ON RANDOM REPRESENTABLE MATROIDS

D. G. Kelly,*
Departments of Mathematics and Statistics,
University of North Carolina,
Chapel Hill

and

J. G. Oxley,
Department of Mathematics,
Louisiana State University,
Baton Rouge

* Partially supported by O.N.R. Grant No. N00014-83-K-0352.

Abstract

Results are obtained on the likely connectivity properties and sizes of circuits in the column dependence matroid of a random rxn matrix over a finite field, for large r and n. In a sense made precise in the paper, it is shown to be highly probable that when n is less than r such a matroid is the free matroid on n points, while if n exceeds r it is a connected matroid of rank r. Moreover, the connectivity can be strengthened under additional hypotheses on the growth of n and r using the notion of vertical connectivity; and the values of k for which circuits of size k exist can be determined in terms of n and r.

Section 1: Introduction.

In earlier joint papers (1982a, 1982b) and a paper by Oxley alone (1982) we considered the likely behavior of large matroids obtained by randomly and independently retaining (with probability p) or deleting (with probability 1-p) the elements of the finite projective geometry PG(r-1,q). Such a process produces a matroid without loops or multiple points (dependent singletons or pairs), but which has a random number of elements.

In the present paper we consider matroids obtained by randomly and independently choosing n elements of the r-dimensional vector space over GF(q) (the field with q elements, where q is a fixed prime power), allowing the zero vector to be chosen and allowing multiple choices of the same vector. That is, we consider the column dependence matroid of an rxn matrix whose entries are chosen independently and at random from GF(q). Such a matroid has n elements, possibly including loops and multiple points. Allowing the presence of such elements simplifies the calculation of probabilities and thus permits us to obtain more results.

In a sense that we will presently make precise, we show for such random matroids that for large r and n the following are highly probable: if n is less than r, then the matroid is the free matroid on n elements, while if n exceeds r then the

matroid is a connected matroid of rank r. Moreover, under additional hypotheses on the growth of r and n we obtain stronger results on the connectedness of the matroid and estimates of the likely sizes of its circuits.

A more detailed summary of these results will be given below, after we have discussed the terminology and notation we shall use.

Terminology. Let q be a fixed prime power and let $\{n_r\}$ be a sequence of positive integers. For r = 1,2,3,..., let M_r be an rxn_r matrix whose entries are chosen independently from GF(q), each member having probability 1/q of being chosen for any entry. (No assumption need be made concerning the independence of the M_r; they may be mutually independent, or if the n_r are increasing each may be a submatrix of the next.) We will use the symbol M_r to denote both the matrix and its column dependence matroid.

Most of our theorems state that under certain conditions involving the growth of the n_r, and for certain properties, say A, which a matroid may or may not possess, a series

$$\sum_r P[M_r \text{ does not have property A}]$$

converges. By the well-known first Borel-Cantelli Lemma (Lemma 2.1 below), it follows from such a conclusion that with probability 1 there exists a random integer R such that for all $r \geq R$, M_r has property A. To shorten such statements, we will attach the following meaning to the word eventually: if there exists an integer R such that a given property A(r) holds for all $r \geq R$, then we say that A(r) holds eventually. Thus a consequence of the convergence of the above series is that with probability 1 eventually M_r has property A.

We will follow Welsh (1976) for all matroid terminology that is not otherwise explained, with two exceptions. First, we will use rk M to denote the rank of a matroid M. Second, we will say that a matroid M is connected even if it contains loops, provided that deleting the loops leaves a matroid that is connected in the usual sense.

We will also use the O, o, and $\sim$ notations as they are customarily used. Thus, for example, $a_r = b_r + o(1)$ means that $a_r - b_r$ approaches 0 as r increases, and $a_r \sim b_r$ means that $\lim_{r\to\infty} a_r/b_r = 1$.

Summary of results. Section 3 concerns the rank of M_r. Its results imply that if n_r/r is eventually bounded below 1, then with probability 1 eventually M_r is the free matroid on n_r

elements; while if n_r/r is eventually bounded above 1, then with probability 1 eventually M_r has rank r.

In section 4 we show that if n_r/r is eventually bounded above 1, then with probability 1 eventually M_r is connected. Moreover, under additional hypotheses on the limiting value of n_r/r, we can make considerably stronger statements concerning the commectivity of M_r. To do this, we use the notion of vertical m-connectivity, the matroid generalization of the graph-theoretic concept of m-connectivity. Vertical m-connectivity was introduced by Tutte (1961, 1966) and has been studied by several authors including Cunningham (1981), Inukai and Weinberg (1981), and Oxley (1981). Theorem 4.4 provides that if n_r/r approaches a limit large enough to satisfy a certain inequality, then with probability 1 eventually M_r is vertically r-connected. For smaller limiting values of n_r/r, Theorem 4.5 gives in effect the vertical connectivity of M_r. A table at the end of the section gives, for various q, the critical limiting value of n_r/r for vertical r-connectivity and the vertical connectivity for various smaller limiting values of n_r/r.

In Section 5 we consider the existence of circuits of various sizes. Theorem 5.1 gives an asymptotic value for the probability that M_r has no circuits of size k_r, when $\{k_r\}$ is a

sequence with $k_r = o(n_r)$. Theorem 5.2 asserts, for a sequence $\{k_r\}$ for which k_r/n_r is bounded above zero, that with probability 1 eventually M_r has or does not have circuits of size k_r according as a certain quantity is eventually bounded below or above 1. A table at the end gives, for various q and various limiting values of n_r/r greater than 1, the size of the largest circuits that can be expected in M_r.

Related work. Our study of random matroids has from the beginning been motivated by the extensive theory of random graphs, begun by Erdös (1959) and Erdös and Rényi (1959, 1960). The subject is well expounded and documented in the books of Erdös and Spencer (1974) and Bollobas (1977) and the articles by Spencer (1978) and Bollobas (1981), and the reader is referred to these works and their bibliographies.

The only result obtained in our earlier papers that is directly comparable to a result of this paper is Theorem 2.1 in Kelly and Oxley (1982b). This theorem provides that rq^{-r} is a threshold probability for the property that a random submatroid of PG(r-1,q) have full rank. Otherwise stated: if the expected proportion of elements retained, which corresponds to $n_r q^{-r}$ in the present paper, is $o(rq^{-r})$, then with probability 1 eventually the rank is less than r; while if $rq^{-r} = o(n_r q^{-r})$,

then with probability 1 eventually the rank is r. This result corresponds precisely with the results of Section 3 of this paper.

Other work on random matrices appears in papers of Erdös and Rényi (1963, 1968) and of Komlós (1967, 1968). Erdös and Rényi are primarily concerned with the permanent of a random square matrix of zeroes and ones, while Komlós studies random matrices over the field of real numbers.

Section 2: Preliminary Lemmas.

Our first lemma will be used in most of our theorems to deduce the likely behavior of random matroids of large rank from the convergence of certain series. The remaining lemmas are elementary bounds from probability theory. Unexplained notions can be found in Feller (1968).

