t^r-t)\cdots(t^r-t^{k-1}).$$

If the probability of dimension r is $p(r,t)=p_r$ we can write

$$\mathbf{E}(W)_k = \sum_{r\geq k} N_{k,r}p_r. \tag{18}$$

Thus we have the following system of equations which we wish to solve for p_k,

$$\begin{array}{rcccccccccccc} 1 & = & p_0 & + & p_1 & + & p_2 & + & \cdots & + & p_k & + & \cdots \\ \mathbf{E}W & = & & & N_{1,1}p_1 & + & N_{1,2}p_2 & + & \cdots & + & N_{1,k}p_k & + & \cdots \\ \mathbf{E}(W)_2 & = & & & & & N_{2,2}p_2 & + & \cdots & + & N_{2,k}p_k & + & \cdots \\ \vdots & & & & & & & & \cdots & & \cdots & & \cdots \\ \mathbf{E}(W)_k & = & & & & & & & & & N_{k,k}p_k & + & \cdots \\ \vdots & & & & & & & & & & & & \cdots \end{array} \tag{19}$$

We wish to prove that $p_r = 0$ for $r < s$ and for $r \geq s$, $p_r \to \pi_s(r-s,t)$ as given in (3). We claim that p_r is given by

$$p_r = \sum_{l \geq 0} c(r,l)\mathbf{E}(W)_{r+l}, \tag{20}$$

where $c(r,l)$ is from (15). To see this, substitute for $\mathbf{E}(W)_{r+l}$ from (18) into the sum (20). The coefficient of p_r is $c(r,0)N_{r,r} = 1$. If $j > r$, then the coefficient of p_j is

$$a(r)\left(N_{r,j}b(r,0) - N_{r+1,j}b(r,1) + \cdots + (-1)^l N_{r+l,j}b(r,l) + \cdots + (-1)^{j-r}N_{j,j}b(r,j-r)\right).$$

However,

$$\begin{aligned} b(r,l)N_{r+l,j} &= (t^j-1)\cdots(t^j-t^{r+l-1})\frac{t^{-rl}}{\prod_{i=1}^{l}(t^i-1)} \\ &= (t^j-1)\cdots(t^j-t^{r-1})\begin{bmatrix} j-r \\ l \end{bmatrix}_t t^{\binom{l}{2}}. \end{aligned}$$

Thus the coefficient of p_j is

$$a(r)(t^j-1)\cdots(t^j-t^{r-1})\sum_{l=0}^{j-r}\begin{bmatrix} j-r \\ l \end{bmatrix}_t t^{\binom{l}{2}}(-1)^l,$$

so that for $j > r$, this coefficient is identically zero, from (12), with $x = (-1)$.

As we have only estimated $\mathbf{E}(W)_k$ for $1 \leq k \leq k^*$ we must make a slight adjustment. Let $k < k^*$ be fixed and for $0 \leq i \leq k$ let

$$\delta(i) = \sum_{j \geq k+1} N_{i,j}p_j.$$

If $i < k+1 \leq j$ then $N_{k+1,j} = N_{i,j}(t^j-t^i)\cdots(t^j-t^k)$. Thus as

$$\delta(k+1) = \mathbf{E}(W)_{k+1} = t^{s(k+1)}(1+o(1))$$

we have that the tail $\delta(i)$ of the i-th equation is bounded by

$$\delta(i) \leq \frac{t^{s(k+1)}(1+o(1))}{(t^{k+1}-t^i)\cdots(t^{k+1}-t^k)}.$$

Let $\boldsymbol{p} = (p_0, p_1, ..., p_k)'$ and let $\boldsymbol{w} = (1-\delta_0,\ \mathbf{E}W - \delta_1, ..., \mathbf{E}(W)_k - \delta_k)'$. The system of equations (19) is now expressed as $N\boldsymbol{p} = \boldsymbol{w}$ where N is a $((k+1)\times(k+1))$ upper triangular matrix with positive entries $N_{i,j}$ on and above the main diagonal.

The discussion following (20), concerning the extraction of $p_r,\ 0 \leq r \leq k$ is still valid except now

$$p_r = \sum_{l=0}^{k-r} c(r,l) w_{r+l}.$$

Thus the difference $\theta(r) = |p_r - \pi_s(r-s,t)|$ is bounded above by

$$\theta(r) \leq \left| \sum_{l=k-r+1}^{\infty} c(r,l) t^{s(l+r)} \right| + \left| \sum_{l=0}^{k-r} c(r,l) O\left(\frac{1}{\log n}\right) t^{s(l+r)} \right| + \left| \sum_{l=0}^{k-r} c(r,l)\delta(r+l) \right|.$$

The first of these error terms is the truncation of the expansion of $\pi_s(r-s,t)$ in (17) above. The second comes from Theorem 8 where $\mathbf{E}(W)_k = t^{sk}(1+O(1/\log n))$. The third is the subtracted tails $\delta(i)$ of the equations. Provided $k \to \infty$ and r, s are constant it is straightforward to show that $\theta(r) \to 0$ as required. □

6 Bibliography

[A1] A. N. Alekseychuk, On uniqueness of the problem of moments in the class of q-distributions. Discrete Math. Appl 8.1 (1998) 1-16.

[A2] A. N. Alekseychuk, Conditions for uniqueness of the problem of moments in the class of q-distributions. Discrete Math. Appl. 9.6 (1999) 615-625.

[B] G. V. Balakin, The distribution of the rank of random matrices over a finite field. Theory of Probability and its Applications 8.4 (1968) 594-605.

[BKW] J. Blömer, R. Karp, E. Welzl, The rank of sparse random matrices over finite fields, Random Structures and Algorithms 10(4) (1997), 407-419 .

[CC] C. Cooper, On the rank of random matrices, Random Structures and Algorithms (2000) 209-232.

[CC1] C. Cooper, The rank of very sparse random matrices, (2000).

[Ha] G. Hadley, Linear Algebra, Addison-Wesley, 1979.

[Ko] V. F. Kolchin, Random Graphs, Cambridge University Press, Cambridge, England, 1999.

[K1] I. N. Kovalenko, On the limit distribution of the number of solutions of a random system of linear equations in the class of Boolean functions. Theory of Probability and its Applications 7.1 (1967) 47-56

[KL] I. N. Kovalenko and A. A. Levitskaya, Stochastic properties of systems of random linear equations over finite algebraic structures. Probabilistic Methods in Discrete Mathematics, (editor V. F. Kolchin) TVP Sci. Publ. 1993.

[KLS] I. N. Kovalenko, A. A. Levitskya and M. N. Savchuk, Selected Problems in Probabilistic Combinatorics (in Russian), Naukova Dumka, Kyiv,1986.

[vLM] J. H. van Lint and R. M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, England, 1992.