Séminaire Lotharingien de Combinatoire **51** (2004), Article B51g

ON THE NUMBER OF MATROIDS ON A FINITE SET

W. M. B. DUKES

Abstract. In this paper we highlight some enumerative results concerning matroids of low rank and prove the tail-ends of various sequences involving the number of matroids on a finite set to be log-convex. We give a recursion for a new, slightly improved, lower bound on the number of rank-r matroids on n elements when $n = 2^m - 1$. We also prove an adjacent result showing the point-lines-planes conjecture to be true if and only if it is true for a special subcollection of matroids. Two new tables are also presented, giving the number of paving matroids on at most eight elements.

1. Definitions

Let S_n be a finite set of size n. A matroid M is a pair $M(S_n, \mathcal{B})$ such that $\mathcal{B}$ is a non-empty collection of subsets of S_n satisfying the following basis-exchange property:

$$\forall\, X, Y \in \mathcal{B},\ \ \forall x \in X - Y, \exists y \in Y - X \text{ s.t } X - \{x\} \cup \{y\} \in \mathcal{B}.$$

S_n is called the *ground set* of the matroid and $\mathcal{B}$ the collection of *bases*. A consequence of this axiom is that all sets in $\mathcal{B}$ have the same cardinality, called the *rank* of the matroid. The collection of *independent* sets of M is $\mathcal{I}(M) = \{I : I \subseteq B, B \in \mathcal{B}(M)\}$. An element $x \in S_n$ is called a *loop* if $\{x\} \notin \mathcal{I}(M)$. If for every pair of distinct elements $\{x, y\} \subseteq S_n$ there exists $I \in \mathcal{I}(M)$ s.t. $I \supseteq \{x, y\}$, then M is called a *simple*.

Let $\mathbb{M}_r^k(S_n)$ be the class of rank-r matroids on S_n with all k-element sets independent, non-empty for all $0 \leqslant k \leqslant r \leqslant n$, and the union of these classes over $k \leqslant r \leqslant n$ is denoted $\mathbb{M}^k(S_n)$. We say two matroids $M_1(S_n, \mathcal{B}_1)$ and $M_2(S_n, \mathcal{B}_2)$ are *isomorphic* if there exists a permutation π of S_n such that $\mathcal{B}_2 = \{\pi(B) : B \in \mathcal{B}_1\}$. Let $\mathcal{M}_r^k(S_n)$ and $\mathcal{M}^k(S_n)$ be the corresponding classes of non-isomorphic matroids (i.e. 'different' matroids). The collections $\mathbb{M}_r^0(S_n)$, $\mathbb{M}_r^1(S_n)$ and $\mathbb{M}_r^2(S_n)$ identify the classes of rank-r matroids, loopless matroids and simple matroids, respectively, on S_n. $\mathbb{M}_r^{r-1}(S_n)$ is the class of rank-r paving matroids on S_n and the single matroid in $\mathbb{M}_r^r(S_n)$ is the uniform rank-r matroid on n elements. Note

2000 *Mathematics Subject Classification.* 05B35.

Key words and phrases. Matroid, enumeration, paving matroid, points-lines-planes conjecture, free erection.

Supported by EC's Research Training Network 'Algebraic Combinatorics in Europe', grant HPRN-CT-2001-00272 while the author was at the Università di Roma Tor Vergata, Italy.

that $\mathbb{M}_r^{i+1}(S_n) \subset \mathbb{M}_r^i(S_n)$ for all $0 \leqslant i < r$. Given $M \in \mathbb{M}_r^0(S_n)$ and $X \subseteq S_n$, the *restriction* of M to X, denoted $M|X$, is the matroid with independent sets $\{I \cap X : I \in \mathcal{I}(M)\}$. The *dual* of M is the matroid $M^\star \in \mathbb{M}_{n-r}^0(S_n)$ with $\mathcal{B}(M^\star) := \{S_n - B : B \in \mathcal{B}(M)\}$.