Lemma 2.1 (Borel-Cantelli). If $\{A_r\}$ is a sequence of events in a probability space and if $\sum_r P[A_r]$ converges, then with probability 1 there is a random integer R such that none of the A_r occur for $r \geq R$.

Proof can be found in Feller (1968).□

Lemma 2.2. If A, B, and C are events in a probability space and $P[B \cap C] > 0$, then

$$P[A] \leq P[A \cap B \cap C] + P[\text{not } B] + P[\text{not } C]$$

$$\leq P[A|B \cap C] + P[\text{not } B] + P[\text{not } C].$$

This follows easily from the definition of conditional probability. □

Lemma 2.3. If n and k are positive integers and $0 < k \leq n$, then

$$(\frac{n}{k})^k \leq \binom{n}{k} \leq (\frac{ne}{k})^k .$$

Proof. The first inequality is an easy inductive consequence of the inequality $\frac{a}{b} \leq \frac{a-1}{b-1}$, which is valid for $a \geq b > 1$. The second inequality follows because obviously $\binom{n}{k} \leq \frac{n^k}{k!}$ and because Stirling's formula $k^k e^{-k}(2\pi k)^{\frac{1}{2}}$ underestimates $k!$. □

Lemma 2.4 (The first- and second-moment methods). If X is a nonnegative integer-valued random variable, then

$$P[X > 0] \leq EX.$$

If X has finite variance, then

$$P[X = 0] \leq \frac{EX^2}{(EX)^2} - 1.$$

Proof. We omit the easy proof of the first assertion. A proof of the second is found in the paper of Kelly and Oxley (1982a). □

Section 3: Rank.

Let q be a fixed prime power, let $\{n_r\}$ be a sequence of positive integers, and for r = 1, 2, ..., let M_r be (the column dependence matroid of) an r x n_r matrix whose entries are chosen independently and at random from GF(q).

Theorem 3.1. If eventually $n_r \leq \alpha r$ for some α with $0 < \alpha < 1$, then

$$\sum_r P[\text{rk } M_r < n_r] < \infty.$$

Consequently, with probability 1, eventually M_r is the free matroid on n_r elements.

The proof appears below.

Corollary 3.2. If $\{n_r\}$ is arbitrary and $\{k_r\}$ is a sequence of positive integers with $k_r \leq n_r$ and eventually $k_r \leq \alpha r$ for some α with $0 < \alpha < 1$, then

$$\sum_r P[\text{the first } k_r \text{ columns of } M_r \text{ are dependent}] < \infty.$$

Consequently, with probability 1, eventually the first k_r

columns of M_r are independent. □

Corollary 3.3. If eventually $n_r \geq (1+\alpha)r$ for some $\alpha > 0$, then

$$\sum_r P[\text{rk } M_r < r] < \infty.$$

Consequently, with probability 1, eventually M_r has full rank r.

Proof of Corollary 3.3. Rearrange the sequence $\{n_r\}$ as $\{n_{r_j}\}$ so that $n_{r_1} \leq n_{r_2} \leq \ldots$, and let M_j^* be the transpose of M_{r_j}. The M_j^* form a subsequence of a sequence satisfying the hypotheses of the theorem, and the assertion follows. □

Proof of Theorem 3.1. The proof is in three steps:

1. A combinatorial argument and simple inequalities show that

$$P[\text{rk } M_r < n_r] = \sum_{j=0}^{n-1} P[\text{rk } M_r = j]$$

$$\leq \sum_{j=0}^{n-1} a_j,$$

where

$$a_j = \binom{n}{j} q^{(j-r)(n-j)} .$$

(Here and elsewhere we will drop the subscripts from n_r and k_r when it is convenient to do so.)

2. Consideration of the ratios a_{j+1}/a_j shows that for sufficiently large r, $a_0 \le a_1 \le \cdots \le a_{n-1}$.

3. Consequently, $P[\text{rk } M_r < r] \le na_{n-1}$, which is at most $r^2 q^{r(\alpha-1)}$. This is the r^{th} term in a convergent series.

Proof of 1: Let C denote the set of columns of M_r.

$$P[C \text{ is dependent}] = P[\text{all entries of } M_r \text{ are } 0]$$

$$+ \sum_{j=1}^{n-1} P[\text{some } j\text{-subset of C is a basis for } M_r]$$

$$\le q^{-rn} + \sum_{j=1}^{n-1} \binom{n}{j} P[\text{columns } 1,\ldots,j \text{ are a basis for } M_r]$$

$$= q^{-rn} + \sum_{j=1}^{n-1} \binom{n}{j} \frac{q^r-1}{q^r} \frac{q^r-q}{q^r} \cdots \frac{q^r-q^{j-1}}{q^r} \left(\frac{q^j}{q^r}\right)^{n-j}$$

$$\le \sum_{j=0}^{n-1} \binom{n}{j} \frac{q^{jr} q^{j(n-j)}}{q^{nr}}$$

$$= \sum_{j=0}^{n-1} a_j .$$

Proof of 2: For $j = 0,1, \ldots,n-2$,

$$\frac{a_{j+1}}{a_j} = \frac{n-j}{j+1} q^{r+n-2j-1}$$

$$\geq \frac{2}{n-1} q^{r+n-2(n-2)-1}$$

$$\geq (1/n) q^{r-n+3} .$$

But eventually $n \leq \alpha r$, and so

$$\frac{a_{j+1}}{a_j} \geq (1/\alpha r)\, q^{r(1-\alpha)+3} ,$$

and since $\alpha < 1$ this is eventually greater than 1. Hence eventually a_{n-1} is the largest among $a_1, \ldots, a_{n-1}$.

Proof of 3: Therefore

$$P[\text{the columns of } M_r \text{ are dependent}] \leq n a_{n-1}$$

$$= n^2 q^{n-r-1} \leq r^2 q^{(\alpha-1)r} .$$

Since $\alpha < 1$, this is the r^{th} term in a convergent series. □

Section 4: Connectivity and vertical connectivity.

In this section we show that when n_r/r is larger than 1, M_r is connected. Moreover, when n_r/r is larger than 2, the connectivity of M_r is considerably strengthened. It will be convenient to assume not merely that eventually $n_r/r \geq 1 + \alpha$ (where $1 < \alpha \leq \infty$), but that $\lim_{r\to\infty} n_r/r = 1 + \alpha$. Little generality is lost by this assumption, and our proofs will be simplified.

A matroid M of rank r is said to be vertically k-separated if there are two sets partitioning the ground set of M, each of rank at least k, such that the sum of their ranks equals r-1+k. For an integer $m \geq 2$, M is vertically m-connected if M is not vertically k-separated for any $k = 1, 2, \ldots, m-1$.

By way of illustration we mention three elementary properties of vertical m-connectivity. The third of these will be used in the proof of the next theorem.

Proposition 4.1. If M is the cycle matroid of a graph G, then M is vertically m-connected if and only if G is m-connected.

Proofs of this result are given independently in Theorem 1 of Cunningham (1981), Theorem 2 of Inukai and Weinberg (1981), and

Theorem 2 of Oxley (1981).□

Proposition 4.2. A matroid is vertically 2-connected if and only if it is connected.

