Connectivity in Random Matroids

W.M.B. Dukes*

November 12, 1998

Abstract

We look at $f_M(p)$, the probability that a random matroid (generated by a bernoulli measure on its ground set) is 2-connected. Upper and lower bounds on this value are proven in terms of the number of circuits and dependent sets of the matroid. Another inequality is presented for the case where M is known in terms of connected components. Some results as regards matroid enumeration are given at the end.

1 Introduction

Several authors have published papers on "Random Matroids", although each seems to have his own view on what a random matroid is. Reif and Spirakis [5] were concerned with the probability of a structure being a matroid. Alternatively, Knuths' paper [1] exhibited an algorithm to generate all possible matroids, the *random* element enters in the choice of including sets at stages during the algorithm. The random matroid we look at was introduced by Lomonosov [3] and recently the subject of futher research by Kordecki [2], very much analagous to the idea of a random graph. Given a matroid structure, we look at submatroids of the matroid generated by a bernoulli measure on the ground set.

A matroid $M(S, \mathcal{I})$ is a set S, called the *ground set* of M, together with a set $\mathcal{I}$ which is a collection of subsets of S, called the independent sets of M, satisfying the following axioms;

*School of Theoretical Physics, Dublin Institute for Advanced Studies, 10 Burlington Rd, Dublin 4, IRELAND. E-mail: dukes@stp.dias.ie
DIAS-APG-98-12

I1 $\emptyset \in \mathcal{I}$

I2 A$\in \mathcal{I}$, B $\subseteq$A $\Rightarrow$ B $\in \mathcal{I}$

I3 If A,B $\in \mathcal{I}$ and |A| < |B|, then $\exists\ x \in$ B\A s.t. A$\cup\{x\} \in \mathcal{I}$

A non-independent set is called a *dependent* set, a *circuit* is a minimal dependent set, a *base* is a maximal independent set. Let $\mathcal{D}$ denote the set of dependent sets of M, $\mathcal{C}$ the set of circuits, $\mathcal{B}$ the set of bases. The *rank* of $A \subseteq S$, written ρA, is the size of the largest independent set contained within A. We say that a matroid $M(S,\mathcal{I})$ is $2-$*connected* (herein *connected*) if $\rho A + \rho(S\backslash A) > \rho S$, for all proper $A \subset S$. An equivalent, a maybe more intuitive, condition for connectedness is the statement: connected iff every pair of distinct ground set elements are contained within at least one circuit. The *restriction* of a matroid M to a set A is $M_{|A}$, the submatroid $M'(A,\mathcal{I}_A)$, where $\mathcal{I}_A := \{I \cap A | I \in \mathcal{I}\}$. A random matroid $\omega(M,p)$ is a submatroid of a matroid $M(S,\mathcal{I})$ such that;

$$P(\omega(M,p) = M_{|A}) = p^{|A|}q^{|S|-|A|},$$

where $A \subseteq S$ and $q = 1-p$ throughout.

2 Connectedness

The idea of a random structure possessing a certain property is fundamental to the theory of random structures. Several authors have investigated the property of a random matroid possessing the same rank as the original matroid. Here we examine the property of connectedness. Let $f_M(p)$ denote the probability that the random matroid $\omega(M,p)$ is connected, then;

$$\begin{aligned} f_M(p) &= \sum_{A\subseteq S} P(\omega(M,p) = M_{|A})\mathbb{I}\{M_{|A} \textit{ is connected}\} \\ &= \sum_{A\subseteq S} p^{|A|}q^{|S|-|A|}.\prod_{X\subset A} \mathbb{I}\{\rho X + \rho(A\backslash X) > \rho A\} \qquad (1) \end{aligned}$$

Note that we have; $f_M(0) = 1$, $f'_M(0) = 0$, $f'_M(1) = 0$ for all matroids M. If M itself is connected, then $f_M(1) = 1$, otherwise $f_M(1) = 0$.

2.1 Upper and lower bounds on $f_M(p)$

Lemma 1 $|\mathcal{C}|\min\{p^{|S|},q^{|S|}\} \leq f_M(p) \leq |\mathcal{D}|\max\{p^{|S|},q^{|S|}\}$.

Proof:

For the left inequality, we Notice that if C is a circuit and $X \subset C$, $\rho X + \rho(C\backslash X) = |C| > \rho C$. So from (1) ;

$$\begin{aligned} f_M(p) &= \sum_{A\subseteq S} p^{|A|}q^{|S|-|A|}\prod_{X\subset A} \mathbb{I}\{\rho X + \rho(A\backslash X) > \rho A\} \\ &\geq \sum_{A\in\mathcal{C}} p^{|A|}q^{|S|-|A|}\prod_{X\subset A} \mathbb{I}\{\rho X + \rho(A\backslash X) > \rho A\} \\ &= \sum_{A\in\mathcal{C}} p^{|A|}q^{|S|-|A|} \\ &\geq |\mathcal{C}|\min_{A\in\mathcal{C}}\{p^{|S|},q^{|S|}\} \\ &= |\mathcal{C}|\min\{p^{|S|},q^{|S|}\} \end{aligned} \tag{2}$$

