On the rank of random matrices

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

February 27, 2001

Abstract

Let $M = (m_{ij})$ be a random $n \times n$ matrix over *GF(2)*. Each matrix entry m_{ij} is independently and identically distributed, with $\Pr(m_{ij} = 0) = 1 - p(n)$ and $\Pr(m_{ij} = 1) = p(n)$. The probability that the matrix M is non-singular tends to $c_2 \approx 0.28879$ provided $\min(p, 1-p) \geq (\log n + d(n))/n$ for any $d(n) \to \infty$. Sharp thresholds are also obtained for constant $d(n)$.
This answers a question posed in the paper *The Rank of Sparse Random Matrices Over Finite Fields* by J. Blömer, R. Karp and E. Welzl, *Random Structures and Algorithms* 10(4) (1997).

1 Introduction

We consider the following model of random $(n \times n)$-matrices over *GF(t)*. Let $M = (m_{ij})$ be a $(n \times n)$-matrix with entries, r, in *GF(t)*, independently and identically distributed as follows:

$$\Pr(m_{ij} = r) = \begin{cases} 1 - p, & r = 0 \\ \\ \frac{p}{t-1}, & r \neq 0 \end{cases}$$

We denote the space of these matrices by $\mathbf{M}(n, p;\ t)$

In the paper, *The Rank of Sparse Random Matrices Over Finite Fields*, J. Blömer, R. Karp and E. Welzl, [BKW], pose the following question about $\mathbf{M}(n, p;\ t)$ at the end of Section 6 (*Generalizations and Open Problems*):

*Research supported by the STORM Research Group.

Is there a function $p(n)$ that tends to 0 as n goes to infinity and a constant $c > 0$ 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 non-singular with probability at least c?

In fact, provided $p(n)$ does not tend to either zero or one too rapidly, the asymptotic probability that such a matrix is non-singular is given by $c \approx 0.28879$. This value of c is the limit of right hand side of (1) below, in the case where $t = 2$.

We will require $p(n)$ to satisfy $\min(p(n), 1 - p(n)) \geq \frac{\log n + d(n)}{n}$, where $d(n) \to \infty$ arbitrarily slowly. For, if $p(n) \geq (\log n + d(n))/n$ where $d(n) \to \infty$, with probability tending to 1, there are no rows or columns of the matrix which are identically zero. Thus any linear dependencies are non-trivial. However, if $p \to 0$ in such a way that $d(n)$ is constant or $d(n) \to -\infty$ then the matrix may have rows or columns which are identically zero. Similarly if $p \to 1$ too rapidly, then the matrix may have two rows or columns consisting entirely of ones. The value c given above extends to the case where $d(n) \to -\infty$ slowly, provided we restrict our attention to the subset of random matrices which avoid these two types of linear dependency.

Consider first the special case in *GF(t)* when $p = \frac{t-1}{t}$, and thus all values and vectors are equiprobable. If the first s columns of the matrix M are linearly independent, they span a vector space of dimension s and size t^s. The probability that the next column avoids this space is $\left(1 - \frac{t^s}{t^n}\right)$, and thus

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

This result is a special case of a theorem (given in eg. [KLS] p33) for the limiting probability of rank of a square matrix in the equiprobable model.

Theorem 1 *Let $p = (t-1)/t$, and let M be a random $(n \times n)$-matrix with entries in GF(t). Let $p_n(k,t)$ be the probability that rank(M) $= n - k$, then*

$$\lim_{n\to\infty} p_n(k,t) = \pi(k,t) = \begin{cases} \prod_{j=1}^{\infty}\left(1 - \left(\frac{1}{t}\right)^j\right) & k = 0 \\ \frac{\prod_{j=k+1}^{\infty}\left(1-\left(\frac{1}{t}\right)^j\right)}{\prod_{j=1}^{k}\left(1-\left(\frac{1}{t}\right)^j\right)} \left(\frac{1}{t}\right)^{k^2} & k \geq 1 \end{cases} \tag{2}$$

The probabilities $\pi(k,t)$ are $\Theta\left(t^{-k^2}\right)$ and tend to zero very rapidly. Some values are tabulated below. Any value not tabulated is less than 1×10^{-10}.

k	$\pi(k,2)$	$\pi(k,3)$	$\pi(k,5)$	$\pi(k,7)$
0	0.2887880951	0.5601260779	0.7603327959	0.8367954017
1	0.5775761902	0.4200945584	0.2376039987	0.1627102180
2	0.1283502645	0.0196919324	0.0020625347	0.0004943453
3	0.0052387863	0.0000873902	0.0000006707	0.0000000296
4	0.0000465670	0.0000000410		
5	0.0000000969			

The precise number, $\eta_n(k,t)$, of $(n \times n)$-matrices of rank $(n-k)$, is a known quantity, and is given by (15) of Section 5. Thus $\pi(k,t)$ can also be obtained as $\pi(k,t) = \lim_{n\to\infty} \eta_n(k,t)/t^{n^2}$.

For *GF(2)*, $c_2 = \pi(0,2)$ is the limiting probability that M is non-singular for a wide range of p, as the following theorem shows.

Theorem 2 *Let* $M \in \mathbf{M}(n,p;\ 2)$ *be a random matrix over* GF(2).

(i) *If* $p = \frac{\log n + d(n)}{n} \leq 1/2$, *then*

$$\lim_{n\to\infty} \Pr(M \textit{ is non-singular }) = \begin{cases} 0 & d(n) \to -\infty \\ c_2 e^{-2e^{-d}} & d(n) \to d \textit{ constant} \\ c_2 & d(n) \to \infty \end{cases} \tag{3}$$

(ii) *If* $p = 1 - \frac{\log n + d(n)}{n} \geq 1/2$, *then*

$$\lim_{n\to\infty} \Pr(M \textit{ is non-singular }) = \begin{cases} 0 & d(n) \to -\infty \\ c_2 e^{-2e^{-d}}(1+e^{-d})^2 & d(n) \to d \textit{ constant} \\ c_2 & d(n) \to \infty \end{cases} \tag{4}$$

(iii) *Let a* unity row *of a matrix, be a row consisting entirely of 1's. Let* $\mathcal{F}$ *denote the event that* M *has no zero rows or columns and at most one unity row and column.*

If $\frac{\log n - \omega}{n} \leq p \leq 1 - \frac{\log n - \omega}{n}$, *where* $\omega = o(\log\log n)$, *then for any finite non-negative integer* k,

$$\lim_{n\to\infty} \Pr(M \textit{ has rank } n-k \mid \mathcal{F}) = \pi(k,2), \tag{5}$$

and in particular

$$\lim_{n\to\infty} \Pr(M \textit{ is non-singular} \mid \mathcal{F}) = c_2. \tag{6}$$

The case in Theorem 2(iii) given by (6) extends the results of Theorem 2(i),(ii) slightly.

Our approach is to count the number, W, of sequences of columns $(M_{i_1}, ..., M_{i_s})$ of M such that $i_1 < i_2 < \cdots < i_s$ and

$$c_1 M_{i_1} + \cdots + c_s M_{i_s} = 0,$$

where $c_i,\ i = 1, ..., s$ are non-zero elements of *GF(t)*. In a vector space over *GF(t)* a linear dependency $c_1\boldsymbol{a} + c_2\boldsymbol{b} = 0$ has $(t-2)$ *associated* dependencies $\alpha(c_1\boldsymbol{a} + c_2\boldsymbol{b}) = 0$ for $\alpha \in GF(t)\backslash\{0,1\}$. In our estimate $\mathbf{E}W$, of the expected number of linear dependencies, in Section 3, we divide our result by $\frac{1}{t-1}$ to count only non-associated dependencies.

Theorem 3 *Let* $t \geq 3,\ t = o(\sqrt{\log n})$ *be a prime power. Let* $M \in \mathbf{M}(n, p;\ t)$ *be a random matrix over* GF(t). *Let* $p = \frac{\log n + \log(t-1) + \omega}{n}$, *where* $\omega \to \infty$, *then the expected number of non-associated linear dependencies in the columns of* M *tends to* $\frac{1}{t-1}$ *as* $n \to \infty$.

A sub-sequence $A = (M_{i_1}, M_{i_2}, ..., M_{i_s})$ of the columns of M is uniquely described by its index set $I_A = \{i_1, i_2, ..., i_s\}$. We will write $A = (a_1, a_2, ..., a_s)$ where $a_j = M_{i_j}$. If there is no ambiguity, we do not distinguish between A and I_A and shall speak of A as a *column set*. We reserve the notation $A_1, A_2, ..., A_j...$ to refer to sets $1, 2, ..., j..$ of columns.

Suppose the rank of M is $n - k$, so that the *defect* is k, (following the notation of [BKW]). We can partition the columns of M into $(M(n-k), M(k))$. Here $M(n-k)$ is an $(n \times (n-k))$-matrix of full column rank, $(n-k)$, and the columns of $M(k)$ lie in the column space of $M(n-k)$. Thus there are $t^k - 1$ (not necessarily distinct) linear dependencies in the columns of M induced by non trivial linear combinations of the columns of $M(k)$.