This is (3.5) in the paper of Tutte (1961).□

Proposition 4.3. A matroid of rank r is vertically r-connected if and only if it is not the union of any two of its hyperplanes.

This is Theorem 5 of Inukai and Weinberg (1981) and also is on p. 208 of Oxley (1981).□

Theorem 4.4. If $\lim_{r\to\infty} n_r/r = 1 + \alpha$ where

(4.1) $$\ln(2q-1)/(2 \ln q - \ln(2q-1)) < \alpha \leq \infty,$$

then

$$\sum_r P[M_r \text{ is not vertically r-connected}] < \infty.$$

Consequently, with probability 1, eventually M_r is vertically r-

connected.

Proof.

$$P[M_r \text{ is not vertically r-connected}]$$

$$\leq P[M_r \text{ is not vertically r-connected} \mid \text{rk } M_r = r] + P[\text{rk } M_r < r].$$

But by Corollary 3.1b, since $n_r \geq (1+\alpha/2)r$ eventually, $\sum_r P[\text{rk } M_r < r] < \infty$, and so it suffices to show that $\sum_r \pi_r < \infty$, where

$$\pi_r = P[M_r \text{ is not vertically r-connected} \mid \text{rk } M_r = r].$$

By Proposition 4.3,

$$\pi_r = P[M_r \text{ is the union of two hyperplanes}]$$

$$\leq P[\text{every column of } M_r \text{ is in the union of some pair of hyperplanes of } V(r,q)]$$

$$\leq (\#\text{ hyperplanes of } V(r,q))^2 \, P[\text{a column is in the union of two distinct hyperplanes}]^n$$

$$= \left(\frac{q^r - 1}{q-1}\right)^2 \left(\frac{2q^{r-1} - q^{r-2}}{q^r}\right)^n$$

$$\leq q^{2r}((2q-1)/q^2)^n$$

$$= \left[q^2((2q-1)/q^2)^{n/r}\right]^r.$$

Now as $r \to \infty$ the quantity in brackets approaches 0 if $\alpha = \infty$ and approaches $(2q-1)^{1+\alpha}/q^{2\alpha}$ otherwise. Therefore the desired result follows if either $\alpha = \infty$ or if $(2q-1)^{1+\alpha} < q^{2\alpha}$; that is, if (4.1) holds. □

The next theorem gives sufficient conditions for vertical m-connectivity when $m < r$.

Theorem 4.5. Let $\{m_r\}$ be a sequence of integers with $1 \leq m_r \leq r$. Suppose that $\lim_{r\to\infty} m_r/r = t$ and $\lim_{r\to\infty} n_r/r = 1+\alpha$, where $0 \leq t < 1$ and $t < \alpha \leq \infty$. Then under any of the following conditions A, B, or C,

$$\sum_r P[\ M_r \text{ is not vertically } m_r\text{-connected }] < \infty,$$

and consequently, with probability 1, eventually M_r is vertically m_r-connected:

A. $0 < t < 1$ and $\alpha = \infty$.

B. $0 < t < 1$ and $t \ln((1+t)\alpha/t^2) < (\alpha-t)\ln q - 2t$.

C. $t = 0$.

On taking $m_r = 2$ for all $r \geq 2$ and using Proposition 4.2, we obtain the following:

Corollary 4.6. If eventually $n_r \geq (1+\alpha)r$ for some $\alpha > 0$, then $\sum_r P[M_r \text{ is not connected}] < \infty$. Consequently, with probability 1, eventually M_r is connected.

Before proving Theorem 4.5 we remark on Condition B and establish a lemma.

Notice that for fixed values of t and q, Condition B is always satisfied for sufficiently large α. Table 1 at the end of this section gives the smallest such value of α for various t

and q.

Lemma 4.7. If M is a random r×n matrix over GF(q) and D is any set of columns of M, then

$$P[\ M \text{ is vertically } k\text{-separated and } rk\ M = r \text{ and } D \text{ is independent }]$$

$$\leq \sum_{j=k}^{\lfloor \frac{1}{2}(r+k-1) \rfloor} \binom{n-|D|}{r+k-1-|D|} \binom{r+k-1}{j} \left[\frac{q^j + q^{r+k-1-j} - q^{k-1}}{q^r} \right]^{n-(r+k-1)}.$$

Proof. Suppose M has rank r and is vertically k-separated, and that D is an independent set of columns. Then for some j in $\{k, k+1, \ldots, \lfloor \frac{1}{2}(r+k-1) \rfloor\}$, there are sets X and Y of ranks j and r+k-1-j partitioning the set of columns of M, and they have bases X_0 and Y_0 containing $X_1 = X \cap D$ and $Y_1 = Y \cap D$, respectively. Let $X_2 = X_0 - X_1$ and $Y_2 = Y_0 - Y_1$. Let $E = X_2 \cup Y_2$.

Otherwise stated: there exists $E \subseteq M-D$ of size $r+k-1-|D|$ and a partition of $D \cup E$ into X_0 and Y_0 of sizes j and r+k-1-j, such that X_0 and Y_0 are independent; and all the other columns are either in the span of X_0 or in the span of Y_0.

The number of choices of such E, X_0, and Y_0 is

$$\binom{n-|D|}{r+k-1-|D|}\binom{r+k-1}{j},$$

and the probability for any such choice that the other columns are spanned by X_0 or by Y_0 is

$$\left[\frac{q^j+q^{r+k-1-j}-q^{k-1}}{q^r}\right]^{n-(r+k-1)}.$$

The result follows. □

Proof of Theorem 4.5.

First we notice that the sufficiency of A or the sufficiency of B implies that of C; for if $t = 0$ then we choose $t' > 0$ small enough that B holds (or choose t' arbitrarily if $\alpha = \infty$), and let $m_r' = \lfloor t'r \rfloor$, which is eventually greater than m_r since $m_r/r \to 0$. Then for sufficiently large r,

$$P[M_r \text{ is not vertically } m_r\text{-connected}]$$
$$\leq P[M_r \text{ is not vertically } m_r'\text{-connected}];$$

and because A or B holds the latter is the r^{th} term in a convergent series.

Now we prove the sufficiency of A and that of B. For any ϵ with $0 < \epsilon < 1$ let $D(r,\epsilon)$ (or simply D) denote the set consisting of the first $\lfloor r(1-\epsilon) \rfloor$ columns of M_r. Then by Lemma 4.6,

$$\begin{aligned} &P[M_r \text{ is not vertically } m_r\text{-connected}] \\ &\leq P_r + P[\text{rk } M_r < r] + P[D \text{ is dependent}], \end{aligned} \tag{4.2}$$

where

$$\begin{aligned} P_r = P[&M_r \text{ is not vertically } m_r\text{-connected, rk } M_r = r, \\ &\text{and } D \text{ is independent}]. \end{aligned}$$

By Corollaries 3.2 and 3.3, each of the last two terms in (4.2) is the r^{th} term in a convergent series; thus it suffices to show that $\sum_r P_r < \infty$. The sufficiency of A and of B for this will follow from the inequality

$$P_r \leq \frac{r^2}{2} \frac{n}{r} e B_r{}^r, \tag{4.3}$$

where

$$B_r = e^{\epsilon+2m/r} \left(\frac{1+m/r}{(m/r)^2}\right)^{m/r} (m/r)^{-\epsilon} \times$$

$$\times(-1+n/r)^{\epsilon+m/r}((1+q^{m-r})/q)^{(n/r)-(m/r)-1} .$$

The important quantity in this expression is

$$C_r = (1/q)(1 + q^{m-r}) = (1/q)(1 + q^{r(-1+m/r)}),$$

which approaches 1/q as r increases, because m/r approaches t, which is less than 1.

