Combinatorics, Probability and Computing (2006) 15, 463–471. © 2006 Cambridge University Press
doi:10.1017/S0963548305007339 Printed in the United Kingdom

Singular 0/1-Matrices, and the Hyperplanes Spanned by Random 0/1-Vectors

THOMAS VOIGT[†] and GÜNTER M. ZIEGLER[‡]

Inst. Mathematics, MA 6-2, TU Berlin, D-10623 Berlin, Germany
(e-mail: {tvoigt,ziegler}@math.tu-berlin.de)

Received 6 August 2003; revised 16 August 2004

Let $P_s(d)$ be the probability that a random 0/1-matrix of size $d \times d$ is singular, and let $E(d)$ be the expected number of 0/1-vectors in the linear subspace spanned by $d-1$ random independent 0/1-vectors. (So $E(d)$ is the expected number of cube vertices on a random affine hyperplane spanned by vertices of the cube.)

We prove that bounds on $P_s(d)$ are equivalent to bounds on $E(d)$:

$$P_s(d) = \left(2^{-d}E(d) + \frac{d^2}{2^{d+1}}\right)(1 + o(1)).$$

We also report on computational experiments pertaining to these numbers.

1. Introduction

0/1-polytopes arise naturally in a great variety of interesting contexts, including a prominent role in combinatorial optimization, yet some basic characteristics of 'typical' (that is, random) 0/1-polytopes are unknown. (For a survey of a variety of aspects of 0/1-polytopes see [8].)

One of the key open questions in this context is rather notorious:

- Pick $d+1$ random vertices of the d-cube independently (with respect to the uniform distribution). What is the probability that these vectors do not form a d-simplex?

If we assume without loss of generality that one of these points is the origin $\mathbf{0}$ the question can be rephrased: Let $C^d = [0,1]^d$ be the d-dimensional unit hypercube, and let

$$\mathscr{M}_d := \{0,1\}^{d\times d}$$

be the set of all 0/1-matrices of size $d \times d$.

[†] Supported by Deutsche Forschungs-Gemeinschaft (DFG) ZI 475/3.
[‡] Partially supported by Deutsche Forschungs-Gemeinschaft (DFG), FZT86 and ZI 475/4.

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

- What is the asymptotic behaviour of the probability

$$P_s(d) := \text{Prob}\big[\det(M) = 0 \mid M \in \mathscr{M}_d\big]$$

that a random square d-dimensional 0/1-matrix is singular?

This central but difficult question has received careful attention; see Komlós [6], Bollobás [2], Kahn, Komlós and Szemerédi [5]. It has been conjectured that

$$P_s(d) = \frac{d^2}{2^d}(1 + o(1)),$$

which is essentially the probability that two rows or two columns of a random matrix are equal. However, the known upper bounds are far off this mark; currently the best upper bound is $P_s(d) < (1 - \varepsilon)^d$, for some rather small $\varepsilon > 0$. (This was proved by Kahn, Komlós and Szemerédi in [5] with $\varepsilon = 0.001$.)

A closely related problem is as follows:

- Given r random vertices $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ of C^d, what is the expected number of 0/1-vectors in the affine subspace spanned by these vectors?

Improving a result by Odlyzko [7], Kahn, Komlós and Szemerédi derived in [5] that there exists a constant C independent from d such that the probability that such an affine subspace contains any 0/1-vector other than $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ is $4\binom{r}{3}(\frac{3}{4})^d(1 + o(1))$, provided that $r < d - C$. However, so far no results were known for the case $r = d$.

In this paper we will show that determining the expected number of vertices of C^d in the affine subspace spanned by d random vertices of C^d is just as hard as determining $P_s(d)$. More precisely, let $\mathscr{G}$ denote the set of all linearly independent $(d-1)$-sets of 0/1-vectors of length d, and for a set S of arbitrary vectors let $v(S)$ be the number of 0/1-vectors in the linear subspace spanned by S. Then the following theorem holds.