We can also regard M as a sequence of columns $(M_1, ..., M_n)$ which we reveal one at a time. Suppose that the defective columns have indices $i_1, ..., i_k$. We can define unique *smallest* linearly dependent column sets $A_1, ..., A_k$, where the final column of A_j is i_j. If the columns of A_j are $(M_{s_1}, ..., M_{i_j})$, then $(i_j - s_1)$ is the smallest of all index differences of linearly dependent sequences of columns with final column M_{i_j}.

Let $A \Delta B$ be the symmetric set difference $A \cup B - A \cap B$ of the sets A and B. In the case of column sets A, B we shall write $A \Delta B$ to mean the set of columns with index set $I_A \Delta I_B$.

If the defect of M is k and the field is *GF(2)*, the smallest column sets $A_1, ..., A_k$ generate $2^k - (k+1)$ other linearly dependent sets $A_1 \Delta A_2,\ \ A_1 \Delta A_3, ...,\ \ A_1 \Delta A_2 \Delta \cdots \Delta A_k$.

For reasons given below, we definitely do not want to count all $2^k - 1$ dependent sets arising from a defect of k. But we cannot quite count just the smallest dependencies $A_1, ..., A_k$ either. We settle for a compromise and count *simple* sequences[1] of linearly dependent column sets $\boldsymbol{B} = (B_1, ..., B_k)$. A k-tuple of sets $\boldsymbol{B} = (B_1, ..., B_k)$ is simple, if no set B_i in $\boldsymbol{B}$ is a set difference of other sets B_j in $\boldsymbol{B}$. In other words, events

$$B_{j_1} \Delta B_{j_2} \Delta \cdots \Delta B_{j_l} = \emptyset \qquad (j_1 < j_2 < ... < j_l) \qquad (1 \leq l \leq k)$$

do not occur.

[1] In the paper [Ko], V. Kolchin also recognises the value of simple sequences. He calls such sequences *independent*, perhaps a better notation. We retain the notation *simple* in order to make a distinction from general discussions of linear independence.

Let $V(M) = \{\emptyset\} \cup \{B : B$ is zero-sum in $M\}$, then $(V(M), \Delta)$ is a vector space over *GF(2)* under the convention that $0 \cdot B = \emptyset,\ 1 \cdot B = B$. In $V(M)$ a simple sequence $(B_1, ..., B_k)$ is an ordered basis of dimension k.

If W is the number of linear dependencies in M, we calculate the expected number of simple l-sequences, for $l \geq 1$. Denote this by $\mathbf{E}(W, l;\ \text{simple })$ We will show that in *GF(2)*, $\mathbf{E}(W, l;\ \text{simple }) \sim 1$. Of course the restricted expectation $\mathbf{E}(W, l;\ \text{simple })$ is much less than the usual (unrestricted) l-th factorial moment $\mathbf{E}(W)_l$ of W, but that is just as well. As proved in [KLS] (p34-35), the limiting probabilities $\{\pi(k, t)\}$ do not satisfy the Carleman condition (see eg [Du]) to recover the distribution $\{\pi(k, t)\}$ from the moments $\mathbf{E}W^l$, where W is the number of linear dependencies in M.

For simplicity of notation we denote $\mathbf{E}(W, l;\ \text{simple })$ by $\mathbf{E}(W)_l$ throughout this paper.

Let $A = (a_1, ..., a_m)$ be a subsequence of the columns $(M_1, ..., M_n)$ of M, and $\boldsymbol{c} = (c_1, ..., c_m)$ a sequence of *non-zero* coefficients from *GF(t)*. The matrix M is singular if and only if there exist $\boldsymbol{c}$ and A such that

$$c_1 a_1 + c_2 a_2 + \cdots + c_m a_m = 0 \qquad c_i \neq 0,\ i = 1, ..., m. \tag{7}$$

Given a subsequence A of M, we count $\sum_{\boldsymbol{c}} 1_{(\boldsymbol{c}A=0)}$, where 1_X is the indicator for the event X and where $\boldsymbol{c} \in (GF(t) \setminus \{0\})^m$. Because *GF(t)* is a field, and by definition any non-zero element has probability $p/(t-1)$, for *fixed* non-zero $c_i,\ i = 1, ..., m$ the event given in (7) has the same probability as the event, $a_1 + \cdots + a_m = 0$, that the set of columns A is *zero-sum*.

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

$$\rho_m(r) = \begin{cases} \frac{1}{t}\left(1 + (t-1)(1 - \frac{t}{t-1}p)^m\right) & r = 0 \\ \\ \frac{1}{t}\left(1 + (-1)(1 - \frac{t}{t-1}p)^m\right) & r \neq 0 \end{cases} \tag{8}$$

The results (8) are derived by recurrence relations (see eg. [BKW]).

Let $\rho_m(0) = \rho_m$. The probability that a subsequence $A = (a_1, ..., a_m)$ of the columns of M satisfies $a_1 + \cdots + a_m = 0$ is ρ_m^n. The number W_m of non-associated linearly dependent m-subsets has expectation

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

2 The structure of the proof of Theorem 2

We prove Theorem 2(i),(ii) in three parts corresponding to the three cases listed in (3) or (4). The case where $d(n) \to -\infty$ is more or less trivial as zero rows (resp. pairs of unity rows) occur with probability tending to 1 as $p \to 0$ (resp. $p \to 1$), and this case is not treated in any detail. The case treated in **Sections 3,4** is for the range $\min(p, 1-p) \geq (\log n + d(n))/n$ where $d(n) \to \infty$. The case of Theorem 2(i),(ii) where $d(n) = d$, constant, (the sharp threshold) follows directly from the proof of Theorem 2(iii) given in **Sections 6, 7**.

In **Section 3** we calculate the expected number of linear dependencies $\mathbf{E}W$ in the columns of M over *GF(t)*. We show that, provided $d(n) \to \infty$, **whp**[2] any linear dependencies in the columns of M must be of size about $n(t-1)/t$, and we condition on this event in all subsequent calculations.

In **Section 4** we focus on *GF(2)*. We calculate the expected number $\mathbf{E}(W)_k = \mathbf{E}(W, k;$ simple $)$ of *simple* k-tuples of linearly dependent column sets $(A_1, A_2, ..., A_k)$ where each $|A_i| \sim n/2$. We show that $\mathbf{E}(W)_k \sim 1$. This result holds for $k \geq 1$, and provided k does not tend to infinity too quickly. The result is formally stated in Lemma 6, but the entire section is devoted to the proof.

The proof that $\mathbf{E}(W)_k \sim 1$ requires a technical lemma, Lemma 7, to bound the error terms. The most important part of Lemma 7 is part (iii) which deals with the cancellation of these error terms. To maintain continuity of exposition, the proof of Lemma 7 is given in the Appendix.

In **Section 5** we obtain the limiting probability distribution $(\pi(j, 2),\ j \geq 0)$ of the defect of M from the moments $\mathbf{E}(W)_k$. The values of $\pi(j, 2)$ are given by Theorem 1. The preliminary discussion is true for a general finite field *GF(t)*. This discussion includes a proof of Theorem 1. We then restrict our attention to *GF(2)* to complete the proof of Theorem 2. The only detail required for convergence to the distribution $(\pi(j, 2),\ j \geq 0)$ is that $\mathbf{E}(W)_k \sim 1$, so that proving this result in **Sections 4, 6, 7** establishes the required convergence for the various cases of Theorem 2.

In working with $\mathbf{E}(W)_k$, the lattice we count over is subspaces of a vector space, rather than subsets of a set. Thus the usual formula for recovering the probability distribution from the factorial moments is incorrect here. The main function of Section 5 is to draw together various standard results on Möbius inversion on a lattice of vector spaces, in an asymptotic context.

Section 6 considers the proof of Theorem 2(i), (ii), (iii) for *GF(2)* in the case where $p = (\log n + d(n))/n$ and $|d(n)| = o(\log \log n)$ (the sharp threshold). When $|d|$ is constant or tends to infinity very slowly, the number of zero rows and columns occurring in M is asymptotically Poisson with parameter $2e^{-d}$. Fortunately, the correlation between any zero rows or columns and large $(m \sim n/2)$ linear dependent sets of columns is asymptotically zero. Conditioning on the event that there are no zero rows or columns, we can show $\mathbf{E}(W)_k \sim 1$, and the results of Sections 5 hold.

[2]With high probability: with probability tending to 1 as $n \to \infty$

Section 7 considers the sharp threshold for *GF(2)* in the case where $1-p=(\log n+d(n))/n$ and $|d(n)|=o(\log\log n)$. Because (8) is symmetric in p and $1-p$ when $t=2$ and m is even (see (23)) we can adapt the proofs of the previous section.

3 The expected number of linear dependencies

We calculate the expected number of linear dependencies $\mathbf{E}W$ in the columns of M, where

$$\mathbf{E}W=\sum_{m=1}^{n}\mathbf{E}W_m.$$

This calculation is for any *GF(t)*, $t=o(\sqrt{\log n})$ under the assumption that $p\geq p_0$, where $p_0=(\log n+\log(t-1)+d(n))/n$. In the case of *GF(2)* we further require that $p\leq 1-p_0$. Provided $d(n)\to\infty$ the main contribution to $\mathbf{E}W$ is from $\mathbf{E}W_m$ where $m\sim n(t-1)/t$. Specifically, $\sum_{m\sim n(t-1)/t}\mathbf{E}W_m\to\frac{1}{t-1}$ and $\sum_{m\not\sim n(t-1)/t}\mathbf{E}W_m\to 0$. The case $m\sim n(t-1)/t$ is straightforward. The 'other m' analysis requires more care. To preserve continuity of exposition, the calculations are given in the appendix.