Before proving (4.3) we show how it implies the sufficiency of A and of B for the summability of $\sum_r P_r$.

All that is needed is to show that under each of these conditions, there is a choice of $\epsilon > 0$ for which $\lim_{r\to\infty} B_r < 1$.

Under condition A, $\lim_r B_r = 0$.

Under condition B,

$$\lim B_r = e^{2t+\epsilon}\ ((t+1)/t^2)^t\ t^{-\epsilon\alpha t+\epsilon q t-\alpha} ,$$

and there will exist $\epsilon > 0$ for which this is less than 1 if

$$e^{2t}((t+1)/t^2)^t \alpha^t q^{t-\alpha} < 1;$$

equivalently, if

$$\alpha^{-t} q^{\alpha} > (e^2(t+1)q/t^2)^t,$$

or

$$t \ln(e^2(1+t)q/t^2) < \alpha \ln q - t \ln \alpha,$$

and this is Condition B.

So we complete the proof of the theorem by proving (4.3). Now

$$P_r \leq \sum_{k=1}^{m-1} P[M_r \text{ is vertically k-separated, rk } M_r = r, \text{ and D is independent}],$$

and so according to Lemma 4.6,

$$P_r \leq \sum_{k=1}^{m-1} \sum_{j=k}^{\lfloor \frac{1}{2}(r+k-1) \rfloor} b(j),$$

where

$$b(j) = \binom{n-|D|}{r+k-1-|D|} \binom{r+k-1}{j} ((q^j + a^{r+k-1-j} - q^{k-1})/q^r)^{n-(r+k-1)}.$$

We proceed in three steps:

1. For sufficiently large r and for any k in {1, 2, ..., m-1},

$$b(k) \geq b(k+1) \geq \ldots \geq b(\lfloor (r+k-1)/2 \rfloor).$$

2. Consequently

$$P_r \leq \sum_{k=1}^{m-1} (r/2)b(k)$$

$$= (r/2) \sum_{k=1}^{m-1} \binom{n-|D|}{r+k-1-|D|} \binom{r+k-1}{k} ((q^k + q^{r-1} - q^{k-1})/q^r)^{n-(r+k-1)},$$

and we will find a bound on each term in this sum that is independent of k.

3. Finally we perform more manipulations to produce (4.3).

Details.

1. For any j in {k, k+1, ..., $\lfloor (r+k-1)/2 \rfloor - 1$},

$$b(j)/b(j+1) = \frac{j+1}{r+k-j-1} A^{n-(r+k-1)} ,$$

where

$$A = (q^j + q^{r+k-j-1} - q^{k-1})/(q^{j+1} + q^{r+k-j-2} - q^{k-1})$$

$$=(q^{j-k+1} + q^{r-j} - 1)/(q^{j-k+2} + q^{r-j-1} - 1) .$$

Now we show that

(4.4) $$A \geq \frac{q^2+1}{2q} .$$

This inequality is equivalent to

$$2q^{j-k+2} + 2q^{r-j+1} - 2q$$

$$\geq q^{j-k+4} + q^{r-j+1} - q^2 + q^{j-k+2} + q^{r-j-1} - 1;$$

that is, to

$$q^{r-j+1} - q^{r-j-1} + (q-1)^2 \geq q^{j-k+4} - q^{j-k+2} .$$

Ignoring $(q-1)^2$ and dividing by q^2-1, both of which are positive, we see that to prove (4.4) it is sufficient to show that $q^{r-j-1} \geq q^{j-k+2}$; that is, that $r+k-3 \geq 2j$. But this is true if

$$j \leq \left\lfloor \frac{r+k-1}{2} \right\rfloor - 1.$$

Thus (4.4) is proved. Also,

$$\frac{j+1}{r+k-j-1} \geq \frac{2}{r+k}$$

(as may be seen by cross-multiplying and noting that $j \geq 1$). Consequently

$$b(j)/b(j+1) \geq \frac{2}{r+k} \left(\frac{5}{4}\right)^{n-r-k+1} .$$

Because $k \leq m-1$,

$$b(j)/b(j+1) \geq \frac{2}{r+m} \left(\frac{5}{4}\right)^{n-r-m}$$

$$= \frac{2}{r(1+m/r)} \left(\frac{5}{4}\right)^{r\left(\frac{n}{r}-\frac{m}{r}-1\right)} .$$

But $\frac{n}{r} - \frac{m}{r} - 1$ approaches $\alpha - t$, which is positive; and

therefore for large r, b(j)/b(j+1) is positive for all j in $\{k, k+1, \ldots, \lfloor \frac{1}{2}(r+k-2) \rfloor - 1\}$.

2. Therefore

$$P_r \leq \sum_{k=1}^{m-1} \tfrac{1}{2} r\, b(k)$$

$$= \tfrac{1}{2} r \sum_{k=1}^{m-1} \binom{n-|D|}{r+k-1-|D|} \binom{r+k-1}{k} \left[\frac{q^k + q^{r-1} - q^{k-1}}{q^r}\right]^{n-(r+k-1)}.$$

To bound the binomial coefficients we use Lemma 2.3.

$$\binom{r+k-1}{k} = \binom{r+k-1}{r-1} \leq \binom{r+m-1}{r-1}$$

$$= \binom{r+m-1}{m} \leq \binom{r+m}{m} \leq \left(\frac{(r+m)e}{m}\right)^m.$$

Also,

$$\binom{n-|D|}{r+k-1-|D|} = \binom{n-r+v}{k-1+v} \leq \left[\frac{(n-r+v)e}{k-1+v}\right]^{k-1+v},$$

where v denotes $\lceil r\epsilon \rceil$.