Theorem 1.1. *Let*

$$E(d) := \frac{1}{|\mathscr{G}|}\sum_{G \in \mathscr{G}} v(G)$$

be the expected number of 0/1*-points on the hyperplane spanned by a random linearly independent set of* $d-1$ 0/1*-vectors. Then*

$$P_s(d) = \left(\frac{1}{2^d}E(d) + \frac{d^2}{2^{d+1}}\right)(1 + o(1)).$$

We can give a (trivial) lower bound for $E(d)$ by just considering the $\binom{d}{2} + d$ 'fat' hyperplanes (faces $x_i = 0$ and hyperplanes $x_i - x_j = 0$) containing 2^{d-1} vertices each. Since $d-1$ points chosen randomly from such a hyperplane span the hyperplane with probability $1 - (1 - \varepsilon)^{d-1}$ (according to [5]) it is easy to verify that $E(d) \geqslant \frac{d^2}{2}(1 + o(1))$.

In fact the conjectured upper bounds on $P_s(d)$ and $E(d)$ are strictly equivalent.

Corollary 1.2. *As* $d \to \infty$,

$$P_s(d) = \frac{d^2}{2^d}(1 + o(1))$$

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

if and only if

$$E(d) = \frac{d^2}{2}(1 + o(1)).$$

Using symmetry we could switch to an affine version, replacing $\mathscr{G}$ by the set of affinely independent d-sets of 0/1-vectors and checking the expected value of 0/1-vectors in a hyperplane spanned by such a set. However, for the purpose of this paper the linear version will be more convenient to handle; so we will consider only hyperplanes containing the origin $\mathbf{0}$.

To our knowledge the problem of determining the expected number of 0/1-vectors on a hyperplane h spanned by random vertices of C^d has not yet been studied independently. Some basic results were derived in [2] and [5] by examining the structure of the defining equations $\boldsymbol{a}$ for planes $h = \{\boldsymbol{x} \in \mathbb{R}^d \mid \boldsymbol{a}^t\boldsymbol{x} = 0\}$ (which is perhaps the most natural approach). The Littlewood–Offord lemma (see Section 2) is a classical tool. It states that if all a_j are nonzero then the number of 0/1-points in this plane is at most $\binom{d}{\lfloor d/2 \rfloor}$. If the coefficients satisfy additional conditions, this number can be reduced considerably (see Halász [3, 4]). In order to obtain such conditions it would be of considerable interest to learn more about the distribution of determinants of 0/1-matrices: if $d-1$ vectors span a hyperplane and we write these vectors into a $d \times (d-1)$ matrix M, then a defining equation $\boldsymbol{a}^t\boldsymbol{x} = 0$ is given by $a_j = (-1)^j \det(r_j(M))$, where $r_j(M)$ is the matrix obtained from M by deleting the jth row.

The rest of this paper is organized as follows. In Section 2 we state some consequences of the Littlewood–Offord lemma. The proof of Theorem 1.1 is given in Section 3. In Section 4 we present some experimental estimates of $P_s(d)$ for $d \leqslant 30$.

Some definitions. We use standard vector notation $\boldsymbol{a} = (a_1, \ldots, a_d)^t$, where d denotes the dimension. The expected value of a random variable X is denoted by $E[X]$; the probability of an event Y is $\mathrm{Prob}[Y]$. Define $r(F)$ as the (linear) rank of a family or set of vectors F.

The next definition is useful for partitioning sets of matrices into subsets with 'nice' properties and was frequently used in the analysis of 0/1-matrices (see [2] or [5]). Given a $d \times d$ matrix M we define the *strong rank* $\bar{\bar{r}}(M)$ as the largest $k \leqslant d$ such that all k-subsets of columns from M are independent. (Equivalently, it is the largest k such that the truncation to rank k of the matroid given by the columns of the matrix m is uniform of rank k.) We also consider the strong rank of sets and of families of d-dimensional vectors.

2. The Littlewood–Offord lemma

The 'Littlewood–Offord lemma' is a classical tool [2, 7] for obtaining upper bounds on $P_s(d)$.