The right inequality is shown in a similar fashion. Let $I \in \mathcal{I}$ and $X \subset I$, then $\rho X + \rho(I\backslash X) = |I| \not> \rho I$. This means $\mathbb{I}\{\rho X + \rho(I\backslash X) > \rho I\} = 0$. Thus ,

$$\begin{aligned} f_M(p) &= \sum_{A\subseteq S} p^{|A|}q^{|S|-|A|}\prod_{X\subset A} \mathbb{I}\{\rho X + \rho(A\backslash X) > \rho A\} \\ &= \sum_{A\in\mathcal{D}} p^{|A|}q^{|S|-|A|}\prod_{X\subset A} \mathbb{I}\{\rho X + \rho(A\backslash X) > \rho A\} \\ &\leq \sum_{A\in\mathcal{D}} p^{|A|}q^{|S|-|A|} \\ &\leq |\mathcal{D}|\max\{p^{|S|},q^{|S|}\} \end{aligned} \tag{3}$$

Suppose that the original matroid M is not nescessarily connected, then we may form M as the unique direct sum of its connected components, $M(S,\mathcal{I}) = M_1(S_1)\oplus\cdots\oplus M_m(S_m)$, where the S_i are pairwise disjoint and each of the matroids $M_i(S_i)$ is connected, see [4]. We derive an expression for $f_M(p)$ in this case and examine it.

Theorem 2 *If $M(S,\mathcal{I}) = M_1(S_1)\oplus\cdots\oplus M_m(S_m)$ for some $m \geq 1$, where the $\{M_i\}$ are the connected components of the matroid M, then;*

$$q^{|S|}\left(\left(\frac{p}{q}\right)^{|S_1|}+\cdots+\left(\frac{p}{q}\right)^{|S_m|}\right) \leq f_M(p) \leq q^{|S|}\left(\frac{1}{q^{|S_1|}}+\cdots\frac{1}{q^{|S_m|}}-(m-1)\right).$$

Proof:

$$\begin{aligned}
f_M(p) &= \sum_{\substack{A\subseteq S \\ M_{|A} \text{ connected}}} p^{|A|}q^{|S|-|A|} \\
&\leq \sum_{i=1}^{m}\sum_{A\subseteq S_i} p^{|A|}q^{|S|-|A|} - (m-1)q^{|S|} \\
&= \sum_{i=1}^{m}\sum_{A\subseteq S_i} p^{|A|}q^{|S|-|A|} - (m-1)q^{|S|} \\
&= \sum_{i=1}^{m} q^{|S|-|S_i|}\sum_{A\subseteq S_i} p^{|A|}q^{|S_i|-|A|} - (m-1)q^{|S|} \\
&= \sum_{i=1}^{m} q^{|S|-|S_i|} - (m-1)q^{|S|} \\
&= q^{|S|}(\frac{1}{q^{|S_1|}} + \cdots \frac{1}{q^{|S_m|}} - (m-1)).
\end{aligned} \tag{4}$$

Also;

$$\begin{aligned}
f_M(p) &= \sum_{\substack{A\subseteq S \\ M_{|A} \text{ connected}}} p^{|A|}q^{|S|-|A|} \\
&= \sum_{i=1}^{m} \sum_{\substack{A\subseteq S_i \\ M_{|A} \text{ connected}}} p^{|A|}q^{|S|-|A|} \\
&\geq \sum_{i=1}^{m} p^{|S_i|}q^{|S|-|S_i|} \\
&= q^{|S|}\left(\left(\frac{p}{q}\right)^{|S_1|} + \cdots + \left(\frac{p}{q}\right)^{|S_m|}\right).
\end{aligned} \tag{5}$$

3 Enumeration

We present some results from looking at enumeration as regards matroids. The exact number of matroids on a finite set of size n is unknown but upper and lower bounds are know for it. A matroid is now defined in terms of its bases, which is to say, maximal independent sets. It is a consequence of the definition that all these sets are equal in size.

Definition 3 *A matroid $\mathcal{M}$ is a pair $(S_n, \mathcal{B})$, where $\mathcal{B} \subseteq 2^{S_n}$ which satisfies the axioms;*

(i) $\mathcal{B} \neq \emptyset$

(ii) *Given* $X, Y \in \mathcal{B}$ *then* $\forall x \in X \backslash Y$, $\exists y \in Y \backslash X$ *such that* $X - \{x\} \cup \{y\} \in \mathcal{B}$.

Lemma 4 *Let* $\mathcal{B} = \{B_1, \cdots, B_k\}$ *be a basis for a matroid* $M(S_n)$ *of rank* m. *Then for each pair of bases,* B_i, B_j, *we have that* $0 < |B_i \backslash B_j| \leq k - 2$ *for all* $k > 2$.