Now because $(a/x)^x$ is increasing for $0 < x \leq a/e$, and because (for sufficiently large r) $m+v \leq n-r+v$, it follows that

$$\binom{n-|D|}{r+k-1-|D|} \leq \left(\frac{(n-r+v)e}{m+v}\right)^{m+v}$$

$$\leq \left(\frac{(n-r+r\epsilon+1)e}{m+r\epsilon}\right)^{m+r\epsilon+1} .$$

In addition,

$$\left[\frac{q^k+q^{r-1}-q^{k-1}}{q^r}\right]^{n-(r+k-1)} \leq \left[\frac{q^k+q^{r-1}-q^{k-1}}{q^r}\right]^{n-(r+m-1)}$$

(because the quantity in parentheses is less than 1)

$$\leq \left[\frac{q^{r-1}+q^{m-2}(q-1)}{q^r}\right]^{n-(r+m)} .$$

Therefore

$$P_r \leq \tfrac{1}{2}rm\left[\frac{(n-r+r\epsilon+1)e}{m+r\epsilon}\right]^{m+r\epsilon+1} \left(\frac{(r+m)e}{m}\right)^m \left[\frac{q^{r-1}+q^{m-2}(q-1)}{q^r}\right]^{n-(r+m)} .$$

3. Now we express the above bound as much as possible as an r^{th} power of quantities involving m/r and n/r, which we denote

by M and N, respectively.

$$rm/2 = \frac{r^2}{2} M \; ; \qquad \frac{r+m}{m} = 1 + \frac{1}{M} \; ;$$

$$\frac{n-r+r\epsilon+1}{m+r\epsilon} = \frac{N-1+\epsilon+(1/r)}{M+\epsilon} \leq \frac{N-1}{M} \text{ for large } r;$$

$$\frac{q^{r-1}+q^{m-2}(q-1)}{q^r} = (1+q^{m-r-1}(q-1))/q \leq (1+q^{m-r})/q \; ;$$

and therefore

$$P_r \leq \frac{r^2}{2} M \left[\frac{(N-1)e}{M}\right]^{r(M+\epsilon+(1/r))} (e(1+\tfrac{1}{M}))^{rM} \left[(1+q^{m-r})/q\right]^{r(N-M-1)}$$

$$= \frac{r^2}{2} (N-1)eB_r{}^r \leq \frac{r^2}{2} NeB_r{}^r,$$

where

$$B_r = \left[\frac{(N-1)e}{M}\right]^{M+\epsilon} (e(1+\tfrac{1}{M}))^{M} \left[(1+q^{m-r})/q\right]^{N-M-1}$$

$$= e^{2M+\epsilon} \left[\frac{M+1}{M^2}\right]^{M} M^{-\epsilon} (N-1)^{M+\epsilon} \left[(1+q^{m-r})/q\right]^{N-M-1} . \square$$

The following table shows, for selected values of q and selected limiting values of n/r, the supremum of the values of

t for which Condition B of Theorem 4.5 holds. (Note that the α of Theorem 4.5 is one less than the limiting value of n/r.) Values in the table are to three decimal places, rounded down. Roughly speaking, for a given value of q and ratio of n to r, one can expect a large rxn matroid over GF(q) to be vertically m-connected if m/r is less than the tabulated value of t.

In addition, the rightmost column of the table shows, for each q, the infimum of the limiting values of n/r for which the hypothesis of Theorem 4.4 is satisfied. Values are rounded up. Roughly speaking, for a given value of q, one can expect a large rxn matroid over GF(q) to be vertically r-connected if n/r exceeds the tabulated value.

Table 1.

limiting value of $\frac{n}{r}$ for r-connectivity

q	1.01	1.05	1.1	1.2	1.5	2.0	2.5	3.0	
2	.0005	.003	.006	.014	.041	.091	.147	.205	3.82
3	.0008	.005	.011	.024	.070	.158	.254		2.74
4	.001	.006	.014	.031	.091	.205			2.35
5	.001	.007	.016	.037	.107	.241			2.15
7	.001	.009	.020	.045	.130				1.93
8	.001	.010	.022	.048	.139				1.87
9	.001	.010	.023	.051	.146				1.81
16	.002	.013	.028	.063	.180				1.63
31	.002	.016	.034	.075					1.49
43	.002	.017	.037	.081					1.44
125	.003	.020	.044	.096					1.33
2^{10}	.004	.026	.055	.118					1.22
2^{20}	.006	.073							1.11

Section 5: Existence of circuits.

Again we let M_r be (the column dependence matroid of) a random r x n_r matrix over GF(q). From Theorem 3.1 we have that if eventually $n_r < \theta r$ for some $\theta < 1$, then with probability 1 eventually M_r has no circuits at all. Consequently we shall assume that eventually $n_r \geq \theta r$ for some $\theta > 0$. (The natural assumption, that n_r/r is eventually bounded above 1, is stronger than what is needed for our results.)

Let $\{k_r\}$ be a sequence of nonnegative integers, and for r = 1, 2, ..., let C_r denote the number of k_r-circuits in M_r.

Our first theorem concerns small circuits; that is, the case in which k_r/n_r approaches zero as r increases. In its proof, as elsewhere, we shall freely drop the subscripts from n_r and k_r.

Theorem 5.1. Let

$$a_r = \frac{(q-1)^{k_r-1}}{k_r!} \frac{n_r^{k_r}}{q^r} .$$

Suppose that $\lim_{r\to\infty} k_r/n_r = 0$ and also that $n_r^{k_r} q^{-r}$ is bounded. Then

$$P[C_r = 0] \sim e^{-a_r} .$$

Proof. For any r and k, let $D_r(k)$ denote the number of circuits of sizes 0,1,2,...,k in M_r. Then

$$P[C_r=0] - P[D_r(k)=0] = 1 - P[D_r(k-1)=0].$$

We complete the proof by showing that

$$P[D_r(k-1)=0) \to 1 \text{ and } P[D_r(k)=0] \sim e^{-a_r}.$$

Now the event $[D_r(k) = 0]$ is the intersection of E_0, E_k, E_{k+1}, ..., E_n, where: E_0 is the event that the first k-1 columns are independent, and for j = k, k+1, ..., n, E_j is the event that column j is not 0 or a linear combination of k-1 of the first j-1 columns. For these events we have

$$P[E_0] = \frac{q^r-1}{q^r} \frac{q^r-q}{q^r} \cdots \frac{q^r-q^{k-2}}{q^r} ;$$

$$P[E_k|E_0] = 1 - q^{-r} \sum_{i=0}^{k-1} \binom{k-1}{i}(q-1)^i ;$$

$$P[E_{k+1}|E_0 \text{ and } E_k] = 1 - q^{-r} \sum_{i=0}^{k-1} \binom{k}{i}(q-1)^i ;$$

etc. Hence

$$P[D_r(k)=0] = \frac{q^r-1}{q^r}\,\frac{q^r-q}{q^r}\,\ldots\,\frac{q^r-q^{k-2}}{q^r}\,\prod_{j=k-1}^{n-1}\left[1-q^{-r}\sum_{i=0}^{k-1}\binom{j}{i}(q-1)^i\right] .$$

Now

$$\frac{q^r-1}{q^r}\,\frac{q^r-q}{q^r}\,\ldots\,\frac{q^r-q^{k-2}}{q^r}$$

$$= (1 - q^{-r})(1 - q^{-r+1})\ldots(1 - q^{-r+k-2})$$

$$\geq 1 - q^{-r}\sum_{i=0}^{k-2} q^i \geq 1 - q^{-r+k-1}.$$

Since $n^k\, q^{-r}$ is bounded and $\lim_{r+\infty} \frac{k}{n} = 0$, eventually $k \leq \frac{1}{2}r$. Thus

$$\frac{q^r-1}{q^r}\,\frac{q^r-q}{q^r}\,\ldots\,\frac{q^r-q^{k-2}}{q} \to 1 \text{ as } r \to \infty.$$