Lemma 2.1 (Littlewood–Offord). *Let $s \in \mathbb{R}$, $n \in \mathbb{N}$ and let $a_i \in \mathbb{R}$ with $|a_i| \geqslant 1$ for $1 \leqslant i \leqslant n$. Then at most $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ of the 2^n sums $\sum_{i=1}^n \varepsilon_i a_i$, $\varepsilon_i = \pm 1$ fall in the open interval $(s-1, s+1)$.*

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

Corollary 2.2. *Let $a_i \in \mathbb{R}, i = 1, \ldots, n$ with at least t of the a_i nonzero. Then at most $\binom{t}{\lfloor t/2 \rfloor} 2^{n-t} \approx \frac{2^n}{\sqrt{\frac{\pi}{2} t}}$ of the 2^n sums $\sum_{i=1}^n \varepsilon_i a_i$, $\varepsilon_i \in \{0, 1\}$ can have the same value.*

As observed in [5], this lemma suffices to show that with very high probability the strong rank of a random 0/1-matrix is either close to d or at most 1.

Lemma 2.3. *Let $M \in \mathscr{M}_d$ be a random matrix. Let E be the event that M has a $d \times (k+1)$ submatrix of strong rank k for some $k \in \{2, \ldots, d - 3\frac{d}{\ln(d)}\}$. Then, for large d,*

$$\text{Prob}[E] \leqslant 2^{-d}.$$

Proof. The proof follows [2, Chapter 14.2] (see also [5, Section 3.1]) and is sketched here for the reader's convenience.

Let M be a random 0/1-matrix and $k < d$. If M contains $k+1$ columns $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1}$ of strong rank k then clearly we can find a $k \times (k+1)$ submatrix of M of strong rank k by deleting $d - k$ linearly dependent rows from $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1})$.

If we want to upper-bound the probability that arbitrarily chosen columns $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1}$ have strong rank k, then it suffices to give an upper bound on the probability that $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1}$ have rank k conditioned on the event that an arbitrary $k \times (k+1)$ submatrix $\tilde{M}$ of $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1})$ has strong rank k. $\tilde{M}$ has strong rank k if and only if the last column of $\tilde{M}$ is a unique linear combination of the first k columns and all coefficients in this combination are nonzero. Under this condition the probability that any of the remaining $d - k$ rows of $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1}$ satisfy the linear dependency equation defined by $\tilde{M}$ is at most $2^{-k}\binom{k}{\lfloor \frac{k}{2} \rfloor}$ by Lemma 2.2, so the probability that $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k+1}$ have rank k is at most $(2^{-k}\binom{k}{\lfloor \frac{k}{2} \rfloor})^{d-k}$. Since there are at most $\binom{d}{k}\binom{d}{k+1}$ such submatrices $\tilde{M}$ we find

$$\text{Prob}[\bar{\bar{r}}(M) = k] \leqslant \binom{d}{k}\binom{d}{k+1}\left(2^{-k}\binom{k}{\lfloor \frac{k}{2} \rfloor}\right)^{d-k}.$$

We derive

$$\sum_{k=3}^{\lfloor d - 3\frac{d}{\ln(d)} \rfloor} \binom{d}{k}\binom{d}{k+1}\left(2^{-k}\binom{k}{\lfloor \frac{k}{2} \rfloor}\right)^{d-k} \leqslant 2^{-d} \tag{2.1}$$

by checking that each summand in (2.1) is at most $\frac{1}{d2^d}$ if d is large (using Stirling's formula and elementary, but somewhat tedious calculations).

To complete the proof of Lemma 2.3 we observe that the event $\bar{\bar{r}}(M) = 2$ depends on the existence of three columns $\boldsymbol{m}_i, \boldsymbol{m}_j, \boldsymbol{m}_k$ such that $\boldsymbol{m}_i + \boldsymbol{m}_j = \boldsymbol{m}_k$, which happens with probability $\Theta(d^3(\frac{3}{8})^d)$. □

Corollary 2.4. *Let $M \in \mathscr{M}_d$ be a random matrix. Then*

$$\text{Prob}\left[\bar{\bar{r}}(M) \leqslant d - 3\frac{d}{\ln(d)}\right] \leqslant \frac{d^2}{2^{d+1}}(1 + o(1)).$$

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

3. Proof of Theorem 1.1

Let $\mathscr{S} \subset \mathscr{M}_d$ be the set of singular matrices and $\mathscr{R} = \mathscr{M}_d \setminus \mathscr{S}$. We will partition $\mathscr{S}$ into subsets $\mathscr{S}_j \subset \mathscr{S}, j \in \{1, \ldots, 4\}$ and derive precise bounds on the sizes of two of these sets in terms of $|\mathscr{G}|$ and $E(d)$. The other two sets are small. This allows us to estimate the value $P_s(d) = \frac{|\mathscr{S}|}{|\mathscr{S}|+|\mathscr{R}|}$.