Lemma 4 *Let the field be* GF(t)*, where* $t=o(\sqrt{\log n})$*. Let* $p=c/n$ *where* $c=\log n+\log(t-1)+\omega$*, and* $\omega\to\infty$*.*

$$\mathbf{E}W=\frac{1}{t-1}\left(1+O(e^{-\omega})\right).$$

Lemma 5 *Let the field be* GF(t)*, where* $t=o(\sqrt{\log n})$*. Let* $p=c/n$ *where* $c=\log n+\log(t-1)+d(n)$ *where* $d(n)>-o(\log\log n)$*.*

(i) With probability $1-o(1/n)$ *no linearly dependent set,* A*, of columns of* M *has* $\log n\leq|A|\leq m_2=n\frac{t-1}{t}\left(1-4\sqrt{\frac{\log n}{n}}\right)$ *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 probability* $1-O(e^{-\omega})$ *there are no linearly dependent sets* A *of size* $1\leq|A|\leq\log n$*.*

4 Factorial moments of W in GF(2)

We now restrict our attention to *GF(2)* and $d(n)\to\infty$. We calculate $\mathbf{E}(W)_k$ over all simple k-tuples $(A_1,...,A_k)$ of zero-sum sets. Let $(W)_k=\sum 1_{(A_1,...,A_k)}$, where $1_{(A_1,..,A_k)}$ is the indicator for the event that the column sets $(A_j:j=1,...,k)$ of M are zero-sum.

Say A is *Small* if $|A| < m_2$, where $m_2 = n^{\frac{t-1}{t}}\left(1 - 4\sqrt{\frac{\log n}{n}}\right)$. Let $\mathcal{N}$ be the property that no zero-sum set is Small. By Lemma 5 $\mathcal{N}$ occurs with probability $1 - O(e^{-\omega})$. In this section we prove the following result.

Lemma 6 $\mathbf{E}(W)_k = 1+(2^k-1)e^{-\omega}(1+o(1))$. *The counting is over all simple k-tuples, and restricted to $\mathcal{N}$.*

This result is proved for $k = 1$ in (31) of the appendix.

In order to calculate the k-th factorial moment of W we dissect any k-tuple of zero-sum sets $A_1, ..., A_k$ into disjoint sets $I_j,\ j = 1...L$ and express each A_i as the union of a suitable subset of the I_j, indexed by a set $C(A_i) \subset \{1, ..., L\}$. The parity of A_i depends on the parity of the selected subsets I_j. The parities of the subsets, I_j which allow $A_1, ..., A_k$ to be simultaneously zero-sum is described by an equation $\boldsymbol{Ay} = \mathbf{0}$.

As a motivating example, consider two zero-sum sets A_1, A_2. This defines three (index) sets $I_1 = A_1 \cap \overline{A}_2,\ I_2 = A_1 \cap A_2,\ I_3 = \overline{A}_1 \cap A_2$. The parity restrictions on the subsets, I_j, given by $\boldsymbol{Ay} = \mathbf{0}$ has vector $\boldsymbol{y} = (y_1, y_2, y_3)$ for the parities of (I_1, I_2, I_3) and matrix $\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. Thus, in *each* row of M, the only possible simultaneous parities of the sum of the entries in these subsets are:

$A_1 \cap \overline{A}_2$	$A_1 \cap A_2$	$\overline{A}_1 \cap A_2$
0	0	0
1	1	1

Suppose, now, we have zero-sum column sets $A_1, A_2, ..., A_k$. To calculate factorial moments, we need to consider the $L = 2^k - 1$ subsets arising from the intersection of the sets A_j. The general intersection is $I = X_1X_2...X_k$, where $X_j \in \{A_j, \overline{A}_j\}$, and where XY denotes $X \cap Y$. We write these intersections (in some order) as $I_1, ..., I_L$ and let $I_{L+1} = \overline{A}_1\overline{A}_2...\overline{A}_k$.

We fix our attention on row s of M. Let

$$f(I) = \sum_{i \in I} m_{si} \pmod 2$$

be the total (mod 2) in row s of entries m_{si} of M with columns idexed by the subset I. In order for $A_1, ..., A_k$ to be simultaneously zero-sum in row s of M, we have k equations $EQ_1(A_1), ...EQ_k(A_k)$ restricting the parity (in row s) of the sums $f(I)$ on the sets $I_1, ..., I_L$. Thus, for example, A_1 is dissected into 2^{k-1} subsets $A_1X_2 \cdots X_k$ and $EQ_1(A_1)$ is

$$f(A_1\overline{A}_2 \cdots \overline{A}_k) + f(A_1A_2\overline{A}_3 \cdots \overline{A}_k) + \cdots + f(A_1A_2 \cdots A_k) = 0 (\mathrm{mod}\ 2).$$

In general, EQ_i is $\sum_{I_j \subset A_i} f(I_j) = 0 (\text{mod } 2)$. We will record which sets A_i, $(i = 1, ..., k)$ occur uncomplemented in the subsets I_j, $(j = 1, ..., L)$ as a $(k \times L)$-matrix $\boldsymbol{A} = (a_{ij})$. The i-th row of $\boldsymbol{A}$ corresponds to A_i, and

$$a_{ij} = \begin{cases} 0 & X_i = \overline{A}_i \text{ in } I_j \\ 1 & X_i = A_i \text{ in } I_j \end{cases}$$

The terms $y = f(I)$ of EQ_i are evaluated on the non-zero entries a_{ij} in row i of $\boldsymbol{A}$. We write the equations $EQ_1, ..., EQ_k$ as $\boldsymbol{Ay} = \boldsymbol{0}$. Here $\boldsymbol{y} = (y_1, ..., y_L)$ is a column vector over *GF(2)*. We give the proof of the following lemma in the Appendix.

Lemma 7 *Let $(A_1, A_2, ..., A_k)$ be a simple k-tuple of zero-sum sets.*

(i) *At most $L - k$ sets I can be empty.*

(ii) *Let $T = \{\boldsymbol{y} : \boldsymbol{Ay} = \boldsymbol{0}\}$. If $0 \le i \le L - k$ sets I are empty then $|T| = 2^{L-k-i}$.*

(iii) *Let $J = \{j_1, ..., j_s\}$ index a subset of the columns of $\boldsymbol{A}$. Let*

$$\lambda(J) = \sum_{\boldsymbol{y} \in T} (-1)^{y_{j_1} + \cdots + y_{j_s}}.$$

There is a set S consisting of $|S| = (2^k - 1)$ index sets $C \subset \{1, ..., L\}$ such that

$$\lambda(J) = \begin{cases} |T| & \textit{if } J = C \in S \\ 0 & \textit{otherwise.} \end{cases}$$

(iv) *For $C \in S$ let the sets I_j indexed by $C = \{j_1, ..., j_N\}$ satisfy*

$$I_{j_1} \cup \cdots \cup I_{j_N} = B_C.$$

There are sets $A_{i_1}, ..., A_{i_l}$ indexed by $\{i_1, ..., i_l\} \subset \{1, ..., k\}$ such that $C = C(i_1, ..., i_l)$ and

$$B_C = A_{i_1} \Delta \cdots \Delta A_{i_l},$$

and thus the set B_C is zero-sum.

Basically, this lemma says the following: Let $\boldsymbol{e} = (e_j : j = 1, ..., L)$ be a vector and let $J = \{j : e_j = 1\}$. The only J with non-zero $\lambda(J)$ are those with $\boldsymbol{e}(J)$ in the row space of $\boldsymbol{A}$. This is because such an $\boldsymbol{e}(J)$ describes a linear combination of the zero-sum sets $A_1, ..., A_k$ so that $y_{j_1} + \cdots + y_{j_s} \equiv 0 (\text{mod } 2)$.

Let x_j denote the number of columns of M in I_j.

Consider the s-th row of M. Provided no $I = \emptyset$, from equation (8) we find

$$\begin{aligned}
\pi(x_1, ..., x_L) &= \Pr(A_1, A_2, ..., A_k \text{ are zero-sum in the } s\text{-th row of } M) \\
&= \sum_{(y_1,...,y_L)\in T} \prod_{j=1}^{L} \left\{ \tfrac{1}{2}\left(1 + (-1)^{y_j}(1-2p)^{x_j}\right)\right\} \\
&= \frac{1}{2^L}\left(|T| + \sum_{i=1}^{L} \sum_{J=\{j_1,...,j_i\}} (1-2p)^{x_{j_1}+\cdots+x_{j_i}} \sum_{\boldsymbol{y}\in T} (-1)^{y_{j_1}+\cdots+y_{j_i}} \right),
\end{aligned}$$

where $|T| = 2^{L-k}$. Thus, by Lemma 7(iii),

$$\pi = \frac{1}{2^k}\left(1 + \sum_{C\in S}(1-2p)^{x_{j_1}+\cdots+x_{j_N}}\right). \tag{9}$$

Let $B = I_{j_1} \cup \cdots \cup I_{j_N}$. If $|B| \geq m_2$ then $x_{j_1} + \cdots + x_{j_N} = \frac{n}{2}(1 - 4\sqrt{\frac{\log n}{n}})$ and

$$(1-2p)^{x_{j_1}+\cdots+x_{j_N}} = \frac{e^{-\omega}}{n}(1+o(1)). \tag{10}$$

However, by Lemma 7(iv), if $C = \{j_1, ..., j_N\} \in S$ then $B = B_C$ is zero-sum, and hence $|B| \geq m_2$ as we have conditioned on $\mathcal{N}$. Thus as $|S| = 2^k - 1$ and $L + 1 = 2^k$,

$$\begin{aligned}
\mathbf{E}(W)_k &= \sum \binom{n}{x_1, ..., x_{L+1}} (\pi(x_1, ..., x_L))^n \\
&= \left(1 + (2^k-1)e^{-\omega}(1+o(1))\right) \sum \binom{n}{x_1, ..., x_{L+1}} \frac{1}{2^{kn}} \\
&= 1 + (2^k-1)e^{-\omega}(1+o(1))
\end{aligned}$$

as required. The multinomial sum was approximated in a manner similar to (29).

