A note on the rank of a sparse random matrix

Colin Cooper* Alan Frieze† Wesley Pegden‡

November 21, 2019

Abstract

Let $\mathbf{A}_{n,m;k}$ be a random $n \times m$ matrix with entries from some field $\mathbb{F}$ where there are exactly k non-zero entries in each column, whose locations are chosen independently and uniformly at random from the set of all $\binom{n}{k}$ possibilities.

In a previous paper (arXiv:1806.04988), we considered the rank of a random matrix in this model when the field is $\mathbb{F} = GF(2)$. In this note, we point out that with minimal modifications, the arguments from that paper actually allow analogous results when the field $\mathbb{F}$ is arbitrary.

In particular, for any field $\mathbb{F}$ and any fixed $k \geq 3$, we determine an asymptotically correct estimate for the rank of $\mathbf{A}_{n,m;k}$ in terms of c, n, k where $m = cn/k$, and c is a constant. This formula works even when the values of the nonzero elements are adversarially chosen. When $\mathbb{F}$ is a finite field, we also determine the threshold for having full row rank, when the values of the nonzero elements are randomly chosen.

1 Introduction

Let $\mathbf{A} = \mathbf{A}_{n,m;k}$ be the $n \times m$ matrix with entries from some field $\mathbb{F}$ where there are exactly $k \geq 3$ non-zero entries in each column, the other entries being zero. The locations of the non-zeros of the columns are chosen independently and uniformly at random from the set of all $\binom{n}{k}$ possibilities. Given the locations of non-zeros, one can consider various models for the choice of their values (e.g., random, fixed choice, adversarial, *etc.*).

The rank of this matrix model has attracted some recent attention. In a previous paper, we analyzed the case where $\mathbb{F}_2 = GF(2)$ [5]. Ayre, Coja-Oghlan, Gao, and Müller [1] independently obtained the same result as [5] independent for any finite field $\mathbb{F}_q$. Of course in $\mathbb{F}_2$, there is no choice of how to select the non-zero elements; in [1], the requirement was that the list of k non-zero values from $\mathbb{F}^+ = \mathbb{F} \setminus \{0\}$ in each column is chosen independently from a fixed distribution which is symmetric with respect to permutation of the k positions.

Coja-Oghlan and Gao [3] considered the more general case of a sparse random matrix over a finite field $\mathbb{F}_q$ where both the the columns and rows are given prescribed numbers of non-zeros (which may also be random); Coja-Oghlan, Ergr, Hetterich and Rolvienhref [2] extended the results of [3] to arbitrary fields. For both of these results, all non-zero elements are required to be chosen independently from a fixed distribution (giving

*Research supported in part by EPSRC grant EP/M005038/1
†Research supported in part by NSF Grant DMS1661063
‡Research supported in part by NSF grant DMS1363136

a permutation-symmetric distribution on the lists of k non-zeros). One remarkable feature of all these results is that the asymptotic formulae do not depend on the choice of field $\mathbb{F}$.

The point of the present note is simply to demonstrate that our arguments from the previous paper [5] generalize beyond $GF(2)$. Our arguments go beyond the results of [1] in this setting also, since our purely combinatorial argument applies even when there are no restrictions on the process of choosing the values of the non-zero elements for each column—they can even be chosen adversarially once all the locations of the non-zeros have already been randomly chosen. Thus the proof strategy used in [5] allows a purely combinatorial proof strategy for the asymptotic rank of $\mathbf{A}_{n,m;k}$ for general fields, which is also considerably shorter than the more algebraic methods used in [1].

To state our result, let $H = H_{n,m;k}$ denote the random k-uniform hypergraph with vertex set $[n]$ and m random edges taken from $\binom{[n]}{k}$. There is a natural surjection from $\mathbf{A}_{n,m;k}$ to $H_{n,m;k}$ in which column $\mathbf{c}$ is replaced by the set $\{i : \mathbf{c}_i \neq 0\}$. The ρ-core of a hypergraph H (if it is non-empty) is the maximal set of vertices that induces a sub-hypergraph of minimum degree ρ. The 2-core $C_2 = C_2(H)$ plays an important role in our theorem. Parametrizing $m = cn/k$, let c_k be the threshold in c for the emergence of a 2-core. We state our theorem in terms of functions $\Phi(c)$ and $\Psi(c)$ of c, defined precisely in Section 2.1, which are asymptotic proxies for the ratios $|V(C_2)|/n$ and $|E(C_2)|/n$, respectively.