Let $N_d := \lfloor d - \frac{3d}{\ln(d)} \rfloor$ and partition $\mathscr{S}$ into the disjoint sets

$$\begin{aligned}
\mathscr{S}_1 &:= \{M \in \mathscr{M}_d \mid r(M) = d-1,\ \bar{\bar{r}}(M) = 1\},\\
\mathscr{S}_2 &:= \{M \in \mathscr{M}_d \mid r(M) = d-1,\ \bar{\bar{r}}(M) > N_d\},\\
\mathscr{S}_3 &:= \{M \in \mathscr{M}_d \mid \bar{\bar{r}}(M) \in \{0, 2, \ldots, N_d\}\},\\
\mathscr{S}_4 &:= \{M \in \mathscr{M}_d \mid r(M) < d-1,\ \bar{\bar{r}}(M) = 1 \ \text{ or } \ \bar{\bar{r}}(M) > N_d\}.
\end{aligned}$$

We will give precise estimates for the sizes of the sets $\mathscr{R}$, $\mathscr{S}_1$, and $\mathscr{S}_2$, and check that the sets $\mathscr{S}_3$ and $\mathscr{S}_4$ are small enough. More precisely, we will show that

$$|\mathscr{R}| = |\mathscr{G}|\, d! \frac{2^d - E(d)}{d}, \tag{3.1}$$

$$|\mathscr{S}_1| = |\mathscr{G}|\, d! \frac{d-1}{2}, \tag{3.2}$$

$$|\mathscr{S}_2| = |\mathscr{G}|\, d! \frac{E(d)}{d}(1 + o(1)), \tag{3.3}$$

$$|\mathscr{S}_1| \leqslant |\mathscr{S}_2|(1 + o(1)), \tag{3.4}$$

$$|\mathscr{S}_3| \leqslant \frac{c_1}{d}|\mathscr{S}_1|, \tag{3.5}$$

$$|\mathscr{S}_4| \leqslant \frac{c_2}{\sqrt{d}}(|\mathscr{S}_1| + |\mathscr{S}_2|) \tag{3.6}$$

for some constants $c_1, c_2 > 0$.

- While most matrices from $\mathscr{M}_d$ with two equal columns are in $\mathscr{S}_1$, most matrices with two equal rows lie in $\mathscr{S}_2$. To see this, pick a random $(d-1) \times d$ matrix $N = (\boldsymbol{n}_1, \ldots, \boldsymbol{n}_d)$. Using the result of Kahn, Komlós and Szemerédi [5] that $P_s(d) \leqslant (1-\varepsilon)^d$ for some $\varepsilon \geqslant 0.001$, we obtain $d(1-\varepsilon)^{d-1}$ as an upper bound on the probability that at least one of the $(d-1) \times (d-1)$ submatrices $c_j(N)$ is singular, where $c_j(N)$ is the matrix obtained from N by deleting the jth column $\boldsymbol{n}_j$. Cramer's rule gives $\sum_{j=1}^{d}(-1)^j d_j \boldsymbol{n}_j = \boldsymbol{0}$ for the determinants $d_j = \det(c_j(N))$. Thus, N has strong rank $d-1$ if all determinants are nonzero, which establishes (3.4):

$$|\mathscr{S}_1| \leqslant |\mathscr{S}_2|(1 + o(1)).$$

- By Lemma 2.3 a random matrix $M \in \mathscr{M}_d$ lies in $\mathscr{S}_3$ with probability at most $(d+1)2^{-d}$. The probability that two columns are equal is $d^2 2^{-d-1}(1 + o(1))$. Again, almost all matrices with two identical columns have strong rank $d-1$ and are in $\mathscr{S}_1$ (up to an exponentially small subset), which implies (3.5):

$$|\mathscr{S}_3| = O\left(\frac{1}{d}|\mathscr{S}_1|\right).$$

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

For each matrix $M \in \mathscr{R} \cup \mathscr{S}_1 \cup \mathscr{S}_2$ there is at least one $G \in \mathscr{G}$ that is a subset of the column set of M. The estimates (3.1), (3.2) and (3.3) are obtained by examining this in detail.