If i of the sets I are empty, then

$$\pi(x_1, ..., x_{L-i}) = \frac{1}{2^{L-i}}\left(|T| + \sum_{s=1}^{L-i} \sum_{J=\{j_1,...,j_s\}} (1-2p)^{x_{j_1}+\cdots+x_{j_s}} \sum_{\boldsymbol{y}\in T} (-1)^{y_{j_1}+\cdots+y_{j_s}} \right),$$

where all the sets indexed by J are nonempty. But now, $|T| = 2^{L-k-i}$ so that

$$\pi = \frac{1}{2^k}\left(1 + \sum_{C\in S}(1-2p)^{x_{j_1}+\cdots+x_{j_N}}\right),$$

as before. Possibly, some of the $x_j = 0$, but $x_{j_1} + \cdots + x_{j_N} \geq m_2$ and $|S| = 2^k - 1$. Thus

$$\mathbf{E}(W)_k \sim \left(\frac{2^k - i}{2^k}\right)^n = o(1).$$

5 Limiting probability distribution of matrix defect

The initial discussion in this section is true for general *GF(t)* and concerns the distribution $(\pi(r,t),\ r \geq 0)$ given in (2). The t-nomial theorem[3] states that, for $r \geq 1$,

$$(1+x)(1+tx)\cdots(1+t^{r-1}x) = \sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix}_t t^{\binom{k}{2}} x^k, \tag{11}$$

where the Gaussian coefficients are defined, for $t > 0$ by $\begin{bmatrix} r \\ 0 \end{bmatrix}_t = 1$ and

$$\begin{bmatrix} r \\ k \end{bmatrix}_t = \frac{(t^r-1)(t^{r-1}-1)\cdots(t^{r-k+1}-1)}{(t^k-1)(t^{k-1}-1)\cdots(t-1)}.$$

If we define

$$\begin{bmatrix} \infty \\ k \end{bmatrix}_z = \frac{1}{(1-z^k)\cdots(1-z)} \qquad |z|<1, \qquad k \geq 1,$$

then

$$\prod_{r=0}^{\infty}(1+z^r x) = \sum_{k=0}^{\infty} \begin{bmatrix} \infty \\ k \end{bmatrix}_z z^{\binom{k}{2}} x^k. \tag{12}$$

We note that if $t > 1$ then

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

Using the convention that $\prod_{j=1}^{0}(t^j-1) = 1$, let us define $a(r),\ b(r,l)$ and $c(r,l)$ by

$$c(r,l) = (-1)^l \frac{t^{-\binom{r}{2}}}{\prod_{j=1}^{r}(t^j-1)} \frac{t^{-rl}}{\prod_{j=1}^{l}(t^j-1)} = (-1)^l a(r) b(r,l). \tag{13}$$

Then from (2) and (12),

$$\begin{aligned} \sum_{l\geq 0} c(r,l) &= \frac{t^{-\binom{r}{2}}}{\prod_{j=1}^{r}(t^j-1)} \sum_{l\geq 0} \begin{bmatrix} \infty \\ l \end{bmatrix}_{\left(\frac{1}{t}\right)} \left(\frac{1}{t}\right)^{\binom{l}{2}} \left(\frac{-1}{t^{r+1}}\right)^{l} \\ &= \frac{t^{-\binom{r}{2}}}{\prod_{j=1}^{r}(t^j-1)} \prod_{l\geq 0}\left(1+\left(\frac{1}{t}\right)^{l}\left(\frac{-1}{t^{r+1}}\right)\right) \\ &= \pi(r,t). \end{aligned} \tag{14}$$

[3] See ([Cm] (p125),[Kn] (p78) or [vLW] (p291)) for more details.

To obtain the values $c(r,l)$ we used the result (see [vLW] (p303)), that the number of $(n\times n)$-matrices over *GF(t)* with defect r is

$$\eta_n(r,t) = \begin{bmatrix} n \\ r \end{bmatrix}_t \sum_{l=0}^{n-r} (-1)^l \begin{bmatrix} n-r \\ l \end{bmatrix}_t t^{n(n-(r+l))+\binom{l}{2}}. \tag{15}$$

When $p=(t-1)/t$ and all matrices of the space $\mathbf{M}(n,p;t)$ are equiprobable, we have $Pr(\text{ Defect} = r) = \eta_n(r,t)/t^{n^2}$. It can be easily shown that

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

which we have already proved is $\pi(r,t)$. We now prove the following lemma:

Lemma 8 *Let the field be* GF(2) *and let $\pi(r,2)$ be given by Theorem 1. Let $\{M\}$ be a space of random $(n\times n)$-matrices for which $\mathbf{E}(W)_k = 1+\epsilon(k)$. Let r be constant. If $\sum_{l\geq 0} c(r,l)\epsilon(r+l) \to 0$ then*

$$\lim_{n\to\infty} Pr\,(M \text{ has defect } r) = \pi(r,2).$$

Proof Let $t=2$. Let $(A_1,\ldots,A_k)$ be a k-tuple of simple zero-sum sets of columns A_j of M. Let $N_{k,r}$ be the number of simple k-tuples if the defect of M is r. Simple k-tuples are ordered k-sequences of linearly independent vectors, in the vector space over *GF(2)* generated by the set differences $A\Delta B$ of zero-sum columns of M. Thus $N_{k,r}$ is the number of ordered k-bases of an r-dimensional vector space[4], 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 defect k is $p(k,t)=p_k$ we can write

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

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

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

[4]See [Ko] for an alternative discussion of this.

The tail of the distribution $\{p(k,t)\}$ is small even for constant k, as

$$\sum_{j\geq k} p_j \leq \frac{\mathbf{E}(W)_k}{N_{k,k}} < t^{-\binom{k}{2}}.$$

We wish to prove $p_r = p(r,t) \to \pi(r,t)$ as given in (2). To extract $p_r = p(r,t)$ we will multiply $\mathbf{E}(W)_{r+l}$ for $l \geq 0$ by $c(r,l)$, given by (13) and add.

The right hand side gives p_r exactly. For, if $j = r+s,\ s \geq 0$, 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,

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

Thus the coefficient of p_j is

$$a(r)(t^j-1)\cdots(t^j-t^{r-1})\sum_{l=0}^{j-r}\left[\begin{array}{c} j-r \\ l \end{array}\right]_t t^{\binom{l}{2}}(-1)^l,$$

so that for $j > r$, this coefficient is identically zero, from (11), with $x = (-1)$.

As $\mathbf{E}(W)_k \sim 1$ the left hand side will tend to $\pi(r,t)$ by the argument of (14) above. The least accurate estimate of $\mathbf{E}(W)_k$ occurs in Section 4 so we consider this case in most detail. Specifically, from Lemma 6 let $\mathbf{E}(W)_k = 1 + (2^k-1)e^{-\omega}(1+o(1))$, then

$$\begin{aligned} \sum_{l\geq 0} c(r,l)\mathbf{E}(W)_{r+l} &= \pi(r,2) + \sum_{l\geq 0}\left((2^{r+l}-1)e^{-\omega}\right)(1+o(1))(-1)^l a(r)\frac{2^{-rl}}{\prod_{j=1}^{l}(2^j-1)} \\ &= \pi(r,2) + 2^r e^{-\omega}O(1) \\ &\sim \pi(r,2), \end{aligned}$$

provided $2^r e^{-\omega} \to 0$, which it does as r is constant and $\omega \to \infty$. □

6 The sharp threshold as $p \to 0$.

Let $np = \log n + d(n)$ where $|d(n)| = o(\log\log n)$. To be specific, we will choose $|d| \leq \log(\frac{1}{2}\log\log n)$ so that $1/(\log n) \leq \exp(-2e^{-d}) \leq 1$. We wish to condition on the event $\mathcal{F}$ that M has no zero rows or columns, and at most one unity row and column. The following remarks constitute the proof of Theorem 2(iii) and of Theorem 2(i),(ii) when d is constant (the sharp threshold) and $p \to 0$.