Theorem 1. *Given constants c and $k \geq 3$, we have that if $m = cn/k$, then w.h.p.*

$$\mathit{rank}(\mathbf{A}_{n,m;k}) \approx \begin{cases} \frac{cn}{k} & c \leq c_k \\ n\left(\frac{c}{k} - \Psi(c) + \Psi(c_k) + \Phi(c) - \Phi(c_k)\right) & c > c_k, \end{cases}$$

even if the values of the non-zero elements in $\mathbf{A}_{n,m;k}$ are chosen adversarially after their locations are determined.

The notation $X_n \approx Y_n$ indicates that $\lim_{n\to\infty} X_n/Y_n = 1$.

We will also consider the threshold for full row rank. For this we will restrict out attention to finite fields and assume that the non-zeros are randomly chosen.

Theorem 2. *Let $m = n(\log n + c)/k$ where $c = c_n$ and let $\mathbb{F}_q$ be a field with q elements. Suppose that the non-zeros of $\mathbf{A}$ are chosen independently and uniformly at random from $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Then*

$$\lim_{n\to\infty} \mathbb{P}(\mathit{rank}(\mathbf{A}) = n) = \begin{cases} 0 & c_n \to -\infty. \\ e^{-e^{-c}} & c_n \to c. \\ 1 & c_n \to +\infty. \end{cases} \tag{1}$$

We emphasize that Theorems 1 and 2 are proved essentially the same way as the more restrictive theorems from [5]. For the convenience of the reader, we give the complete proofs in this note, including parts which are unchanged from [5].

2 Proof of Theorem 1

2.1 The 2-core

We will use some results on the 2-core of random hypergraphs. In random graphs $G_{n,m} = H_{n,m;2}$ the 2-core grows gradually with m following the emergence of the first cycle. For $k \geq 3$, the 2-core is either empty or of linear size and emerges around some threshold value m_k.

The typical asymptotic values of $|V(C_2)|, |E(C_2)|$ can be found in Cooper [4] and Molloy [9]. In particular, to describe the size of the 2-core, we parameterise m as $m = cn/k$, $c = O(1)$ and consider the equation

$$x = (1 - e^{-cx})^{k-1}. \tag{2}$$

For $k \geq 3$, define c_k by

$$c_k = \min \left\{ c : x = (1 - e^{-cx})^{k-1} \text{ has a solution } x_c \in (0, 1] \right\}.$$

It is known that $c < c_k$ implies that $C_2 = \emptyset$ w.h.p. If $c > c_k,\ c = O(1)$, let x_c be the largest solution to (2) in $[0, 1]$. Let

$$\Phi(c) = x_c^{1/(k-1)} - cx_c + cx_c^{k/(k-1)}.$$
$$\Psi(c) = \frac{cx_c^{k/(k-1)}}{k}.$$

Then q.s.[1] if $c > c_k$ then

$$\big| |V(C_2)| - n\Phi(c) \big| \leq n^{3/4}, \tag{3}$$
$$\big| |E(C_2)| - n\Psi(c) \big| \leq n^{3/4}. \tag{4}$$

2.2 Matrix Rank

We let $c = km/n$ and H_i denote the hypergraph induced by the first i columns of $\mathbf{A}$.

The first step of our proof is to "peel off" edges of the hypergraph H_m, and thus columns of the matrix $\mathbf{A}$, containing vertices of degree 1.

In particular, so long as H_i contains a vertex v_i of degree 1, then for the edge $e_i \ni v_i$ in H_i, we set

$$E(H_{i-1}) = E(H_i) \setminus \{e_i\}$$
$$V(H_{i-1}) = V(H_i) \setminus \{v \in e_i \mid \deg_{H_i}(x) = 1\}.$$