Consequently we complete the proof by showing

$$\text{(5.1)} \qquad \prod_{j=k-1}^{n-1}\left[1 - q^{-r}\sum_{i=0}^{k-1}\binom{j}{i}(q-1)^i\right] \sim e^{-a_r+o(1)}$$

and

$$(5.2) \qquad \prod_{j=k-2}^{n-1}\left[1 - q^{-r}\sum_{i=0}^{k-2}\binom{j}{i}(q-1)^i\right] \to 1.$$

Proof of (5.1): Denote the left side of (5.1) by A_r. If $x \leq \frac{1}{2}$, then

$$\ln(1-x) = -x - K(x)x^2 \qquad \text{where } \tfrac{1}{2} \leq K(x) \leq 1.$$

We now obtain a uniform upper bound on

$$q^{-r}\sum_{i=0}^{k-1}\binom{j}{i}(q-1)^i$$

for all j such that $k-1 \leq j \leq n-1$, that will enable us to apply the above observation to get $\ln A_r$.

$$q^{-r}\sum_{i=0}^{k-1}\binom{j}{i}(q-1)^i$$

$$\leq q^{-r}\binom{n-1}{k-1}\sum_{i=0}^{k-1}(q-1)^i \qquad \text{(for large r)}$$

$$\leq q^{-r} \left[\frac{(n-1)e}{k-1}\right]^{k-1} \sum_{i=0}^{k-1} (q-1)^i \qquad \text{(by Lemma 2.3)}$$

$$\leq q^{-r} \left[\frac{(n-1)e}{k-1}\right]^{k-1} q^{k-1}$$

$$\leq \frac{1}{n} n^k q^{-r} \left(\frac{eq}{k-1}\right)^{k-1} .$$

Since $n^k q^{-r}$ is bounded, the last expression approaches 0 as $r \to \infty$. Therefore eventually

$$\ln A_r = - \sum_{j=k-1}^{n-1} q^{-r} \sum_{i=0}^{k-1} \binom{j}{i} (q-1)^i - B_r,$$

where

$$B_r = \sum_{j=k-1}^{n-1} K_j \left[q^{-r} \sum_{i=0}^{k-1} \binom{j}{i} (q-1)^i\right]^2$$

and $\frac{1}{2} \leq K_j \leq 1$ for all j. Thus eventually

$$B_r \le \sum_{j=k-1}^{n-1} \left[q^{-r} \sum_{i=0}^{k-1} \binom{j}{i} (q-1)^i \right]^2$$

$$\le \sum_{j=k-1}^{n-1} \left[\frac{1}{n} n^k q^{-r} \left(\frac{eq}{k-1} \right)^{k-1} \right]^2$$

$$\le n \left[\frac{1}{n} n^k q^{-r} \left(\frac{eq}{k-1} \right)^{k-1} \right]^2 .$$

As $n^k q^{-r}$ is bounded, it follows that $B_r = o(1)$ and so

$$\ln A_r = -q^{-r} \sum_{i=0}^{k-1} (q-1)^i \sum_{j=k-1}^{n-1} \binom{j}{i} + o(1)$$

$$= -q^{-r} \sum_{i=0}^{k-1} (q-1)^i \left[\binom{n}{i+1} - \binom{k-1}{i+1} \right] + o(1)$$

$$= -\binom{n}{k} (q-1)^{k-1} q^{-r} - F_r + o(1),$$

where

$$F_r = q^{-r} \sum_{i=0}^{k-2} (q-1)^i \left[\binom{n}{i+1} - \binom{k-1}{i+1} \right]$$

$$\leq q^{-r} \sum_{i=0}^{k-2} (q-1)^i \binom{n}{i+1}$$

$$\leq \binom{n}{k-1} q^{-r} \sum_{i=0}^{k-2} (q-1)^i \qquad \text{(for large r)}$$

$$\leq \binom{n}{k-1} q^{-r} q^{k-2}$$

$$\leq \left(\frac{ne}{k-1}\right)^{k-1} q^{-r} q^{k-2} \qquad \text{(by Lemma 2.3)}$$

$$\leq \frac{1}{n} n^k q^{-r} \left(\frac{eq}{k-1}\right)^{k-1}$$

$$= o(1).$$

Thus

$$\ln A_r = -q^{-r}(q-1)^{k-1}\binom{n}{k} + o(1)$$

$$= - \frac{q^{-r}(q-1)^{k-1}n^k}{k!} + o(1)$$

$$= -a_r + o(1).$$

Proof of (5.2): The left side is bounded below for large r by

$$\left[1 - q^{-r} \sum_{i=0}^{k-2} \binom{n-1}{i}(q-1)^i\right]^n ,$$

and for large r this is greater than

$$\left[1 - \binom{n-1}{k-2}q^{-r} \sum_{i=0}^{k-2} (q-1)^i\right]^n$$

$$\geq \exp\left[-n\binom{n-1}{k-2}q^{-r} \sum_{i=0}^{k-2} (q-1)^i\right]$$

$$\geq \exp\left[-n\binom{n-1}{k-2}q^{-r}q^{k-2}\right],$$

and so it remains only to show that $n\binom{n-1}{k-2}q^{-r}q^{k-2} \to 0$. But

$$n\binom{n-1}{k-2}q^{-r}q^{k-2} \leq n\left[\frac{(n-1)e}{k-2}\right]^{k-2} q^{-r}q^{k-2}$$

$$\leq \frac{1}{n} n^k q^{-r} \left(\frac{eq}{k-2}\right)^{k-2}.$$

Again since $n^k q^{-r}$ is bounded, the result follows. □

Our final theorem concerns large circuits; that is, the case in which k_r/n_r is bounded away from 0. Our proof uses the first- and second-moment methods, employing the inequalities of Lemma 2.4. Before proceeding to the theorem we obtain estimates for the bounds given by that lemma for the random variable C_r. Again we drop the subscripts from n_r and k_r when it is convenient to do so.

Lemma 5.2.

$$EC_r = \binom{n}{k} T(r,k-1) \frac{(q-1)^{k-1}}{q^r}, \tag{5.3}$$

and

$$\frac{EC_r^2}{(EC_r)^2} - 1 \leq \sum_{j=0}^{k-1} \frac{\binom{n-k}{k-j}\binom{k}{j}}{\binom{n}{k}} [S(r,j)-1]$$

(5.4)

$$+ \frac{1}{\binom{n}{k}} \left[S(r,k-1) \frac{q^r}{(q-1)^{k-1}} - 1 \right] ,$$

where

$$T(r,j) = \frac{q^r-1}{q^r} \frac{q^r-q}{q^r} \cdots \frac{q^r-q^{j-1}}{q^r}$$

and

$$S(r,j) = \frac{1}{T(r,j)} .$$

Proof. For any k-set J of columns let

$$X_J = \begin{cases} 1 \text{ if } J \text{ is a circuit,} \\ 0 \text{ if not.} \end{cases}$$

Then

$$c_r = \sum_{|J|=k} X_J .$$

Now $J = \{c_1,\ldots,c_k\}$ is a circuit if and only if $c_1,\ldots,c_{k-1}$ are independent and c_k is a linear combination of them with all coefficients nonzero. Therefore

$$EX_J = EX_J^2 = P[J \text{ is a circuit}]$$

$$= \frac{q^r-1}{q^r} \frac{q^r-q}{q^r} \cdots \frac{q^r-q^{k-2}}{q^r} \frac{(q-1)^{k-1}}{q^r} ,$$

and (5.1) follows.