(R1) The probability the matrix has no zero rows and columns:

We show that

$$\begin{aligned} \Pr(\text{ No zero rows or columns }) &= (1-(1-p)^n)^{2n}(1+o(1)) && (16)\\ &\sim e^{-2e^{-d}}. && (17) \end{aligned}$$

In fact, for (R2), we will consider a matrix M on m rows and n columns, with a fixed set R of r distinguished columns. The number of zero rows in M is $B(m,(1-p)^n)$, and $\Pr(\text{ No zero rows }) = (1-(1-p)^n)^m$. Let the values m, r and k satisfy $|n-m|, r, k = O(\log n)$. Let X be the number of zero columns in $M-R$, and let $(X)_k$ denote the (ordinary) factorial moment of X. For fixed $k \le \log n$

$$\begin{aligned} \mathbf{E}((X)_k \mid \text{ No zero rows in } M) &= (n-r)_k(1-p)^{km}\frac{\left(1-(1-p)^{n-k}\right)^m}{(1-(1-p)^n)^m}\\ &= (n-r)_k(1-p)^{mk}\left(1-kpe^{-d}(1+o(1))\right) \end{aligned}$$

Thus by (standard) inclusion-exclusion, and using the Bonferroni Inequalities to halt the summation at $k=\log n$ (see eg. [Pa] p141)

$$\Pr(\text{No zero columns in } M-R \mid \text{ No zero rows in } M) = (1-(1-p)^m)^{n-r}\left(1+o\left(\frac{\log^7 n}{n}\right)\right) \tag{18}$$

and (16) follows when $r=0$ and $m=n$.

(R2) Lemma 5 is still true: In particular, conditional on 'No zero rows or columns', with probability $1-o(1)$ there are no Small ($< m_2$) zero-sum subsets of columns.

Proof We note that

$$\begin{aligned} \mathbf{E}(W \mid \text{ No zero rows or columns }) &\le (\mathbf{E}W)/(Pr(\text{ No zero rows or columns })) \\ &\le 2\mathbf{E}We^{2e^{-d}} \end{aligned}$$

where $e^{2e^{-d}} \le \log n$. We can use the estimates of $\sum \mathbf{E}W_m$ of cases $\log n \le m \le m_2$ and $m_3 \le m \le n$ from Section 3, Lemma 5 as these are are $o(1/n)$. We now consider the case of $2 \le m \le \log n$.

We first prove that **whp** a set of m columns of M has at most e^2mnp non-zero entries. Let Z be a Binomial random variable with mean μ, and let $\alpha \ge 1$, then by the Chernoff Inequality,

$$Pr(Z \ge \alpha\mu) \le \left(\frac{e}{\alpha}\right)^{\alpha\mu} e^{-\mu}.$$

The number of entries in the columns is $B(nm,p)$ with mean $\mu = mnp$. Let $\mathcal{R}$ be the event that there exists a set columns with at least $e^2\mu$ entries, then

$$\begin{aligned} Pr(\mathcal{R}) &\leq \binom{n}{m} e^{-(e^2+1)\mu} \\ &< \exp -em\log n. \end{aligned} \tag{19}$$

Let N be the $(n \times m)$-matrix consisting of the selected columns. Each column of N must have at least one non-zero entry, as no column of M is zero. Let $n-s$ rows of N be zero. The remaining s rows must each have at least two non-zero entries. Thus N has at least $\theta = \max(m, 2s)$ non-zero entries. The expected number of (m,s) pairs satisfying this condition is at most

$$\nu(m,s) = \binom{n}{m}\binom{n}{s}(1-p)^{(n-s)m} Pr(X \geq \theta),$$

where $X \sim B(sm,p)$. Thus by the Chernoff Inequality

$$\begin{aligned} Pr(X \geq m) &\leq (esp)^m e^{-smp} \\ Pr(X \geq s) &\leq (\tfrac{1}{2}emp)^{2s} e^{-smp}. \end{aligned}$$

Case $s \leq \lfloor m/2 \rfloor$:

$$\begin{aligned} \nu(m,s) &\leq \frac{n^m}{m!}\frac{n^s}{s!}(\exp -npm)(esp)^m \\ &\leq O(1)\left(e^{-d+2}(\log n)\right)^m e^s \left(\frac{s}{n}\right)^{m-s} \\ &\leq (\log n)^{2m}\left(\frac{m}{n}\right)^{m-\lfloor m/2 \rfloor}. \end{aligned}$$

Case $s > \lfloor m/2 \rfloor$:

$$\begin{aligned} \nu(m,s) &\leq \frac{n^m}{m!}\frac{n^s}{s!}(\exp -npm)(\tfrac{1}{2}emp)^{2s} \\ &\leq \left(\frac{e^{-d+1}}{m}\right)^m \left(\frac{e^3 m(\log n)^2}{n}\right)^s. \end{aligned}$$

Thus

$$\sum_s \nu(m,s) \leq O\left(\left(\frac{(\log n)^3}{n}\right)^{m/2}\right),$$

so that $\sum_{m,s} \nu(m,s) = O\left(\frac{\log^4 n}{n}\right)$.

Let N have s non-zero rows, S. By (19) $|S| = s \le e^2 mnp$. We can rearrange M into

$$M = \begin{pmatrix} S & S_1 & O \\ O & R & M_1 \end{pmatrix}.$$

The matrix S_1 is $s \times r$ and each column contains non-zero entries, arising from the rows of S in $M - N$. By (19), S_1 almost always has $r \le e^2 snp$ columns. The matrix M_1 is $(n-s) \times (n-m-r)$. By the condition that M has no zero rows or columns, the matrix $(R \;\; M_1)$ has no zero rows, and the columns of M_1 are non-zero. By (18) of (R1) the probability of this event is asymptotically equal to the conditioning probability (16) of the event that M has no zero rows or columns. The result follows.

$\square$

(R3) We now prove $\mathbf{E}((W)_k \mid \text{ No zero rows or columns }) = 1 + o\left(\frac{\log^4 n}{\sqrt{n}}\right)$.

(R3a) We modify (9), so that π becomes $\phi = \pi - (1-p)^n$, for the event that $A_1, ..., A_k$ are zero-sum in the given row, but the row is not identically zero.

$$\begin{aligned} \phi &= \Pr((A_1, ..., A_k) \text{ are zero-sum in row } j) \text{ and (Row } j \text{ is not zero))} \\ &= \frac{1}{2^k}\left(1 + \sum_{C \in S}(1-2p)^{x_{j_1}+\cdots+x_{j_N}} - 2^k(1-p)^n\right) \\ &= \frac{1}{2^k}\left(1 - \frac{e^{-d}}{n}\left(1 + o\left(\frac{\log^2 n}{\sqrt{n}}\right)\right)\right), \end{aligned} \tag{20}$$

because, by (R2) $x_{j_1} + \cdots + x_{j_N} \ge m_2 = \frac{n}{2}\left(1 - 4\sqrt{\frac{\log n}{n}}\right)$, and $|S| = 2^k - 1$, so

$$\sum_{C \in S}(1-2p)^{x_{j_1}+\cdots+x_{j_N}} = (2^k - 1)\frac{e^{-d}}{n}\left(1 + o\left(\frac{\log^2 n}{\sqrt{n}}\right)\right).$$

Thus

$$\Pr(((A_1, ..., A_k) \text{ are zero-sum) and (No zero rows)}) = \frac{1}{2^{kn}} e^{-e^{-d}}\left(1 + o\left(\frac{\log^3 n}{\sqrt{n}}\right)\right). \tag{21}$$

(R3b) We next prove

$$\Pr(\text{ No zero columns } \mid ((A_1, ..., A_k) \text{ are zero-sum) and (No zero rows)))} \sim e^{-e^{-d}} \tag{22}$$

Proof Let $X(k) = \sum_{s=1}^n X_s(k)$, where

$$X_s(k) = \begin{cases} 1 & \text{if } (M_s \text{ is a zero column}),\ ((A_1, ..., A_k) \text{ are zero-sum) and (No zero rows)} \\ 0 & \text{otherwise} \end{cases}$$

Let $m = |\cup_{i=1...k} A_i|$. Considering l-tuples of zero columns, we find for fixed $l \leq \log n$

$$\begin{aligned}
\frac{\mathbf{E}(X(k))_l}{l!} &= \sum_{j=0}^{l} \binom{n-m}{l-j}\binom{m}{j}(1-p)^{nl} \\
&\quad \times \left(\frac{1}{2^k}\left(1+\sum_{C\in S}(1-2p)^{\mu(j,C)} - 2^k(1-p)^{n-l}\right)\right)^n \\
&= \left[\frac{e^{-e^{-d}}}{2^{nk}}\left(1+o\left(\frac{\log^3 n}{\sqrt{n}}\right)\right)\right]\binom{n}{l}(1-p)^{nl}.
\end{aligned}$$

The superscript $\mu(j,C) = \sum_{s\in C} x_s - j_C$ where j_C is the number of zero columns in the subset of $\cup A_i$ indexed by C. The final line follows from the argument used on ϕ in (R3a). We then use (standard) inclusion-exclusion as in (R1). $\square$

(R3c) Thus from (16), (21), (22)

$$\Pr((A_1,...,A_k) \text{ is zero-sum } \mid \text{ No zero rows or columns }) = \frac{1}{2^{nk}}\left(1+o\left(\frac{\log^4 n}{\sqrt{n}}\right)\right).$$

7 The sharp threshold as $p \to 1$.

Let $p = 1 - (\log n + d(n))/n$, and $|d(n)| = o(\log\log n)$. Substitution of $q = 1-p$ into (8) gives

$$\begin{aligned}
\rho_m(0) &= \tfrac{1}{2}(1+(-1)^m(1-2q)^m) \\
\rho_m(1) &= \tfrac{1}{2}(1+(-1)^{m+1}(1-2q)^m),
\end{aligned} \tag{23}$$

which is the same as (8) provided m is even. Thus, we propose to imitate the previous arguments, substituting q for p.