- For each $G \in \mathscr{G}$ we have exactly $\frac{d!}{2}(d-1)$ matrices from $\mathscr{S}_1$ containing only columns from G (since we have $d-1$ choices for a duplicate column and $\frac{d!}{2}$ permutations). This gives (3.2):

$$|\mathscr{S}_1| = |\mathscr{G}|\frac{d!}{2}(d-1).$$

- For any fixed $G \in \mathscr{G}$ we can construct $d!(v(G)-d)$ different matrices $S \in \mathscr{S}_2 \cup \mathscr{S}_3$ (using columns from G and an additional nonzero column in the span of G that is not in G). Summing over $G \in \mathscr{G}$ we obtain $d!E(d)(1+o(1))|\mathscr{G}|$ matrices in $\mathscr{S}_2$, since (3.4) and (3.5) imply that $|\mathscr{S}_3|$ is small compared to $|\mathscr{S}_2|$. On the other hand each matrix $M \in \mathscr{S}_2$ is constructed $\bar{\bar{r}}(M)+1$ times: if $M \in S_2$ and $M\boldsymbol{a} = 0$ for some $\boldsymbol{a} \neq \mathbf{0}$ then $|\mathrm{supp}(\boldsymbol{a})| = \bar{\bar{r}}(M)+1$ (equality holds since $r(M) = d-1$) and $\{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_{k-1}, \boldsymbol{m}_{k+1}, \ldots, \boldsymbol{m}_d\}$ is independent if and only if $a_k \neq 0$. This gives (3.3):

$$\begin{aligned} |\mathscr{S}_2| &= \frac{1}{d-o(d)} d!E(d)(1+o(1))|\mathscr{G}| \\ &= d!\frac{E(d)}{d}(1+o(1))|\mathscr{G}|. \end{aligned}$$

- Similarly, we get $d!(2^d - E(d))|\mathscr{G}|$ matrices in $\mathscr{R}$ and each matrix $M \in \mathscr{R}$ is constructed d times. This gives (3.1):

$$|\mathscr{R}| = \frac{d!}{d}\big(2^d - E(d)\big)|\mathscr{G}|.$$

A little more work is required for the upper bound (3.6) on $|\mathscr{S}_4|$. So far we have established an upper bound on the number of matrices of rank $d-1$ in terms of the number of regular matrices. A similar argument will be used to show that for any $k \leqslant d-2$ there are significantly fewer matrices of rank k than matrices of rank $k+1$, which gives the desired result.

(i) First consider the matrices $\hat{\mathscr{S}}$ with the property that the rows or the columns admit more than one trivial dependency (*i.e.*, zero-vectors or pairs of identical vectors). This probability is dominated by the probability that a matrix has two pairs of identical rows or columns, which happens with probability $O(\binom{d}{4}2^{-2d})$, so clearly $|\mathscr{S}_4 \cap \hat{\mathscr{S}}|$ is exponentially smaller than $\frac{1}{\sqrt{d}}(|\mathscr{S}_1| + |\mathscr{S}_2|)$.

(ii) Let $\check{\mathscr{S}}$ be the set of matrices whose columns or rows have a subset with strong rank in $\{2, \ldots, N_d\}$. Lemma 2.3 gives that this happens with probability of at most 2^{-d}, while the probability that two columns are equal is $d^2 2^{-d-1}(1+o(1))$. This implies $|\check{\mathscr{S}}| \leqslant O(\frac{1}{d^2}|\mathscr{S}_1|)$.

(iii) To estimate the number of the remaining matrices in $\mathscr{S}_4$, we use similar techniques as in [2, Chapter 14.2]. We can use the Littlewood–Offord lemma to give an upper bound on the number of 0/1-vectors in the span of a set of vectors $\mathscr{C}$. Let $\boldsymbol{a}$ be in the orthogonal space of $\mathscr{C}$, *i.e.*, $\boldsymbol{a}^t\boldsymbol{c} = 0$ for all $\boldsymbol{c} \in \mathscr{C}$. Clearly all vectors $\boldsymbol{v}$ in the span of

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

$\mathscr{C}$ satisfy $\boldsymbol{a}^t\boldsymbol{v} = 0$. If s is the number of nonzero entries in $\boldsymbol{a}$ then Lemma 2.2 assures us that the span of $\mathscr{C}$ contains at most $\binom{s}{\lfloor s/2 \rfloor} 2^{d-s}$ 0/1-vectors.

