Littlewood-Offord Lemma (proved by Erdős in 1945; an easy consequence of Sperner's theorem). *Let $a_1, \dots, a_n$ be real numbers with $|a_i| \geq 1$. Then, among the 2^n signed sums $\sum \varepsilon_i a_i$, $\varepsilon_i = \pm 1$, at most $\binom{n}{n/2}$ fall into the open interval $(-1, 1)$.*
The interval $(-1, 1)$ could be substituted by any open (or semi-closed) interval of length 2.

Remark: The lemma is true in any linear metric space (Kleitman 1970). Note the significance of the openness of the interval in the lemma: let the a_i's be the standard unit vectors in $\mathbb{R}^n$ with ℓ^∞ metric; *all* the 2^n sums are in the closed unit cube but only $\binom{n}{n/2}$ in the open cube.

We will use the notation $p_k := \binom{k}{\lfloor k/2 \rfloor} 2^{-k}$. Note that p_k is decreasing and $p_k \sim c/\sqrt{k}$, $c = \sqrt{2/\pi}$. The Littlewood-Offord lemma will be applied in the following form.

Lemma 1. *Let $a_1, \dots, a_n$ be integers at least k of which are non-zero. Let S_n be the random sum $S_n = \sum \varepsilon_i a_i$, where $\varepsilon_i = \pm 1$ are chosen independently and uniformly. Then, for any fixed real number x, $P(S_n = x) \leq p_k$.*

Definition. *The* **crank** *of a matrix M is the largest k such that* **any** k **columns** *of M are linearly independent. (Clearly, $crank(M) \leq rank(M)$.)*

Now we are ready for our main theorem.

Theorem (Komlós 1963). *Let M be a random $n \times n$ ± 1-matrix. The probability that M is singular is $O(1/\sqrt{n})$.*

Remark: The method actually yields: $P(|Det(M)| \leq \exp\{o(\sqrt{n})\}) = 1 - o(1)$.

Proof. (This is the simplified proof from my circulated unpublished manuscript of 1977.) Let $M = M_{mn}$ be a random $m \times n$ ± 1-matrix. We will write $\mathbf{b}_1, \dots, \mathbf{b}_n$ for the columns of M, and for $1 \leq k \leq n$ we let E_k be the event that the first $k-1$ rows of M are linearly independent but the k-th row is their linear combination. Note that

$$P(rank(M_{mn}) < m) = P(\bigcup_{1 \leq k \leq m} E_k) \leq \sum_{1 \leq k \leq m} P(E_k).$$

The theorem follows from the following lemmas. (We will sometimes assume that n is large and will not bother with rounding to integers.)

Lemma 2. *For any $1 \leq k \leq n$,*

$$P(crank\{\mathbf{b}_1, \dots, \mathbf{b}_k\} = k-1) \leq \binom{m}{k-1} p_k^{m-k+1},$$

whence

$$P(crank\{\mathbf{b}_1, \dots, \mathbf{b}_n\} = k-1) \leq \binom{n}{k} \binom{m}{k-1} p_k^{m-k+1}.$$

Lemma 3. *If $m/2 \leq n \leq 2m$, then*

$$P(crank(M_{mn}) < m/2) \leq \sum_{k \leq m/2} \binom{n}{k} \binom{m}{k-1} p_k^{m-k+1} < 0.8^m$$

Lemma 4. *Let M' be the submatrix consisting of the first $m-1$ rows of M. Then,*

$$P(rank(M) = rank(M')) \leq 2^{rank(M')-n} \leq 2^{m-n-1}.$$

Hence,

$$P(rank(M_{mn}) < m) \leq \sum_{1 \leq k \leq m} P(E_k) \leq \sum_{1 \leq k \leq m} 2^{k-n-1} < 2^{m-n}.$$

Lemma 5. *If $k/2 \leq n \leq 2k$, then $P(E_k) \leq c\, 2^{k-n}/\sqrt{n} + 0.8^k$. (This, combined with Lemma 4, proves the claim of the theorem.)*

Proof of Lemma 2. Let M_k be the matrix formed by the columns $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$. Since $crank(M_k) = k-1$ implies that $rank(M_k) = k-1$, some $k-1$ rows of M_k are linearly independent. It is thus enough to show that

$$P(crank(M_k) = k-1, \text{ and the first } k-1 \text{ rows of } M_k \text{ are linearly independent}) \leq p_k^{m-k+1}.$$

So let's randomize the first $k-1$ rows of M_k first. If they happen to be linearly independent (otherwise the (conditional) probability in question is 0), then they already uniquely determine the (one-dimensional) nullspace of M_k: constants $c_1, \ldots, c_k$, not all zero, such that $\sum_{1 \leq i \leq k} c_i \mathbf{b}_i = \mathbf{0}$ will hold (once the rest of the matrix is randomized) if the rank of M_k is to be $k-1$. And for $crank(M_k) = k-1$ to hold when M_k is later completed, all the c_i have to be non-zero. Since the same linear relation should hold in all the remaining $m-k+1$ rows of M_k (still to be randomized), an application of Lemma 1 concludes the proof. □

Proof of Lemma 3. The inequality follows from a straightforward calculation (for $k = o(n)$ use $p_k \leq 1/2$, otherwise use $p_k < c/\sqrt{k}$.) □

Proof of Lemma 4. Indeed, first randomize the elements of M' and find a basis in its column-set, say the first $rank(M')$ columns of M'. Randomize also the first this many elements of the last row of M. The rest of the last row is uniquely determined if we want $rank(M) = rank(M')$. □

Proof of Lemma 5. (The crux of the whole theorem.) Let R be the submatrix formed by the first k rows of M, and R' the submatrix formed by the first $k-1$ rows of M. To estimate $P(E_k)$, we will estimate instead $P(E_k,\ crank(R') \geq k/2)$ (this is justified by Lemma 3). Let us first randomize the elements of R'. If they happen to be independent and $crank(R') \geq k/2$ (otherwise the conditional probability $P(E_k,\ crank(R') \geq k/2 \,|\, R')$ is 0), then select $k-1$ independent columns in this submatrix; for simplicity of notation assume they are the first $k-1$ columns of R. All other columns of R' are linear combinations of these $k-1$ columns. Let the columns of R' be $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$. Since $crank(M') \geq k/2$, there are (unique) scalars $c_1, \ldots, c_k$ such that $\sum_{1 \leq i \leq k} c_i \mathbf{b}'_i = \mathbf{0}$ and at least $k/2$ of the c_is are nonzero. This dependence must also be present in the first k elements of the last row, say $\mathbf{r}$ of R; these are the k entries of R that we randomize next. The probability of that dependence being preserved is $O(1/\sqrt{n})$. The rest of $\mathbf{r}$ is determined if we want the full $\mathbf{r}$ to be in the span of the rows of R'; each new randomized element is supposed to take a prescribed value - a probability of $1/2$ (or 0) for each. □

P. Erdős, On a lemma of Littlewood and Offord, Bull. Am. Math. Soc. 5 (1945), 898-902.

D. J. Kleitman, On a lemma of Littlewood and Offord on the distribution of linear combinations of vectors, Advances Math. 5 (1970), 155-157.

J. E. Littlewood and C. Offord, On the number of real roots of a random algebraic equation. III. Mat. Sbornik 12 (1943), 277-286.

János Komlós, On the determinant of 0-1 matrices, Studia Sci. Math. Hung. 2 (1967), 7-21.