(P1) A column of M is *unity* if it consists entirely of 1's. Trivial linear dependencies occur in the rows of M if two or more rows are unity, and similarly for the columns.

The number of unity columns is $B(n, p^n) = B(n, (1-q)^n)$. The total number of unity rows is asymptotically $Po(e^{-d})$ for constant d, by (R1) of the previous section. Let $\mathcal{U}$ be the event that at most one row and at most one column are unity. By an application of the techniques of (R1),

$$\Pr(\mathcal{U}) \sim \left(e^{-e^{-d}}(1+e^{-d})\right)^2.$$

(P2) Let $\mathcal{V}$ be the event that there are no unity rows or columns. Let $\boldsymbol{c} \in \{0,1\}^n$ be fixed vector, where $\boldsymbol{c}$ is $\mathbf{0}$, $\mathbf{1}$ or has $O(\log n)$ zeroes. Let $W(\boldsymbol{c})$ be the number of sets of columns of M adding to $\boldsymbol{c}$. We now show that the calculations of (R2) and (R3) are essentially unaltered and $\mathbf{E}\left((W(\boldsymbol{c}))_k \mid \mathcal{V}\right) \sim 1$.

Case of small sets, size $1 \le m \le \log n$

If $\boldsymbol{c} = \mathbf{0}, \mathbf{1}$, the evaluation of $\mathbf{E}W(\boldsymbol{c})$ leads to an analysis identical to that of $\mathbf{E}W_m$ in (R2), except we now condition on the number of rows, s, with at least two zeroes.

Let $\boldsymbol{c}$ have $k \ge 1$ fixed zeroes. Let m be odd, $m \ge 1$. Let $\theta = \max(k, m)$. The probability of the event that there exist m columns adding to $\boldsymbol{c}$ is at most

$$o(1) + \binom{n}{m} m^\theta q^\theta (1-q)^{(n-\Theta(m\log n))m} = o(1).$$

The first $o(1)$ is from (19), and the second term conditions on the event that the number of zero entries is at most $e^2 mnp$.

Case of sets size $m \sim n/2$

Let A be a column set of size m. Let $\psi(i)$ be the probability that A is i-sum in row s and that row s is not unity, then

$$\begin{aligned}
\psi(0) &= \tfrac{1}{2}\left(1 + (-1)^m (1-2q)^m\right) - (1-q)^n \, 1(m \text{ even}) \\
\psi(1) &= \tfrac{1}{2}\left(1 - (-1)^m (1-2q)^m\right) - (1-q)^n \, 1(m \text{ odd}).
\end{aligned}$$

In either case and for any $m \sim n/2$

$$\psi(i) = \tfrac{1}{2}\left(1 - \frac{e^{-d}}{n}(1+o(1))\right),$$

so that $\psi(i)$ has the same value as ϕ in (20) of (R3a), with $k = 1$. Thus $\mathbf{E}\left(W(\boldsymbol{c}) \mid \mathcal{V}\right) \sim 1$ irrespective of the value of $\boldsymbol{c}$. The generalization of these calculations to $\mathbf{E}(W)_k$ in (R3) follows naturally.

(P3) Suppose we condition on $\mathcal{U}$. Either $\mathcal{V}$ holds, or there is at least one unity row or column. If one of each (Case (C1)) let the row be $\boldsymbol{u}$, the column $\boldsymbol{v}$. Else (Case (C2)) let it be a unity row, $\boldsymbol{u}$, and choose a column $\boldsymbol{v}$ at random. Let M_1 be the $(n-1) \times (n-1)$-matrix obtained from M by deleting $\boldsymbol{u}, \boldsymbol{v}$.

In Case (C1) the matrix M_1 satisfies the property $\mathcal{V}$. In Case (C2), what is the probability that we have made another unity row by deleting $\boldsymbol{v}$? It is at most ϕ, the expected number of rows where the column $\boldsymbol{v}$ had the only zero entry in that row. But,

$$\phi = n(1-p)p^{n-1} = O\left(\frac{\log^2 n}{n}\right).$$

Thus with probability $1 - o(1)$ either the matrix M or the matrix M_1 has property $\mathcal{V}$. If M has $\mathcal{V}$, we have proved in (P2) that $\mathbf{E}\left((W)_k \mid \mathcal{V}\right) \sim 1$.

(P4) Suppose M_1 has $\mathcal{V}$. Let $\boldsymbol{v}_1$ be the restriction of $\boldsymbol{v}$ to the rows of M_1. Events in M_1 leading to a *possible* linear dependence in M are that a set of columns of M_1 adds to $\mathbf{0}$ or to $\boldsymbol{v}_1$. Such events are counted by the random variables $W(\mathbf{0})$ and $W(\boldsymbol{v}_1)$, evaluated over the columns of M_1.

The effect on $W(\mathbf{0})$ of adding back the row $\boldsymbol{u}$ is to restrict the evaluation of $\mathbf{E}W(\mathbf{0})$ to *even size* column sets $m = 2l$, as only even sets will add to zero in the row $\boldsymbol{u}$. Thus $\mathbf{E}(W(\mathbf{0}) \mid \mathcal{V}) \sim \frac{1}{2}$. Similarly, the effect on $W(\boldsymbol{v}_1)$ of adding back the row $\boldsymbol{u}$ is to restrict the evaluation of $W(\boldsymbol{v}_1)$ to odd size column sets $m = 2l + 1$, (because the entry of $\boldsymbol{v}$ in the row $\boldsymbol{u}$ is 1).

Let $W^*(\mathbf{0})$ be the evaluation of $W(\mathbf{0})$ on even column sets of M_1 and $W^*(\boldsymbol{v}_1)$ the evaluation of $W(\boldsymbol{v}_1)$ over odd size column sets of M_1. Let $Z = W^*(\mathbf{0}) + W^*(\boldsymbol{v}_1)$, then Z is the number of linear dependencies in the columns of M, and

$$\mathbf{E}\left(Z \mid M_1 \text{ has } \mathcal{V}\right) \sim \tfrac{1}{2} + \tfrac{1}{2} = 1.$$

(P5) To extend this argument to higher moments, we retain the definition of simple k-tuples of sets, $(C_1, ..., C_k)$, except now, some sets are zero-sum (denoted by A_j) and some are $\boldsymbol{v}_1$-sum (denoted by B_j). Set differences $A_1 \Delta A_2$, $A \Delta B$ or $B_1 \Delta B_2$ on these sets preserves the joint property '$\boldsymbol{v}_1$-sum or zero-sum'.

Consider row s of M_1. $(C_1, ..., C_k)$ defines a vector $\boldsymbol{c}(s) = (c_1, ..., c_k)$, where $c_i = 0$ if C_i is zero-sum and $c_i = v_{1s}$ if C_i is $\boldsymbol{v}_1$-sum. In the notation of Section 4 we now require that the intersection structure of $(C_1, ..., C_k)$ gives solutions satisfying $\boldsymbol{A}\boldsymbol{y} = \boldsymbol{c}(s)$ in each row s of M_1. The extension of Lemma 7, given by Lemma A6 of the Appendix ensures that the proofs of Section 4 and their extension to (R3) are intact.

Let $(C_1, ..., C_k) = (A_1, ..., A_j, B_1, ..., B_{k-j})$ and let $\mathbf{E}(Z(j))_k$ be the expectation of Z on simple k-tuples with exactly j zero-sum sets, and conditional on $\mathcal{V}$. Thus

$$\mathbf{E}(Z(j))_k \sim \left(\tfrac{1}{2}\right)^k,$$

and

$$\mathbf{E}(Z)_k = \sum_{j=0}^{k} \binom{k}{j} \mathbf{E}(Z(j))_k \sim 1,$$

as before.

8 Bibliography

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

[Cm] P. J. Cameron. *Combinatorics: Topics, Techniques, Algorithms.* Cambridge (1994)

[Du] R. Durrett. *Probability: Theory and Examples.* Wadsworth (1991).

[Ko] V. Kolchin. *Random graphs and systems of linear equations in finite fields.* Random structures and Algorithms 5(1) 135-146 (1994).

[Kn] D. E. Knuth. *The Art of Computer Programming.* Addison-Wesley (1973)

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

[vLM] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics.* Cambridge (1992)

[Pa] E. M. Palmer. *Graphical Evolution.* Wiley-Interscience (1985).

Appendix: Expected number of linear dependencies

The proof of Lemma 5(i) follows from (25), (34), (28), (30) and of Lemma 5(ii) from (26). The proof of Lemma 4 then follows from (31).