Let $\mathscr{S}_4(k)$ be the matrices in $\mathscr{S}_4 \setminus (\hat{\mathscr{S}} \cup \check{\mathscr{S}})$ of rank k. For a fixed $k \leqslant d-2$ and $m \in \mathscr{S}_4(k)$ we know that the columns and rows of m admit at most one trivial dependency (by excluding $\hat{\mathscr{S}}$) and that neither rows nor columns have a submatrix of strong rank between 2 and N_d (by excluding $\check{\mathscr{S}}$). Thus both $\ker(m)$ and $\ker(m^t)$ contain vectors with more than N_d nonzero entries, since they are are at least 2-dimensional. Choose any such vectors $\boldsymbol{a} \in \ker(m)$ and $\boldsymbol{b} \in \ker(m^t)$.

If m is chosen uniformly at random from $\mathscr{S}_4(k)$, then the probability that $a_d \neq 0$ is at least $\frac{N_d}{d} = 1 - \frac{3}{\ln d}$. If we condition on this event (that the last column of m is a nontrivial linear combination of the remaining columns) and consider all 0/1-matrices having the same first $d-1$ columns as m, then (by the observation above) at most $2^{d-N_d}\binom{N_d}{\lfloor N_d/2 \rfloor}$ of these matrices have rank k, since the last column $\boldsymbol{v}$ has to satisfy $\boldsymbol{b}^t\boldsymbol{v} = 0$. Stirling's formula implies that

$$2^{d-N_d}\binom{N_d}{\lfloor N_d/2 \rfloor} \approx 2^d\sqrt{\frac{2}{\pi N_d}} = O\left(\frac{1}{\sqrt{d}}2^d\right).$$

Removing the condition $a_d \neq 0$ changes the number of matrices only by a factor of $1 + \frac{3}{\log d}$, so we find that

$$|\mathscr{S}_4(k)| = \begin{cases} O\left(\frac{1}{\sqrt{N_d}}|\mathscr{S}_4(k+1)|\right) & \text{if } k < d-2, \\ O\left(\frac{1}{\sqrt{N_d}}|\mathscr{S}_1| + |\mathscr{S}_2|\right) & \text{if } k = d-2. \end{cases}$$

This establishes (3.6):

$$|\mathscr{S}_4| \leqslant \frac{c_2}{\sqrt{d}}(|\mathscr{S}_1| + |\mathscr{S}_2|)$$

for some constant $c_2 > 0$.

Thus we have

$$\begin{aligned} P_s(d) &= \frac{|\mathscr{S}|}{|\mathscr{R}| + |\mathscr{S}|} \\ &= \frac{(|\mathscr{S}_1| + |\mathscr{S}_2|)(1 + o(1))}{|\mathscr{R}| + (|\mathscr{S}_1| + |\mathscr{S}_2|)(1 + o(1))} \\ &= \frac{\left(\frac{d-1}{2} + \frac{E(d)}{d}\right)}{\left(\frac{d-1}{2} + \frac{E(d)}{d} + \frac{2^d - E(d)}{d}\right)}(1 + o(1)) \\ &= \left(\frac{1}{2^d}E(d) + \frac{d^2}{2^{d+1}}\right)(1 + o(1)). \end{aligned}$$

This concludes the proof of Theorem 1.1. □

4. Experiments in small dimensions

Complete enumeration of the 0/1-matrices of size $d \times d$ is feasible up to dimension 7 (see [8]), while hyperplanes were enumerated up to dimension 8 (see Aichholzer and

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

Aurenhammer [1]). For some higher dimensions we generated 25,000,000 random matrices and determined an experimental probability $P_x(d)$ that a random matrix is singular. The significance of these numbers is limited for high dimensions (we found very few singular matrices and 25 million is tiny compared to the number of 0/1-matrices), but since the number of singular matrices is sharply concentrated around the expected value the results should still be close to the real values. Up to dimension 17 $P_x(d)$ decreases at a slower rate than the natural lower bound $d^2 2^{-d}$ while in higher dimensions $P_x(d)$ seems to approach this bound.