Now

$$EC_r^2 = \sum_{(J,K)} E(X_J X_K) ,$$

the sum extending over all ordered pairs of k-sets. This sum equals

$$\sum_{j=0}^{k-1} \sum_{(J,K)}^{(j)} E(X_J X_K) + \sum_J EX_J^2,$$

where $\sum_{(J,K)}^{(j)}$ indicates a sum extending over ordered pairs of k-sets whose intersections have j elements, and $\sum_J$ indicates a sum over all k-sets.

Now suppose that J and K are k-sets whose intersection is a j-set for some j, $0 \leq j < k$; say

$$J = \{c_1,\ldots,c_j,c_{j+1},\ldots,c_k\} , \quad K = \{c_1,\ldots,c_j,c'_{j+1},\ldots,c'_k\}.$$

If J and K are both circuits, then $\{c_1,\ldots,c_j,c_{j+1},\ldots,c_{k-1}\}$ and $\{c_1,\ldots,c_j,c'_{j+1},\ldots,c'_{k-1}\}$ are independent, and each of c_k, c'_k is a linear combination of an independent (k-1)-set with all coefficients nonzero. Therefore

$$EX_JX_K = P[J \text{ and } K \text{ are both circuits}]$$

$$= \frac{q^r-1}{q^r}\frac{q^r-q}{q^r}\cdots\frac{q^r-q^{j-1}}{q^r}\left[\frac{q^r-q^j}{q^r}\cdots\frac{q^r-q^{k-2}}{q^r}\frac{(q-1)^{k-1}}{q^r}\right]^2$$

$$= T(r,k-1)^2\,S(r,j)\left[\frac{(q-1)^{k-1}}{q^r}\right]^2 .$$

Also, for $0 \le j < k$, the number of ordered pairs of k-sets whose intersections are j-sets is $\binom{n}{k}\binom{k}{j}\binom{n-k}{k-j}$. Consequently

$$EC_r^2 \le \sum_{j=0}^{k-1}\binom{n}{k}\binom{k}{j}\binom{n-k}{k-j}T(r,k-1)^2S(r,j)\left[\frac{(q-1)^{k-1}}{q^r}\right]^2$$

$$+ \binom{n}{k}T(r,k-1)\frac{(q-1)^{k-1}}{q^r} ,$$

and so

$$\frac{EC_r^2}{(EC_r)^2} \le \sum_{j=0}^{k-1}\frac{\binom{k}{j}\binom{n-k}{k-j}}{\binom{n}{k}}S(r,j) + \frac{1}{\binom{n}{k}}S(r,k-1)\frac{q^r}{(q-1)^{k-1}} .$$

(5.2) follows upon observing that

$$\sum_{j=0}^{k-1} \frac{\binom{k}{j}\binom{n-k}{k-j}}{\binom{n}{k}} + \frac{1}{\binom{n}{k}} = 1,$$

because this is the sum of the probabilities for a hypergeometric distribution. □

Theorem 5.3. Suppose $\{k_r\}$ is a sequence of positive integers such that $k_r < n_r$, $k_r \leq r+1$, and eventually $k_r/n_r \geq \gamma$ for some positive γ. Define

$$b_r = \frac{n_r}{k_r}\left[1 - \frac{k_r}{n_r}\right]^{1-(n_r/k_r)} \frac{q-1}{q^{r/k_r}} .$$

Also assume that eventually $n_r \geq \theta r$ for some positive θ.

a. If eventually $b_r \leq \alpha$ for some α with $0 < \alpha < 1$, then $\sum_r P[C_r > 0]$ converges.

b. If eventually $b_r \geq \beta$ for some $\beta > 1$, and if eventually $k_r/n_r \leq \delta$ for some $\delta < 1$, then $\sum_r P[C_r = 0]$ converges.

Consequently, with probability 1, eventually M_r has no k_r-circuits if b_r is bounded below 1, and M_r has at least one k_r-circuit if b_r is bounded above 1 and k_r/n_r is bounded below 1.

At the end of this section is a table showing, for various values of q and limiting values of n_r/r, the supremum of values of k for which b_r exceeds 1.

Proof. Again we write k and n for k_r and n_r.

Proof of a:

$$P[C_r > 0] \leq EC_r = \binom{n}{k} T(r,k-1) \frac{(q-1)^{k-1}}{q^r}$$

$$\leq \binom{n}{k} \frac{(q-1)^{k-1}}{q^r} . \tag{5.5}$$

Stirling's formula implies that eventually

$$\binom{n}{k} \leq \frac{1}{y}\left[\frac{n}{k}\right]^k \left[\frac{n}{n-k}\right]^{n-k} .$$

Hence eventually

$$P[C_r > 0] \leq \frac{1}{y}\left[\frac{n}{k}\right]^k \left[\frac{n}{n-k}\right]^{n-k} \frac{(q-1)^k}{q^r}$$

$$\sim \frac{1}{y}\left[\frac{n}{k}\left(1 - \frac{k}{n}\right)^{1-\frac{n}{k}} \frac{(q-1)}{q^{r/k}}\right]^k$$

$$= \frac{1}{y} b_r{}^k .$$

Assertion a follows.

Proof of b: From Lemmas 5.2 and 2.4 we get

$$P[C_r = 0] \leq D_r + E_r + F_r,$$

where

$$D_r = \sum_{j=0}^{\lfloor k-3\log_q k \rfloor} \frac{\binom{n-k}{k-j}\binom{k}{j}}{\binom{n}{k}} [S(r,j)-1],$$

$$E_r = \sum_{j=\lfloor k-3\log_q k \rfloor+1}^{k-1} \frac{\binom{n-k}{k-j}\binom{k}{j}}{\binom{n}{k}} [S(r,j)-1],$$

and

$$F_r = \frac{1}{\binom{n}{k}}\left[S(r,k-1)\frac{q^r}{(q-1)^{k-1}} - 1\right] .$$

We show in turn that $\sum_r F_r$, $\sum_r D_r$, and $\sum_r E_r$ all converge if eventually $b_r \geq \beta > 1$.