The rank of $A \subseteq S_n$ is defined by $r(A) := \max\{|X| : X \subseteq A, X \in \mathcal{I}(M)\}$. We call $A \subseteq S_n$ a *flat* if $r(A \cup \{x\}) = r(A) + 1$ for all $x \in S_n - A$. We denote by $\mathcal{F}_k(M)$ the collection of rank-k flats of M and the numbers $W_k(M) := |\mathcal{F}_k(M)|$ are called the *Whitney numbers of the second kind.* We may also define a matroid in terms of its flats: the pair $M(S_n, \mathcal{F} = \{\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_r\})$ is a matroid if for all $0 \leqslant i < r$ and $F_i \in \mathcal{F}_i$, the collection $\{X - F_i : X \in \mathcal{F}_{i+1} \text{ and } X \supset F_i\}$ partitions the set $S_n - \mathcal{F}_i$.

For a general matroid M, the relationship between the collection of flats and independent sets may be seen as follows: a set F is in $\mathcal{F}(M)$ if $I \cup \{x\} \in \mathcal{I}(M)$ whenever $I \subseteq F$, $I \in \mathcal{I}(M)$ and $x \notin F$. Conversely, a set I is in $\mathcal{I}(M)$ if for every $x \in I$, $I - F = \{x\}$ for some $F \in \mathcal{F}(M)$.

The upper truncation $U_k(M)$ of $M \in \mathbb{M}_r^0(S_n)$ is the matroid obtained by removing the rank-i flats of M for $k \leqslant i < r$. The resulting matroid is a rank-k matroid. Given $N \in \mathbb{M}_r^0(S_n)$ and $M \in \mathbb{M}_{r+1}^0(S_n)$, we say M is an *erection* of N if $U_r(M) = N$.

A collection $\mathcal{H}$ of subsets of S_n is a d-partition of S_n if every d-set of S_n is contained in a unique set of $\mathcal{H}$ and $|H| \geqslant d$ for all $H \in \mathcal{H}$. We call the d-partition *trivial* if $\mathcal{H} = \{S_n\}$.

2. Enumerative results and conjectures

Several papers and books addressing the number of matroids on a finite set have used the terms 'number of matroids' where 'number of non-isomorphic matroids' or 'number of non-isomorphic simple matroids' was intended. The tightest bounds on the total number of matroids (i.e., fixing n and summing over r) are to be found in Knuth [12] and Piff and Welsh [19]. Some surprising recent work gives the asymptotics for the number of binary matroids, see Wild [24]. Also, the long-standing conjecture of Welsh [23] that $|\mathcal{M}^0(S_{m+n})| \geqslant |\mathcal{M}^0(S_m)||\mathcal{M}^0(S_n)|$ has recently been proved independently by Lemos [15] and Crapo and Schmitt [8].

To resolve the confusion regarding what the term 'number of matroids' means, in this paper we will distinguish between the six classes: $\mathbb{M}_r^0(S_n)$, $\mathbb{M}_r^1(S_n)$, $\mathbb{M}_r^2(S_n)$, $\mathcal{M}_r^0(S_n)$, $\mathcal{M}_r^1(S_n)$ and $\mathcal{M}_r^2(S_n)$.

To align our notation with the the standard literature on this subject, let us mention the following; Crapo [5] gives the first 4 numbers in the $|\mathcal{M}^2(S_n)|$ row of the table for $|\mathcal{M}_r^2(S_n)|$ in Section 5. The table for $|\mathcal{M}_r^2(S_n)|$ was first given in Blackburn, Crapo and Higgs [4] and is reprinted in Welsh [21, p.306]. The table $|\mathcal{M}_r^0(S_n)|$ was first given in Acketa [3], extending earlier results from Acketa [2], and is reprinted at the back of Oxley's book [18]. The numbers enumerated in Acketa [1] were $|\mathcal{M}_2^0(S_n)|$.

Let $p(i)$ be the number of partitions of the integer i, $\left\{ {n \atop i} \right\}$ the Stirling numbers of the second kind and $b(i)$ the i^{th} Bell number. Through consideration of the loops and points of general matroids, we have the following relations: $|\mathcal{M}_0^0(S_n)| = 1$, $|\mathbb{M}_0^0(S_n)| = 1$, $|\mathbb{M}_1^1(S_n)| = 1$, $|\mathcal{M}_1^1(S_n)| = 1$, $|\mathbb{M}_n^2(S_n)| = 1$, $|\mathcal{M}_n^2(S_n)| = 1$,

$$\begin{aligned} |\mathbb{M}_r^0(S_n)| &= \sum_{i=r}^{n} \binom{n}{i} |\mathbb{M}_r^1(S_i)|, \\ |\mathbb{M}_r^1(S_n)| &= \sum_{i=r}^{n} \left\{ {n \atop i} \right\} |\mathbb{M}_r^2(S_i)|, \\ |\mathcal{M}_r^0(S_n)| &= \sum_{i=r}^{n} |\mathcal{M}_r^1(S_i)|. \end{aligned}$$