In a corresponding sequence $\{\mathbf{A}_i\}$ beginning from $\mathbf{A}_m$, we obtain $\mathbf{A}_{i-1}$ from $\mathbf{A}_i$ by removing the column $\mathbf{c}_i$ corresponding to e_i, and the (at least one) rows whose only 1's were in that column. Note that up until the point where every row has at least two non-zeros, we have

$$\text{rank}(\mathbf{A}_i) = \text{rank}(\mathbf{A}_{i-1}) + 1.$$

This recursion terminates at

$$\mathbf{C}_2 = \mathbf{A}_{m_2}, \tag{5}$$

where $m_2 = m - m_1$ is the number of edges in the the 2-core of the hypergraph H, and moreover, we have that H_{m_2} is precisely the 2-core of H. Thus we have that

$$\text{rank}(\mathbf{A}_m) = |E(H)| - |E(C_2)| + \text{rank}(\mathbf{C}_2). \tag{6}$$

[1]A sequence $\mathcal{E}_n$ of events occurs *quite surely* (q.s.) if $\mathbb{P}(\neg\mathcal{E}_n) = O(n^{-C})$ for any constant $C > 0$.

Let $\widehat{C}$ denote the first 2-core i.e. the 2-core when $c \approx c_k$ and let $\widehat{\mathbf{C}}$ denote the corresponding set of columns of $\mathbf{A}$. When $c = c_k$ we have that $\text{rank}(\mathbf{A}) \approx |E(H)|$ which equals the number of edges not in C_2 plus the rank of $\mathbf{C}_2$. This implies that the rank of $\widehat{\mathbf{C}}$ is asymptotic to the number of edges in $\widehat{C}$ i.e. $|E(\widehat{C})| \approx n\Psi(c_k)$ w.h.p. To prove Theorem 1, we will argue that the rank of $\mathbf{C}_2$ increases along with the increase in the number of vertices in C_2. I.e. that w.h.p.

$$\begin{aligned} \text{rank}(\mathbf{C}_2) &\approx \text{rank}(\widehat{\mathbf{C}}) + |V(C_2)| - |V(\widehat{C})| && (7) \\ &\approx n(\Psi(c_k) + \Phi(c) - \Phi(c_k)) && (8) \end{aligned}$$

This together with (6) proves Theorem 1.

We need some basic facts about hypergraphs. We say a hypergraph H is *linear* if edges only intersect in at most one vertex. We define a k-uniform *cactus* as follows. A single edge is a cactus. An $(\ell+1)$-edge cactus C' is the structure obtained from an ℓ-edge cactus C with vertex set $V(C), |V(C)| = (k-1)\ell + 1$ as follows. Choose $x \in V(C)$ and let $V(C') = V(C) \cup \{v_1, ...v_{k-1}\}$ where $\{v_1, ...v_{k-1}\}$ is disjoint from $V(C)$. The edge set $E(C')$ of C' is $E(C) \cup \{e'\}$ where $e' = \{x, v_1, ...v_{k-1}\}$. We need the following simple lemma.

Lemma 3. *A connected k-uniform simple hypergraph C with no cycles is a cactus.*

Proof. This can easily be verified by induction. We simply remove one terminal edge $e = \{v_1, v_2, \ldots, v_k\}$ of a longest path P. We can assume here that $v_2, \ldots, v_k$ are all of degree one, else P can be extended. Deleting e gives a new connected hypergraph C' which is a cactus by induction. □

For a k-uniform linear hypergraph H let $L(H) = (k-1)|E(H)| + 1$.

Lemma 4. *Let H be a connected k-uniform linear hypergraph.*

(a) $|V(H)| \leq L(H)$.

(b) $|V(H)| = L(H)$ if and only if H does not contain any cycles.

(c) By deleting at most $L(H) - |V(H)|$ edges we can create a subgraph H' with $V(H') = V(H)$ and no cycles.

Proof. We consider two cases:
Case 1: H contains no cycles.
In this case, we consider a longest path of edges in H; that is consider a longest sequence $e_1, e_2, \ldots, e_\ell$ such that for each $1 < i < e_\ell$, e_i intersects e_{i-1}, e_{i+1}, and no other edges in the sequence. Since the path is longest and H has no cycles, we know that e_ℓ intersects no edge in H other than $e_{\ell-1}$.