Let the field be *GF(t)*, where $t = o(\sqrt{\log n})$. Let $p = c/n$, $p \leq (t-1)/t$, where $c = \log n + \log(t-1) + d(n)$. We will prove here that for $d(n) \geq -o(\log\log n)$ there are **whp** no linear dependencies in the range $m(L) = \{\log n, ..., \frac{t-1}{t} n \left(1 - 4\sqrt{\frac{\log n}{n}}\right)\}$ or $m(U) = \{\frac{t-1}{t} n \left(1 + 4\sqrt{\frac{\log n}{n}}\right), n\}$. Furthermore, for $d(n) \to \infty$ there are no dependencies in the range $\{1, ..., \log n\}$. Let $\omega_1 \to \infty$ arbitrarily slowly. Let $m_0 = n/c^2$, and $m_i = n\frac{t-1}{t}(1 - \epsilon_i)$ for $i = 1, 2, 3$. Specifically let $m_1 = n\frac{t-1}{t}\left(1 - \frac{1}{\omega_1 \log n}\right)$, $m_2 = n\frac{t-1}{t}\left(1 - 4\sqrt{\frac{\log n}{n}}\right)$ and let $m_3 = n\frac{t-1}{t}\left(1 + 4\sqrt{\frac{\log n}{n}}\right)$.

We now investigate the behaviour of

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

<u>**Case of** $1 \leq m \leq n/c^2 = m_0$**.**</u>

The absolute value of the terms of $(1 - tp/(t-1))^m$ tends steadily to zero for any value of m in this interval, so

$$(1 - \frac{t}{t-1}p)^m \leq 1 - \frac{t}{t-1}mp + \left(\frac{t}{t-1}\right)^2 \frac{m^2p^2}{2}$$

by a standard property of alternating series. Thus $\rho_m \leq (1 - mp(1 - mp))$ and

$$\begin{aligned}
\mathbf{E}W_m &\leq \frac{1}{t-1}\frac{(n(t-1))^m}{m!}\exp -nmp(1-mp) \\
&= \frac{1}{t-1}\frac{(e^{-d(n)+1})^m}{m!}. \qquad (24)
\end{aligned}$$

Thus, when $d(n) \geq -o(\log\log n)$

$$\sum_{m=\log n}^{m_0} \mathbf{E}W_m = o(1/n^2), \qquad (25)$$

and when $d(n) = \omega$

$$\sum_{1}^{m_0} \mathbf{E}W_m = O\left(e^{-\omega}\right). \qquad (26)$$

Case of $m_1 \leq m \leq n$

We note that $f(m,p) = \left(1 + (t-1)\left(1 - \frac{t-1}{t}p\right)^m\right)^n$ tends rapidly to 1 as $d(n) \to \infty$. If $d(n) \geq 3\log n$ then $1 \leq f(m,p) \leq 1 + o(1/n)$ so we consider the case $-o(\log\log n) < d(n) < 3\log n$ in most detail.

Write $m = n(1-\epsilon)(t-1)/t$,

$$\begin{aligned}
\rho_m(0) &= \frac{1}{t}\left(1 + (t-1)(1 - \frac{t}{t-1}p)^m\right) \\
&= \frac{1}{t}\left(1 + (t-1)\exp -c(1-\epsilon) + O(np^2)\right) \\
&= \frac{1}{t}\left(1 + \frac{1}{n}e^{-d(n)+c\epsilon(1+o(1))}\right). \qquad (27)
\end{aligned}$$

Thus,

$$\rho_m^n = \frac{1}{t^n}\left(e^{e^{-d+c\epsilon(1+o(1))}}\right),$$

and

$$\begin{aligned}
\sum_{m_1}^{m_2} \mathbf{E}W_m &= \frac{1}{t-1}\sum_{m=m_1}^{m_2}\binom{n}{m}\frac{(t-1)^m}{t^n}\left(e^{e^{-d+c\epsilon(1+o(1))}}\right) \\
&\leq \frac{1}{t-1}\left(e^{e^{-d+c\epsilon_1(1+o(1))}}\right)e^{-(\epsilon_2)^2\,\frac{t-1}{3t}n} \\
&= o\left(\frac{1}{n^{4/3}}\right). \qquad (28)
\end{aligned}$$

This will follow because the Binomial random variable $X \sim B(n,(t-1)/t)$ is sharply concentrated around the mean $\mu = n(t-1)/t$. Thus

$$\Pr\left(|X - \mu| > \delta\mu\right) \leq 2\exp -\frac{\delta^2\mu}{3}, \qquad (29)$$

by the Hoeffding inequality (see eg [Pa] p136). Let $\delta = \epsilon_2$. It is also an immediate consequence that

$$\sum_{m_3}^{n} \mathbf{E}W_m = o(1/n^2). \tag{30}$$

Finally

$$\sum_{m_2}^{m_3} \mathbf{E}W_m = \begin{cases} \frac{1}{t-1}\exp\left(e^{-d} + o\left(\frac{\log^{5/2} n}{\sqrt{n}}\right)\right) & d > -o(\log\log n) \\ \frac{1}{t-1}(1+e^{-\omega})(1+o(1)) & d(n) = \omega \to \infty \\ \frac{1}{t-1}(1+o\left(\frac{1}{n}\right)) & d(n) \geq 3\log n \end{cases} \tag{31}$$

Case of $m_0 \leq m \leq m_1$.

We will show that $\mathbf{E}W_m$ is a decreasing function of m, up to $m = \frac{1}{2}n\frac{\log c}{c}\frac{t-1}{t}$ and an increasing function of m for $2n\frac{\log c}{c}\frac{t-1}{t} \leq m \leq m_1$. Thus

$$\sum_{m_0}^{m_1} \mathbf{E}W_m \leq n \max\{\mathbf{E}W_{m_0}, \mathbf{E}W_{m_1}, \mathbf{E}W_{m^*}\} \tag{32}$$

where $m^* \in \{bn\frac{\log c}{c}\frac{t-1}{t}$ and $\frac{1}{2} \leq b \leq 2\}$.

Let $\Delta = \frac{t}{t-1}p$. If $R = (\mathbf{E}W_{m+1})/(\mathbf{E}W_m)$ we see that

$$\begin{aligned} R &= \frac{n-m}{m+1}(t-1)\left(1 - \frac{(t-1)\Delta(1-\Delta)^m}{1+(t-1)(1-\Delta)^m}\right)^n \\ &\leq \frac{n-m}{m+1}t\ \exp -(t-1)n\Delta\left(\frac{\exp -m\Delta/(1-\Delta)}{1+(t-1)\exp -m\Delta}\right) \\ &\leq \frac{n-m}{m+1}t\ \exp -ntp\left(\frac{\exp -\left(\frac{t}{t-1}mp(1+O(p))\right)}{1+(t-1)\exp -\left(\frac{t}{t-1}mp\right)}\right) \end{aligned}$$

by repeated application of $\exp -x/(1-x) \leq 1-x \leq \exp -x$.

Let $m = bn\frac{\log c}{c}\frac{t-1}{t}$ where $1/(c\log c) < b < c/(\log c)$. Then $m\Delta = b\log c$ and

$$R \leq \frac{n-m}{m+1}t\ \exp -\left(\frac{tc^{1-b(1+O(p))}}{1+(t-1)c^{-b}}\right).$$

Thus provided $b \leq 1/2$ then $R < 1$ and $\mathbf{E}W_m$ is decreasing.

We now consider $b \geq 2$.

$$\begin{aligned} R &\geq \frac{n-m}{m+1}(t-1)\exp -\left(\frac{ntpe^{-m\Delta/(1-\Delta)}}{1+(t-1)e^{-m\Delta} - tpe^{-m\Delta/(1-\Delta)}}\right) \\ &\geq \frac{n-m}{m+1}(t-1)\exp\left(-\frac{t}{c^{b-1}}(1-o(1))\right). \end{aligned}$$

Thus $R \geq 1$ for $2n\frac{\log c}{c}\frac{t-1}{t} \leq m \leq m_1$ and $\mathbf{E}W_m$ is increasing in this range.

To evaluate $\mathbf{E}W_{m^*}$ we note that, $\binom{n}{m} \leq (ne/m)^m$, so

$$\mathbf{E}W_m \leq \left(\frac{ne(t-1)}{m}\right)^m \frac{1}{t^n} \exp\left(n(t-1)e^{-m\Delta}\right).$$

When $m = m^* = nb\frac{logc}{c}\frac{t-1}{t}$,

$$(\mathbf{E}W_m)^{1/n} \leq \left(\frac{tec}{b\log c}\right)^{\frac{t-1}{t}\frac{b\log c}{c}} \left(\frac{1}{t}\right) \exp\left((t-1)c^{-b}\right).$$

Taking logarithms, the right hand side is

$$-\log t + O\left(b\frac{\log^2 c}{c} + \frac{t}{c^b}\right) \leq -\tfrac{1}{2}\log t,$$

because, as $t = o(\sqrt{\log n})$, $-\log t$ is the dominant term.

We now consider $\mathbf{E}W_{m_1}$.

$$\mathbf{E}W_{m_1} \leq (1 + (t-1)(1-\Delta)^{m_1})^n \Pr(X \leq m_1)$$

where $X \sim B(n, (t-1)/t)$ is a Binomial random variable. Now

$$\begin{aligned}(1 + (t-1)(1-\Delta)^{m_1})^n &\leq \exp\left((t-1)n \exp -m_1\Delta\right) \\ &\leq \exp\left(2(t-1)n^{\frac{1}{\omega_1 \log n}} e^{-d(n)}\right).\end{aligned}$$

So from (29) with $d(n) \geq -o(\log\log n)$

$$\mathbf{E}W_{m_1} \leq 2\exp\left(o(t\log n) - \frac{n}{6(\omega_1 \log n)^2}\right) \tag{33}$$

Finally

$$\sum_{m_0}^{m_1} \mathbf{E}W_m = o(1/n^2) \tag{34}$$

from (32) using (24), (33), and because $\mathbf{E}W_{m^*} = O(t^{-n/2})$.