Using these equalities, we have the following closed forms for certain low-rank matroids:

Theorem 2.1 (Dukes [11])**.** *For all $n \geqslant 2$,*

(i) $|\mathcal{M}_1^0(S_n)| = n$, $|\mathcal{M}_2^0(S_n)| = p(1) + \cdots + p(n) - n$,
(ii) $|\mathbb{M}_1^0(S_n)| = 2^n - 1$, $|\mathbb{M}_2^0(S_n)| = b(n+1) - 2^n$,
(iii) $|\mathbb{M}_2^1(S_n)| = b(n) - 1$, $|\mathcal{M}_2^1(S_n)| = p(n) - 1$.

By duality we can also enumerate high-rank matroids as the following lemma shows:

Lemma 2.2. *For all $n \geqslant 5$,*

(i) $|\mathbb{M}_{n-1}^2(S_n)| = 2^n - 1 - \binom{n+1}{2}$,
(ii) $|\mathcal{M}_{n-1}^2(S_n)| = n - 2$,
(iii) $|\mathbb{M}_{n-2}^2(S_n)| = b(n+1) + \binom{n+3}{4} + 2\binom{n+1}{4} - 2^n - \binom{n+1}{2}2^{n-1}$,
(iv) $|\mathcal{M}_{n-2}^2(S_n)| = p(1) + \ldots + p(n) + 6 - 4n$.

Proof. A matroid $M \in \mathbb{M}_{n-1}^2(S_n)$ is specified by a unique circuit of length k for some $3 \leqslant k \leqslant n$, the elements not contained in this circuit are the isthmuses of M. If $\mathcal{B}(M^\star) = \{\{x_1\}, \ldots, \{x_k\}\}$ then this circuit is $C = \{x_1, \ldots, x_k\}$ and the number of ways to choose such a circuit is simply the number of subsets of S_n of size at least 3, hence $|\mathbb{M}_{n-1}^2(S_n)| = 2^n - 1 - n - \binom{n}{2}$. The corresponding non-isomorphic number is $|\mathcal{M}_{n-1}^2(S_n)| = (n+1) - 3 = n - 2$.

If $M \in \mathbb{M}_2^0(S_n)$ then $M^\star \in \mathbb{M}_{n-2}^0(S_n)$. Suppose $\mathcal{F}_0(M) = \{F_0\}$ and $\mathcal{F}_1(M) = \{H_1, \ldots, H_k\}$. Let $F_i = H_i - F_0$ for all $1 \leqslant i \leqslant k$. Then $\{F_0, F_1, \ldots, F_k\}$ partitions the set S_n. $M^\star$ is not simple iff there exists $X \in \binom{S_n}{n-2}$ such that for all $(f_i, f_j) \in F_i \times F_j$ with $0 < i < j$, $\{f_i, f_j\} \not\subset X$. It transpires that $M^\star$ is not simple if

- $k=2$ and ($|F_1|=1$, $|F_2|\geqslant 1$) or ($|F_1|=2$, $|F_2|\geqslant 2$),
- $k=3$, $|F_1|=|F_2|=1$ and $|F_3|\geqslant 1$,

and relabellings thereof. Enumerating this class of matroids whose duals are not simple gives:

$$\sum_{i=0}^{n-2}\binom{n}{i}(n-i)-\binom{n}{n-2}+3\binom{n}{4}+\sum_{i=5}^{n}\binom{n}{i}\binom{i}{2}+\binom{n}{3}+\sum_{i=4}^{n}\binom{n}{i}\binom{i}{2}$$
$$=\binom{n+1}{2}2^{n-1}-\binom{n+3}{4}-2\binom{n+1}{4}.$$