In particular, we define a hypergraph H' with $E(H') = E(H) \setminus \{e_\ell\}$ and $V(H') = V(H) \setminus (e_\ell \setminus e_{\ell-1})$. H' has one fewer edge and $k-1$ fewer vertices than H, so we have $L(H) = |V(H)|$ by induction, proving the Lemma for this case.
Case 2: H contains a cycle C.
In this case, we consider an edge e in a cycle C of H. Removing the edge e leaves a hypergraph on the same vertex set with one fewer edge and with at most $k-1$ connected components (counting isolated vertices as connected components). Applying the Lemma inductively to each component, we see that the sum of $L(H_i)$ over the $(k-1)$ components H_i of $H \setminus e$ satisfies

$$\sum_{i=1}^{k-1} L(H_i) \leq L(H) - (k-1) + (k-2) \leq L(H) - 1,$$

since removing e decreases the sum by $k-1$, while the additive term in the definition of $L(H)$ inflates the sum by at most $(k-2)$ (as the number of components has increased by up to $k-2$). On the other hand we of course have

$$\sum_{i=1}^{k-1} |V(H_i)| = |V(H)|.$$

We now apply parts (a) and (c) of the Lemma to each component by induction, and conclude that the Lemma does hold for H. $\square$

In the following lemma we prove a property of $H_{n,m;k}$. It will be more convenient to work with $H_{n,p;k}$ where $m = \binom{n}{k}p$. We use the fact that for any hypergraph property $\mathcal{H}$ that is monotone increasing or decreasing with respect to adding edges,

$$\mathbb{P}(H_{n,m;k} \in \mathcal{H}) \le O(1)\mathbb{P}(H_{n,p;k} \in \mathcal{H}). \tag{9}$$

This is well-known for graphs and is essentially a property of the binomial random variable, $E(H_{n,p;k})$, the number of edges of $H_{n,p;k}$.

Similarly, if $\mathcal{A}$ is a matrix property that is monotone increasing or decreasing with respect to adding columns, then

$$\mathbb{P}(\mathbf{A}_{n,m;k} \in \mathcal{A}) \le O(1)\mathbb{P}(\mathbf{A}_{n,p;k} \in \mathcal{A}). \tag{10}$$

Lemma 5. *Suppose that $m = O(n)$.*

(a) Let $\alpha < 1$ be a positive constant. With probability $1 - o(n^{-1})$, for every set of vertices S of size $\ell_0 = \log^{1/2} n \le s \le s_0 = n^{1-\alpha}$ we have that $L(S) \le s + \lfloor \theta s \rfloor$, where $\theta = \frac{1}{\log^{1/4} n}$. Here $H[S]$ is the hypergraph of edges belonging completely to S.

(b) Then w.h.p., there are at most $n^{o(1)}$ vertices in cycles of size at most $\log^{1/2} n$.

Proof. (a) We can use (9) here with $p = \frac{C}{n^{k-1}}$ for some $C = O(1)$ satisfying $m = \binom{n}{k}p$. Let $s_1 = s + \lfloor \theta s \rfloor + 1$. The expected number of sets failing this property can be bounded by

$$\begin{aligned}
&\sum_{s=\ell_0}^{s_0} \binom{n}{s} \sum_{L \ge s_1} \binom{\binom{s}{k}}{L/(k-1)} \left(\frac{C}{n^{k-1}}\right)^{L/(k-1)} \\
&\le \sum_{s=\ell_0}^{s_0} \left(\frac{ne}{s}\right)^s \sum_{L \ge s_1} \left(\frac{Ces^k(k-1)}{k!Ln^{k-1}}\right)^{L/(k-1)} \\
&\le \sum_{s=\ell_0}^{s_0} \sum_{L \ge s_1} (Ce^2)^L \left(\frac{s}{n}\right)^{L-s} \left(\frac{s}{L}\right)^{L/(k-1)} \\
&\le \sum_{s=\ell_0}^{s_0} \sum_{L \ge s_1} \left((Ce^2)\left(\frac{s}{n}\right)^{1-s/L}\right)^L
\end{aligned} \tag{11}$$

Let $u_{s,L}$ denote the summand in (11). Then we have

$$u_{L,s} \le \left((Ce^3)^{2\alpha^{-1}} \left(\frac{s}{n}\right)^{\theta}\right)^s \le n^{-(\alpha - o(1))\theta s} \qquad L \le 2\alpha^{-1}s.$$

$$u_{L,s} \le \left((Ce^3)\left(\frac{s}{n}\right)^{1-\alpha/2}\right)^L \le n^{-(1-o(1))\alpha L/2} \qquad L > 2\alpha^{-1}s.$$