Appendix: Proof of Lemma 7

If column j of row i of $\boldsymbol{A}$ has $a_{ij} = 1$ this means the set A_i is uncomplemented in the intersection I_j. The columns of $\boldsymbol{A}$ are exactly the $(2^k - 1)$ distinct non-zero vectors of length k. Thus the rank of $\boldsymbol{A}$ is k.

Let $\mathcal{L}$ be the k-dimensional vector space generated by the rows $(\boldsymbol{r}_1, ..., \boldsymbol{r}_k)$ of $\boldsymbol{A}$. An element $\boldsymbol{e}$ of $\mathcal{L}$ can be written as $\boldsymbol{e} = c_1\boldsymbol{r}_1 + \cdots + c_k\boldsymbol{r}_k$ where $c_i \in \{0, 1\}$, or as $\boldsymbol{e} = (e_j,\ j = 1, ..., L)$. Associated with $\boldsymbol{e}$ are two sets of indices. The set $R(\boldsymbol{e}) = \{i : c_i = 1\}$, the indices of the selected sets A_i (rows of $\boldsymbol{A}$), and $C(\boldsymbol{e}) = \{j : e_j \equiv 1 (\mathrm{mod}\ 2)\}$, the indices of the subsets I_j (columns of $\boldsymbol{A}$) with non-zero entries in $\boldsymbol{e}$.

Lemma A 1 *Let* $S = \{C(\boldsymbol{e}) : \boldsymbol{e} \in \mathcal{L}\}$*.*

(i) $|S| = 2^k - 1$.

(ii) Let $C(\boldsymbol{e}) \in S$*. The vector* $\boldsymbol{e} = c_1\boldsymbol{r}_1 + \cdots + c_k\boldsymbol{r}_k$ *which has* $R(\boldsymbol{e}) = \{i_1, ..., i_s\}$ *corresponds to the zero-sum column set*

$$B = A_{i_1} \Delta A_{i_2} \Delta \cdots \Delta A_{i_s}.$$

Proof (i) There are $2^k - 1$ distinct non-zero linear combinations $\boldsymbol{e}$ of the rows of $\boldsymbol{A}$, giving $2^k - 1$ distinct sets of column indices $C(\boldsymbol{e})$.

(ii) This is because

$$I_j \subset B \iff \sum_{i \in R(\boldsymbol{e})} a_{ij} \equiv 1 (\mathrm{mod}\ 2) \iff e_j = 1.$$

Thus $B = \cup_{j \in C(\boldsymbol{e})} I_j$ and B is zero-sum. □

This completes the proof of Lemma 7(iv)

Let $T = \{\boldsymbol{y} : \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0}\}$. Let $J = \{j_1, ..., j_s\}$. Say a solution $\boldsymbol{y} \in T$ is even on J, if $y_{j_1} + \cdots + y_{j_s} = 0$, and odd (on J) otherwise. Let $S = S(J) = \{\boldsymbol{y} \in T : \boldsymbol{y}$ is even on $J\}$.

Lemma A 2 *Either* $S = T$ *or* $|S| = \frac{1}{2}|T|$*.*

Proof We note that T is a group under vector addition. Now $\boldsymbol{0} \in S$ and S is closed under addition so S is a subgroup of T. If $\boldsymbol{y}, \boldsymbol{y}' \in T$, the cosets $\boldsymbol{y} + S,\ \boldsymbol{y}' + S$ are equal if and only if $(\boldsymbol{y} - \boldsymbol{y}') \in S$. This occurs if $\boldsymbol{y}, \boldsymbol{y}'$ are both even on J or both odd on J. If $\boldsymbol{y}$ is any odd solution, $\boldsymbol{y} + S$ is the unique odd coset so that $|S| = |\boldsymbol{y} + S|$ and $S \cup (\boldsymbol{y} + S) = T$. □

Lemma A 3

$$\textit{If } S = T \textit{ then } \sum_{\boldsymbol{y} \in T} (-1)^{y_{j_1} + \cdots + y_{j_s}} = |T|.$$

$$\textit{If } S \neq T \textit{ then } \sum_{\boldsymbol{y} \in T} (-1)^{y_{j_1} + \cdots + y_{j_s}} = \tfrac{1}{2}|T| - \tfrac{1}{2}|T| = 0.$$

We now consider the existence of odd solutions. For now, let us assume that no set I is empty.

Lemma A 4 *Let* $T = \{\boldsymbol{y} : \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0}\}$. *Let* $J = \{j_1, ..., j_s\}$. T *has odd solutions on* J *if and only if* $J \neq C(\boldsymbol{e})$ *for some* $\boldsymbol{e} \in \mathcal{L}$ *the row-space of* $\boldsymbol{A}$.

Proof Let $J = \{j_1, ..., j_s\}$, and let $\boldsymbol{\alpha} = (\alpha_j : j = 1, ..., L)$ where

$$\alpha_j = \begin{cases} 1 & j \in J \\ 0 & j \in L \setminus J \end{cases}$$

then $\boldsymbol{y}$ is an even solution on J iff

$$\boldsymbol{a}\boldsymbol{y} = 0 \iff y_{j_1} + \cdots + y_{j_s} = 0.$$

Let $\boldsymbol{A}^* = \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{\alpha} \end{bmatrix}$ and $R = \{\boldsymbol{w} : \boldsymbol{A}^*\boldsymbol{w} = \boldsymbol{0}\}$, so that $R \subseteq T$. Using the rank and nullity theorem,

$$\begin{aligned} \dim(T) &= L - \operatorname{rank}(\boldsymbol{A}) = L - k \\ \dim(R) &= L - \operatorname{rank}(\boldsymbol{A}^*). \end{aligned}$$

If $\boldsymbol{\alpha} = \boldsymbol{e}$ for some $\boldsymbol{e} \in \mathcal{L}$ the row-space of $\boldsymbol{A}$, then $\operatorname{rank}(\boldsymbol{A}) = \operatorname{rank}(\boldsymbol{A}^*)$ and $R = T$.

If $\boldsymbol{\alpha} \notin \mathcal{L}$ then $\operatorname{rank}(\boldsymbol{A}^*) = \operatorname{rank}(\boldsymbol{A}) + 1$ and $|R| < |T|$. Any $\boldsymbol{y} \in T \setminus R$ satisfies $\boldsymbol{\alpha}\boldsymbol{y} = 1$, an odd solution. □

What if some sets $I = \emptyset$?

Lemma A 5 *If* $0 \leq i \leq L - k$ *sets* I *are empty,*

(i) $|T| = 2^{L-k-i}$

(ii) *Let* $S = \{C(\boldsymbol{e}) : \boldsymbol{e} \in \mathcal{L}\}$ *then* $|S| = 2^k - 1$

Proof Let i sets be empty. We delete the corresponding columns of $\boldsymbol{A}$ so that $\boldsymbol{A}$ is now a $k \times (L - i)$-matrix. We claim that the row-space of $\boldsymbol{A}$ still has dimension k. Recall that $(A_1, ..., A_k)$ is simple iff

$$A_{i_1} \Delta ... \Delta A_{i_l} \neq \emptyset \qquad (1 \leq l \leq k).$$

Let $\boldsymbol{e} = \boldsymbol{r}_{i_1} + \cdots + \boldsymbol{r}_{i_l}$. As $A_{i_1} \Delta ... \Delta A_{i_l} \neq \emptyset$ then $C(\boldsymbol{e}) \neq \emptyset$ so that $\boldsymbol{e} \neq \boldsymbol{0}$. Thus the rows are linearly independent.

The solution space now has dimension $L-k-i$ where $0 \leq i \leq L-k$. $\square$

This completes the proof of Lemma 7(i),(ii),(iii).

In order to prove Theorem 2(ii) as $p \to 1$, we need to consider a more general form of Lemma 7(iii), which we now state.

Lemma A 6 *Let $\boldsymbol{c} \in \{0,1\}^k$. Let $T(\boldsymbol{c}) = \{\boldsymbol{x} : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{c}\}$. Let*

$$\lambda(J, \boldsymbol{c}) = \sum_{\boldsymbol{x} \in T(\boldsymbol{c})} (-1)^{\sum_{j \in J} x_j},$$

then

$$\lambda(J, \boldsymbol{c}) = \begin{cases} 0 & J \notin S \\ (-1)^{\xi}|T| & J \in S \end{cases}$$

where $\xi \in \{0,1\}$.

Proof Let $\boldsymbol{z} = (z_i : i = 1, ..., k)$ be a specific solution of $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{c}$ so that $T(\boldsymbol{c}) = T + \boldsymbol{z}$. Then

$$\begin{aligned} \lambda(J, \boldsymbol{c}) &= \sum_{\boldsymbol{x} \in T(\boldsymbol{c})} (-1)^{\sum_{j \in J} x_j} \\ &= \sum_{\boldsymbol{y} \in T} (-1)^{\sum_{j \in J} (y_j + z_j)} \\ &= (-1)^{\sum_{j \in J} z_j} \sum_{\boldsymbol{y} \in T} (-1)^{\sum_{j \in J} y_j}. \end{aligned}$$

The result now follows from the standard form of Lemma 7. $\square$