Thus

$$\begin{aligned}|\mathbb{M}^2_{n-2}(S_n)| &= |\mathbb{M}^0_2(S_n)|-\left\{\binom{n+1}{2}2^{n-1}-\binom{n+3}{4}-2\binom{n+1}{4}\right\}\\ &= b(n+1)-2^n-\binom{n+1}{2}2^{n-1}+\binom{n+3}{4}+2\binom{n+1}{4}\end{aligned}$$

and the corresponding non-isomorphic number is

$$\begin{aligned}|\mathcal{M}^2_{n-2}(S_n)| &= |\mathcal{M}^0_2(S_n)|-(n-1)-(n-3)-(n-2)\\ &= p(1)+\ldots+p(n)-n-3(n-2).\end{aligned}$$

□

A well cited conjecture (proposed by Welsh [22]) states that the number of 'different' matroids on S_n (i.e. $|\mathcal{M}^0_r(S_n)|$) is unimodal in rank. It seems unfair to restrict this conjecture to only one of the six classes of matroids so we propose;

Conjecture 2.3. *The sequences* $\{|\mathbb{M}^0_r(S_n)|\}_{r=0}^n$, $\{|\mathbb{M}^1_r(S_n)|\}_{r=1}^n$, $\{|\mathbb{M}^2_r(S_n)|\}_{r=2}^n$, $\{|\mathcal{M}^0_r(S_n)|\}_{r=0}^n$, $\{|\mathcal{M}^1_r(S_n)|\}_{r=1}^n$ *and* $\{|\mathcal{M}^2_r(S_n)|\}_{r=2}^n$ *are unimodal and attain their maximum at* $r=\lceil n/2\rceil$.

The following theorem summarizes partial progress with this conjecture.

Theorem 2.4 (Dukes [9])**.** *For all* $n\geqslant 6$,

(i) $|\mathbb{M}^0_0(S_n)|\leqslant|\mathbb{M}^0_1(S_n)|\leqslant|\mathbb{M}^0_2(S_n)|\leqslant|\mathbb{M}^0_3(S_n)|$,
(ii) $|\mathcal{M}^0_0(S_n)|\leqslant|\mathcal{M}^0_1(S_n)|\leqslant|\mathcal{M}^0_2(S_n)|\leqslant|\mathcal{M}^0_3(S_n)|$,
(iii) $|\mathbb{M}^1_1(S_n)|\leqslant|\mathbb{M}^1_2(S_n)|\leqslant|\mathbb{M}^1_3(S_n)|$,
(iv) $|\mathcal{M}^1_1(S_n)|\leqslant|\mathcal{M}^1_2(S_n)|\leqslant|\mathcal{M}^1_3(S_n)|$,
(v) $|\mathbb{M}^2_2(S_n)|\leqslant|\mathbb{M}^2_3(S_n)|$,
(vi) $|\mathcal{M}^2_2(S_n)|\leqslant|\mathcal{M}^2_3(S_n)|$.

In problems involving unimodal sequences, it is sometimes easier to show a sequence to be log-concave and therefore unimodal. It is not clear that the sequences $\{|\mathbb{M}^0_r(S_n)|\}_{r=0}^n$, $\{|\mathbb{M}^1_r(S_n)|\}_{r=1}^n$, $\{|\mathbb{M}^2_r(S_n)|\}_{r=2}^n$, $\{|\mathcal{M}^0_r(S_n)|\}_{r=0}^n$, $\{|\mathcal{M}^1_r(S_n)|\}_{r=1}^n$ and $\{|\mathcal{M}^2_r(S_n)|\}_{r=2}^n$ are log-concave. The evidence in the tables would seem to suggest log-concavity. However, this is only the case for n small. We exhibit the following theorem which shows the beginning (in some cases the end) of these sequences to be log-convex once n is sufficiently large. First we require two lower bounds to aid the proof.

Theorem 2.5 (Dukes [10]). *For all $2 < r < n$, $|\mathbb{M}_r^{r-1}(S_n)| > 2^{\binom{n}{r}/2n}$ and $|\mathcal{M}_r^{r-1}(S_n)| > \frac{1}{n!}2^{\binom{n}{r}/2n}$.*