Thus,

$$
\begin{aligned}
\sum_{s \ge \ell_0} \sum_{L \ge s_1} u_{s,L} &\le \sum_{s=\ell_0}^{s_0} \sum_{L=s+\lceil \theta s \rceil}^{2\alpha^{-1}s} n^{-(\alpha - o(1))\theta s} + \sum_{s=\ell_0}^{s_0} \sum_{L \ge 2\alpha^{-1}s} n^{-(1-o(1))\alpha L/2} \\
&\le 2\alpha^{-1} s_0 \sum_{s=\ell_0}^{s_0} n^{-(\alpha-o(1))\theta s} + \sum_{s=\ell_0}^{s_0} n^{-(1-o(1))s/2} \\
&= o(n^{-1}). \qquad (12)
\end{aligned}
$$

(b) The expected number of vertices in small cycles can be bounded by

$$
\sum_{\ell=2}^{\log^{1/2} n} \binom{n}{(k-1)\ell} ((k-1)\ell)! p^\ell \le \sum_{\ell=2}^{\log^{1/2} n} (n^{k-1}p)^\ell \le \sum_{\ell=2}^{\log^{1/2} n} C^\ell = n^{o(1)}.
$$

Part (b) now follows from the Markov inequality. $\square$

2.3 Growth of the mantle

We now consider the change in the rank of the sub-matrix $\mathbf{C}_2$ of the edge-vertex incidence matrix $\mathbf{A}_m$ (see (5)) corresponding to the 2-core of the column hypergraph, caused by adding a column to $\mathbf{A}_m$. We will show that w.h.p. the rank of $\mathbf{C}_2$ grows by the increase in the size of $V(C_2)$, up to error terms that total $o(n)$ overall. At "time" $c < c_k$ the rank of $\mathbf{A}$ is equal to the number of edges in H which is equal to the number of edges not in the empty 2-core. At c_k, C_2 jumps in size, but the rank can only change by at most one per edge/column. Thus at c_k, the rank of C_2 must be asymptotically equal to $|E(\widehat{C})|$. We now have to show that the rank of C_2 grows by the increase in the size of $V(C_2)$.

Assume now that $c > c_k$ so that $|V(C_2)| = \Omega(n)$ q.s. Suppose now that the addition of e increases the size of the 2-core. Let A denote the set of additional vertices and F denote the set of additional edges added to C_2 by the addition of e, where $A \subset V(F)$. We include e in F.

We remark first that with c, x_c as in (2), then (3) and (4)imply that adding an edge to $\mathbf{A}_m$ can only increase $|V(C_2)|$, $|E(C_2)|$ by at most $O(n^{3/4})$. We use Lemma 5 with $\alpha = 3/4$ in our discussion of the hypergraph F.

Obviously the increase in rank from adding F to the 2-core is bounded above by the size of the vertex-set A. To bound it from below, we proceed as follows: in what follows we include a pair of edges e, f such that $|e \cap f| \ge 2$ as determining a cycle.

Case 1: First consider the case where there are no cycles in F. We will show that the rank increases by precisely the number of new vertices.

Let $|A| = k$. We will define an ordering $a_1, \dots, a_k$ of A and a corresponding ordering $f_1, \dots, f_k$ of a subset of F. To begin, we claim there must exist $v \in A$ and $v \in f \in F$, $f \ne e$, such that $f \setminus \{v\} \subseteq C_2$. For this consider a longest path $e_1, \dots, e_\ell$ of edges in F. Since the hypergraph is simple and contains no cycles, we have that $e_\ell \cap (\bigcup_{i=1}^{\ell-1} e_i) = e_\ell \cap e_{\ell-1} = \{v\}$ for some single vertex v. On the other hand, all vertices of e_ℓ must have degree 2 in $F \cup C_2$, and so $e_\ell \setminus v$ must lie entirely in C_2. We set $f_1 = e_\ell$, $a_1 = v$, and then we remove f_1 from F and a_1 from A, defining $C_2^1 = C_2 \cup f_1$ (though it is not a two-core of any hypergraph), and apply induction to obtain the sequences $a_1, \dots, a_k$, $f_1, \dots, f_k$, and the corresponding sequence C_2^i defined by $C_2^0 = C_2$, and $C_2^{i+1} = C_2^i \cup f_{i+1}$.