$\sum_r F_r$:

$$T(r,j) = \prod_{i=0}^{j-1} (1 - q^{-r+i})$$

$$\geq \prod_{i=1}^{\infty} (1 - q^{-i}) ,$$

which is a positive constant, say C. Therefore $S(r,k-1) \leq 1/C$, and

$$F_r \leq \frac{1}{\binom{n}{k}} \frac{q^r}{(q-1)^{k-1}} \frac{1}{C}.$$

But this is a constant multiple of the reciprocal of the quantity (5.5), and that quantity is summable if b_r is bounded below 1. Therefore F_r is summable if b_r is bounded above 1.

$\sum_r D_r$: First notice that

$$S(r,j) - 1 \leq \left[\frac{q^r}{q^r - q^{j-1}}\right]^j - 1$$

$$\leq \left[1 + \frac{1}{q^{r-j}}\right]^j - 1.$$

But for $j \leq k - 3 \log_q k$, $r-j \to \infty$ as r increases, and hence asymptotically for these j,

$$S(r,j) - 1 \leq e^{j/q^{r-j}} - 1.$$

Thus

$$D_r \leq \sum_{j=0}^{\lfloor k-3\log_q k \rfloor} \frac{\binom{n-k}{k-j}\binom{k}{j}}{\binom{n}{k}} \left[e^{j/q^{r-j}} - 1 \right].$$

Because the ratios involving binomial coefficients are hypergeometric probabilities (see Feller (1968)),

$$D_r \leq \exp\left[k/q^{r-k+3\log_q k} \right] - 1$$

$$= \exp(k^{-2}q^{-r+k}) - 1.$$

Because $e^x - 1 \leq 2x$ for small positive x, eventually

$$D_r \leq \frac{2}{k^2 q^{r-k}} .$$

But eventually $k_r \geq \gamma\theta r$, and hence $\sum_r D_r$ converges.

$\sum_r E_r$: As already noted, $S(r,j) - 1$ is bounded above by a positive constant if b_r is bounded above 1. So it suffices to show that if

$$G_r = \sum_{j=\lfloor k-3\log_q k \rfloor+1}^{k-1} \frac{\binom{n-k}{k-j}\binom{k}{j}}{\binom{n}{k}},$$

then $\sum_r G_r$ converges. But writing h for $\lceil 3 \log_q k \rceil$, we have

$$G_r \leq h \frac{\binom{n-k}{h}\binom{k}{k-h}}{\binom{n}{k}} = h \frac{\binom{n-k}{h}\binom{k}{h}}{\binom{n}{k}} .$$

Using Lemma 2.3, we get

$$G_r \leq h\left(\frac{(n-k)e}{h}\right)^h \left(\frac{ke}{h}\right)^h \left(\frac{n}{k}\right)^{-k}$$

$$= h(\frac{e}{h})^{2h} [k(n-k)]^h (\frac{k}{n})^k$$

$$\leq h(\frac{e}{h})^{2h} (\frac{n^2}{4})^h (\frac{k}{n})^k$$

$$= h(\frac{en}{2h})^{2h} (\frac{k}{n})^k.$$

Now our hypotheses imply that $n \leq k/\gamma$ and $\frac{k}{n} \leq \delta < 1$; hence

$$G_r \leq h(\frac{ek}{2\gamma h})^{2h} \delta^k ;$$

because $h = O(\log k)$ this is dominated by δ^k, and because $k \geq \gamma n \geq \gamma\theta r$, $\sum_r G_r$ is summable. □

The following table shows, for selected values of q and selected limiting values of n/r, the supremum of the values of k/r for which the hypotheses of Part b of Theorem 5.3 hold. Values are to three decimal places, rounded down. Roughly

speaking, for a given value of q and ratio of n to r, one can expect a large r x n matroid to have circuits of all sizes less than the tabulated fraction of r.

Table 2.

limiting value of $\frac{n}{r}$

q	1.01	1.5	2.0	5.0	10.0	100
2	.445	.260	.220	.155	.129	.086
3	.603	.373	.318	.231	.195	.132
4	.683	.437	.378	.279	.238	.163
9	.827	.577	.511	.394	.342	.242
25	.911	.687	.622	.500	.442	.324
125	.960	.786	.729	.614	.556	.428
2^{10}	.981	.852	.805	.706	.652	.526
2^{20}	.994	.928	.900	.837	.799	.699

REFERENCES

Bollobás, B. (1977). Graph Theory: An Introductory Course. Graduate texts in Mathematics no. 63, Springer-Verlag, New York, Heidelberg, Berlin.

Bollobás, B. (1981). Random graphs. Pp. 80 - 102 of Combinatorics (H. N. V. Temperley, ed.), London Math. Soc. Lecture Notes No. 52, Cambridge University Press, Cambridge.

Cunningham, W. H. (1981). On matroid connectivity. J. Comb. Theory B 30, 94-99.

Erdös, P. (1959). Graph theory and probability. Canad. J. Math. 11, 34-38.

Erdös, P. and Rényi, A. (1959). On random graphs I. Publ. Math. Debrecen 6, 290-297.

Erdös, P. and Rényi, A. (1960). On the evolution of random graphs. Publ. Math. Inst. Hungar. Acad. Sci. 5, 17-61.

Erdös, P. and Rényi, A. (1961). On the strength of connectedness of a random graph. Acta Math. Acad. Sci. Hungar. 12, 261-267.

Erdös, P. and Rényi, A. (1963). On random matrices. Magyar Tud. Akad. Mat. Kutato Int. Közl. 8, 455-461.

Erdös, P. and Rényi, A. (1968). On random matrices, II. Stud. Sci. Math. Hungar. 3, 459-464.

Erdös, P. and Spencer, J. (1974). Probabilistic Methods in Combinatorics. Academic Press, New York.

Feller, W. (1968). An Introduction to Probability Theory and its Applications, third edition. John Wiley and Sons, New York.

Inukai, T. and Weinberg, L. (1981). Whitney connectivity of matroids. SIAM J. Alg. Disc. Methods 2, 108-120.

Kelly, D. and Oxley, J. (1982a). Asymptotic properties of random subsets of projective spaces. Math. Proc. Camb. Phil. Soc. 91, 119-130.

Kelly, D. and Oxley, J. (1982b). Threshold functions for some properties of random subsets of projective spaces. Quart. J. Math. Oxford (Ser. 2) 33, 463-469.

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

Komlós, J. (1968). On the determinant of random matrices. Stud. Sci. Math. Hung. 3, 387-399.

Oxley, J. (1981). On a matroid generalization of graph connectivity. Math. Proc. Camb. Phil. Soc. 90, 207-214.

Oxley, J. (1982). Threshold distribution functions for some random representable matroids. To appear.

Spencer, J. (1978). Nonconstructive methods in discrete mathematics. Pp. 142-178 of Studies in Combinatorics (G.-C. Rota, ed.) MAA Studies in Mathematics 17, Mathematical Association of America, Providence.

Tutte, W. (1961). A theory of 3-connected graphs. Nederl. Akad. Wetensch. Proc. (A) 64, 441-455.

Tutte, W. (1966). Connectivity in matroids. Canad. J. Math. 18, 1301-1324.

Welsh, D. (1976). Matroid Theory. London Math. Soc. Monographs No. 8, Academic Press, London, New York.