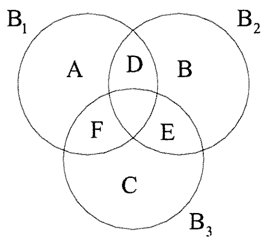
Proof:

Suppose for some $B_i, B_j \in \mathcal{B}$ that $|B_i \backslash B_j| > k - 2$i, then we have that $B_i - x \cup y_x \in \mathcal{B}$, $\forall x \in B_i \backslash B_j$ and corresponding $y_x \in B_j \backslash B_i$. Now $B_i - x \cup y_x \neq B_i, B_j$ for any x. So there are at least $|B_i \backslash B_j|$ sets which must be in $\mathcal{B}$ for it to be a matroid. As they are all distinct we have;

$$
\begin{aligned}
|\mathcal{B}| &\geq 2 + |B_i \backslash B_j| \\
&> 2 + (k - 2) \qquad \text{by hypothesis} \\
&= k.
\end{aligned}
$$

But $|\mathcal{B}| = k$ by definition, thus we have a contradiction and the lemma follows.

Clearly, for $k = 1$, there will be $\binom{n}{m}$ matroids with the same structure and so only one non-isomorphic matroid. For $k = 2$ we must have that $|B_1 \cap B_2| = m - 1$. This means that there are $\binom{n}{2}\binom{n-2}{m-1}$ matroids and so one non-isomorphic matroid. For $k = 3$ we can apply Lemma 4. In this case we know that for $\mathcal{B} = \{B_1, B_2, B_3\}$, that $|B_i \backslash B_j| = 1$ for all $i \neq j$.



So $A + E = A + D = B + E = C + D = C + F = 1$

$\Rightarrow A = B = C$ and $D = E = F$. We have $A + D = 1$. Thus $A = 0$ and $D = 1$ implies

$$
\begin{aligned}
B_1 &= H \cup \{x, y\} \\
B_2 &= H \cup \{y, z\} \qquad (6) \\
B_3 &= H \cup \{z, x\}.
\end{aligned}
$$

for some $H \subseteq S_{n-3}^{(m-2)}$ and so $\mathcal{B}$ is the basis for a matroid.

If $A = 1$ and $D = 0$, then we have

$$\begin{aligned} B_1 &= H \cup \{x\} \\ B_2 &= H \cup \{y\} \\ B_3 &= H \cup \{z\}. \end{aligned} \tag{7}$$

for some $H \subseteq S_{n-3}^{(m-1)}$ and for which the axioms also hold, hence $\mathcal{B}$ is the basis for a matroid.

Theorem 5 *The are $\binom{n}{3}\binom{n-2}{m-1}$ such matroids $\mathcal{M}(S_n, \mathcal{B})$ with where m is the cardinality of the elements in $\mathcal{B}$, and $|\mathcal{B}| = 3$, for all $n \geq 3$ and all $1 \leq m \leq n-1$.*

Proof: The only structures $\mathcal{B}$ which are matroids are those mentioned in (1) and (2). In (1) we m ay choose the elements $\{x, y, z\}$ in $\binom{n}{3}$ ways and the set H in $\binom{n-3}{m-2}$ wa ys, hence there are a total of $\binom{n}{3}\binom{n-3}{m-2}$ matroids whose structure is defined in (1). Similarly, the structure mentioned in (2) can be composed in $\binom{n}{3}\binom{n-3}{m-1}$ ways b y the same argument. Hence all matroids with a three element basis are those matroids whose structur es are identical to (1) and (2), and enumerate to;

$$\binom{n}{3}\binom{n-3}{m-2} + \binom{n}{3}\binom{n-3}{m-1} = \binom{n}{3}\binom{n-2}{m-1}.$$

Corollary 6 *There are $\binom{n}{3}2^{n-2}$ matroids on S_n with a 3-element basis, for all $n \geq 3$.*

Proof: Using the above theorem, we sum over all possible m;

$$\begin{aligned} \sum_{m=1}^{n-1} \binom{n}{3}\binom{n-2}{m-1} &= \binom{n}{3}\sum_{i=0}^{n-2}\binom{n-2}{i} \\ &= \binom{n}{3}2^{n-2}. \end{aligned}$$

References

[1] D. Knuth. Random matroids. *Discrete Math.*, 12:341–358, 1975.

[2] W. Kordecki. *Random matroids*, volume CCCLXVII of *Dissertationes Mathematicae*. Institute of Mathematics, Polish Academy of Sciences, 1997.

[3] M.V. Lomonosov. Bernoulli scheme with closure. *Problems Inform. Transmission*, 10:73–81, 1974.

[4] J.G. Oxley. *Matroid Theory.* Oxford University Press, first edition, 1992.

[5] J.H. Reif and P. Spirakis. Random matroids. In *Proceedings of the* 12^{th} *ACM Symposium on Theory of Computing*, pages 385–397, 1980.