These sequences have the property that

$$\mathrm{rank}(C_2^{i+1}) = \mathrm{rank}(C_2^i) + 1,$$

since the edge f_i added to C_2^i in step $i+1$ contains exactly one vertex outside of C_2^i. (In the matrix, we are adding a column containing a 1 in a row which previously had no 1's).

In particular, the rank in this case increases by exactly the size of A.

Case 2: The total contribution to the rank of the 2-core in $m = O(n \log n)$ steps from the case where F contains a cycle of length at most $\log^{1/2} n$ can be bounded by $n^{3/4+o(1)}$. This follows from Lemma 5(b) and (3), (4). This is negligible, since the core has size $\Omega(n)$ in the regime we are discussing.

Case 3: Suppose that F contains cycles of size at least $\log^{1/2} n$ which we remove by deleting s edges. When we do this we may lose up to ks vertices from A. Let the resulting vertex set be A' and edge set be F'. Up to ks vertices of A' may have degree 1. Attach these vertices to C_2 using disjoint edges to give edge set F''. All vertices of A' now have degree at least 2 in F'' and F'' has no cycles. According to the argument in Case 1, the increase in rank due to adding F'' is $|A'| \geq |A| - ks$ and this is at most ks larger than the increase in rank due to adding F'. Thus the increase in rank due to adding $F \supseteq F'$ is at least $|A| - 2ks$ and at most $|F| \leq |A| + s + 1$. It follows from Lemma 4(c) and Lemma 5(a) that $s = O(|A|/\log^{1/4} n)$.

In summary we find that if $m = O(n)$ and $m \geq m_k$ then, with probability $1 - o(n^{-1})$, the rank of $\mathbf{C}_2$ satisfies

$$\mathrm{rank}(\mathbf{C}_2) - \mathrm{rank}(\widehat{\mathbf{C}}) = \left(1 + O\left(\frac{1}{\log^{1/4} n}\right)\right)(|V(C_2)| - |V(\widehat{C})|). \tag{13}$$

This proves (7). To finish the proof of Theorem 1 we require that (13) remains true if we take expectations. For this we use the error probability of $o(n^{-1})$ in (12).

This completes the proof of Theorem 1.

3 Proof of Theorem 2

As shown in [5], the RHS of (1) is the limiting probability that every row has at least one non-zero. We will only consider the case where $c = O(1)$, the other cases will follow by monotonicity considerations.

We will let $p = \frac{n(\log n + c)}{k\binom{n}{k}}$ and also consider the random matrix $\mathbf{A}_p$. There are $\binom{n}{k}$ possible positions for the non-zeros of a column and in $\mathbf{A}_p$ we include a column with each possible set of positions with probability p. Having chosen the positions of the non-zeros, we fill in values uniformly from $\mathbb{F}^*$. We will use $\mathbb{P}_m, \mathbb{P}_p$ when we we are estimating probabilities w.r.t. $\mathbf{A}, \mathbf{A}_p$ respectively.

For a set $S \subseteq [n]$ we let $\mathcal{B}_S$ denote the event that the rows of $\mathbf{A}$ corresponding to S are minimally linearly dependent. Let $L_0 = \log \log n$. We condition on no empty rows.

Case 1: $s = |S| \in I = [2, L_0]$:
For a set S of s rows, let a denote the number of columns with at least two non-zero entries and let b denote the number of rows with more than $L_1 = \log^{1/2} n$ non-zeros. We note that $a \geq \lceil s/2 \rceil$, else there is a column with a unique non-zero and $\mathcal{B}_S$ does not occur.

Now

$$\mathbb{P}_m(\exists S:|S|\in I,\ a\geq 2s)\leq \sum_{s\in I}\binom{n}{s}\binom{m}{2s}\left(\binom{s}{2}\cdot\left(\frac{k}{n}\right)^2\right)^{2s}\leq \sum_{s\in I}\left(\frac{ne}{s}\right)^s\left(\frac{me}{2s}\right)^{2s}\left(\frac{s^2k^2}{2n^2}\right)^{2s}$$
$$=\sum_{s\in I}\left(\frac{e^3m^2sk^4}{16n^3}\right)^s=o(1).$$