Table 1.

d	matrices	singular	$P_x(d)$	$\frac{d^2}{2^d}$	$P_x(d)2^d d^{-2}$
1	2^1	1	0.5000000	0.500000	1.000
2	2^4	10	0.6250000	1.000000	0.625
3	2^9	338	0.6601562	1.125000	0.587
4	2^{16}	42976	0.6557617	1.000000	0.666
5	2^{25}	21040112	0.6270442	0.781250	0.803
6	2^{36}	$\approx 3.98 \cdot 10^{10}$	0.5803721	0.562500	1.032
7	2^{49}	$\approx 2.92 \cdot 10^{14}$	0.5197696	0.382812	1.358
8	25000000	11230864	0.4492346	0.250000	1.797
9	25000000	9331895	0.3732758	0.158203	2.359
10	25000000	7430305	0.2972122	0.0976562	3.043
11	25000000	5657196	0.2262879	0.0590820	3.830
12	25000000	4108304	0.1643321	0.0351562	4.674
13	25000000	2837245	0.1134898	0.0206299	5.501
14	25000000	1868850	0.0747540	0.0119629	6.249
15	25000000	1175425	0.0470170	0.0068665	6.847
16	25000000	707571	0.0283028	0.0039062	7.246
17	25000000	407077	0.0162831	0.0022049	7.385
18	25000000	225820	0.0090328	0.0012360	7.308
19	25000000	121157	0.0048463	0.0006886	7.038
20	25000000	62500	0.0025000	0.0003815	6.554
21	25000000	31779	0.0012712	0.0002103	6.045
22	25000000	15393	0.0006157	0.0001154	5.336
23	25000000	7383	0.0002953	0.0000631	4.683
24	25000000	3515	0.0001406	0.0000343	4.095
25	25000000	1722	0.0000689	0.0000186	3.698
26	25000000	736	0.0000294	0.0000101	2.923
27	25000000	345	0.0000138	0.0000054	2.541
28	25000000	164	0.0000066	0.0000029	2.246
29	25000000	81	0.0000032	0.0000016	2.068
30	25000000	37	0.0000015	0.0000008	1.766

References

[1] Aichholzer, O. and Aurenhammer, F. (1996) Classifying hyperplanes in hypercubes. *SIAM J. Discrete Math.* **9** 225–232.
[2] Bollobás, B. (1985) *Random Graphs*, Academic Press, London.
[3] Halász, G. (1975) On the distribution of additive arithmetic functions. *Acta Arith.* **27** 143–152.

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press

[4] Halász, G. (1977) Estimates for the concentration function of combinatorial number theory and probability. *Period. Math. Hung.* **8** 197–211.
[5] Kahn, J., Komlós, J. and Szemerédi, E. (1995) On the probability that a random ± 1-matrix is singular. *J. Amer. Math. Soc.* **8** 223–240.
[6] Komlós, J. (1967) On the determinant of $(0, 1)$ matrices. *Stud. Sci. Math. Hung.* **2** 7–21.
[7] Odlyzko, A. (1988) On subspaces spanned by random selections of ± 1 vectors. *J. Combin. Theory Ser. A* **47** 124–133.
[8] Ziegler, G. M. (2000) Lectures on 0/1-polytopes. In *Polytopes: Combinatorics and Computation* (G. Kalai and G. M. Ziegler, eds), Vol. 29 of *DMV Seminar*, Birkhäuser, Basel, pp. 1–41.

Note added in proof:

Recently, T. Tao and V. H. Vu (On the singularity probability of random Bernoulli matrices, preprint, 29 pages, January 2005; http://www.arxiv.org/math.CO/0501313) have significantly improved the upper bound on $P_s(d)$, by proving that $P_s(d) = (\frac{3}{4} + o(d))^d$.

Furthermore, M. Živković has recently computed the number of singular 0/1-matrices of size 8×8 exactly (Classification of small (0, 1) matrices, preprint, 45 pages, November 2005; http://arXiv.org/math.CO/0511636). From this we get that $P_s(8) = 0.4492003726$, so our estimate $P_x(8) = 0.4492346$ wasn't bad.

https://doi.org/10.1017/S0963548305007339 Published online by Cambridge University Press