Now if $\mathcal{B}_S$ occurs and $a\leq 2s$ then we must have $b=0$. But then, if $J=[\lceil s/2\rceil,2s]$,

$$\mathbb{P}_m(\exists S:|S|\in I,a\in J,b=0)\leq$$
$$\sum_{\substack{s\in I\\ a\in J}}\binom{n}{s}\binom{m}{a}\left(\binom{s}{2}\cdot\left(\frac{k}{n}\right)^2\right)^{a}(\mathbb{P}(Bin(m-2s,k/n)\leq L_1))^s\leq$$
$$\sum_{\substack{s\in I\\ a\in J}}\left(\frac{ne}{s}\right)^s\left(\frac{me}{a}\cdot\frac{s^2k^2}{n^2}\right)^a n^{-(s-o(s))}=o(1). \quad (14)$$

Case 2: $L_0<s\leq n_0=n/k-2$**:**

$$\mathbb{P}_p(\mathcal{B}_S)\leq (1-p)^{s\binom{n-s}{k-1}}$$

Explanation: There are $s\binom{n-s}{k-1}$ choices of column for which there is a unique non-zero in rows S in that column.

This gives a bound

$$\mathbb{P}_p(\exists S:\mathcal{B}_S)\leq \binom{n}{s}\exp\left\{-\frac{s(\log n+c)\binom{n-s}{k-1}}{k\binom{n}{k}}\right\}\leq \binom{n}{s}\exp\left\{-s(\log n+c)\left(1-\frac{ks}{n-k}\right)\right\}$$
$$\leq\left(\frac{ne}{s}\cdot\exp\left\{-(\log n+c)\left(1-\frac{ks}{n-k}\right)\right\}\right)^s=\left(\frac{e^{1-c}}{s}\cdot\exp\left\{\frac{ks(\log n+c)}{n-k}\right\}\right)^s=o(1), \quad (15)$$

for $L_0<s\leq n_0$.

Case 3: $n_0<s\leq n$**.**
We can also write

$$\mathbb{P}_m(B_S)\leq (q-1)^s\left(\frac{1}{q-1}+\frac{\binom{n-s}{k}}{\binom{n}{k}}\right)^m.$$

Explanation: There are $(q-1)^s$ choices for the dependency coefficients and then for each column either (i) there are no non-zeros in that column or (ii) the non-zero in the highest indexed row is determined by the other non-zeros.

This gives a bound

$$\mathbb{P}_m(\exists S:\mathcal{B}_S)\leq\binom{n}{s}(q-1)^s\left(\frac{1}{q-1}+\frac{\binom{n-s}{k}}{\binom{n}{k}}\right)^m\leq e^{O(n)}\left(\frac{1}{2}+e^{-(1-o(1))}\right)^m=o(1). \quad (16)$$

Theorem 2 now follows from (14), (15) and (16). We note that while (15) refers to $\mathbf{A}_p$, the inequality translates to $\mathbf{A}$ through monotonicity as is done for $G_{n,p}$ and $G_{n,m}$, see e.g. [8], Lemma 1.3.

References

[1] P. Ayre, A. Coja-Oghlan, P. Gao and N Müller, The satisfiabilty threshold for random linear equations, arXiv:1710.07497 [math.CO].

[2] A. Coja-Oghlan, A. Ergr, S. Hetterich and M. Rolvienhref, The rank of sparse random matrices.

[3] A. Coja-Oghlan and P. Gao, The rank of random matrices over finite fields.

[4] C. Cooper, The cores of random hypergraphs with a given degree sequence, *Random Structures and Algorithms* 25 (2004) 353-375.

[5] C. Cooper, A.M. Frieze and W. Pegden, Electronic Journal of Combinatorics 26, 2019.

[6] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh and M. Rink, Tight Thresholds for Cuckoo Hashing via XORSAT.

[7] O. Dubois and J. Mandler, The 3-XORSAT threshold, *Comptes Rendus Mathematique* 335 (2002) 963-966.

[8] A.M. Frieze amd M. Karoński, Introduction to Random Graphs, Cambridge University Press, 2015.

[9] M. Molloy, Cores in random hypergraphs and random formulas, *Random Structures and Algorithms* 27 (2005) 124-135.

[10] B. Pittel and G. Sorkin, The Satisfiability Threshold for k-XORSAT, *Combinatorics, Probability and Computing* 25 (2016) 238-268.