Theorem 2.6. *The matroid numbers satisfy the following inequalities*

(i) $|\mathbb{M}_0^0(S_n)||\mathbb{M}_2^0(S_n)| > |\mathbb{M}_1^0(S_n)|^2$ *for all* $n \geqslant 4$,
(ii) $|\mathcal{M}_0^0(S_n)||\mathcal{M}_2^0(S_n)| > |\mathcal{M}_1^0(S_n)|^2$ *for all* $n \geqslant 9$,
(iii) $|\mathbb{M}_1^1(S_n)||\mathbb{M}_3^1(S_n)| > |\mathbb{M}_2^1(S_n)|^2$ *for all* $n \geqslant 94$,
(iv) $|\mathcal{M}_1^1(S_n)||\mathcal{M}_3^1(S_n)| > |\mathcal{M}_2^1(S_n)|^2$ *for all* $n \geqslant 67$,
(v) $|\mathbb{M}_{n-2}^2(S_n)||\mathbb{M}_n^2(S_n)| > |\mathbb{M}_{n-1}^2(S_n)|^2$ *for all* $n \geqslant 11$,
(vi) $|\mathcal{M}_{n-2}^2(S_n)||\mathcal{M}_n^2(S_n)| > |\mathcal{M}_{n-1}^2(S_n)|^2$ *for all* $n \geqslant 8$.

Proof. Each follows from combining known closed forms, and in some cases inequalities, for the numbers and using induction. The first and second inequalities follow directly from Theorem 2.1. The third inequality follows since

$$|\mathbb{M}_1^1(S_n)||\mathbb{M}_3^1(S_n)| > |\mathbb{M}_3^2(S_n)| > 2^{(n-1)(n-2)/12},$$

by using Theorem 2.5 with $r = 3$. It can then be verified that

$$2^{(n-1)(n-2)/12} > (b(n) - 1)^2 = |\mathbb{M}_2^1(S_n)|^2$$

for all $n \geqslant 94$. Similarly, the fourth inequality follows from applying the same method but by using the non-isomorphic lower bound of Theorem 2.5. The final two inequalities follow from Lemma 2.2. Some of the inequalities also hold for smaller values of n. □

The above sequences are much more likely to resemble the sequence $\{2^{\binom{n}{r}}\}_{r=0}^n$ which is log-convex at both ends of the sequence and has a log-concave 'cap' in the middle.

3. Lower bound on the number of paving matroids

The tightest asymptotic lower bound for the number of matroids was given in Knuth [12]. The method involved proving a lower bound on the number of rank-$\lfloor n/2 \rfloor$ paving matroids on S_n. Theorem 2.5 showed his lower bound inequality to hold for $2 < r < n$ ([12] proved the case $r = \lfloor n/2 \rfloor$) giving a lower bound on the number of $(r-1)$-partitions of S_n. The class of non-trivial $(r-1)$-partitions corresponds directly to the class of rank-r paving matroids. It was noted in Dukes [10] that experimental results suggested a particular class of the partitions to be larger than each of the other classes. The following lemma gives a recursion for the enumeration of this class, hence the tightest lower bound possible using this approach when the size of the ground set is of the form $2^m - 1$.

Theorem 3.1. *If $n = 2^m - 1$ for some $m \in \mathbb{N}$, then $|\mathbb{M}_r^{r-1}(S_n)| \geqslant 2^{|\mathcal{U}(r,n)|}$ for all $r \geqslant 4$ where $|\mathcal{U}(r,n)|$ satisfies the recursion:*

$$|\mathcal{U}(r+1,n)| \quad = \quad \frac{1}{r+1}\left(\binom{n}{r} - |\mathcal{U}(r,n)| - (n-r+1)|\mathcal{U}(r-1,n)|\right)$$

with initial values $|\mathcal{U}(3,n)| = \binom{n}{3}/(n-2)$ and $|\mathcal{U}(4,n)| = \binom{n}{4}/(n-2)$.

Proof. Let $n = 2^m - 1$. Given an integer i, let $\vec{i}$ be its binary representation. Given two integers i, j, let $i \oplus j$ be binary addition in $\mathbb{Z}_2$. In this proof we assume the set $S_n = \{1, 2, \ldots, n\}$. Let $\mathcal{U}(r,n) := \{\{i_1, \cdots, i_r\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_r} = \vec{0}\}$. Since $n = 2^m - 1$, all possible binary vectors, except the 0 vector, of length m are possible in $\mathcal{U}(r,n)$. It is clear that if $A, B \in \mathcal{U}(r,n)$ and $A \neq B$, then $|A \cap B| \leqslant r-2$. For otherwise there must exist $i_1, \ldots, i_{r-1}, i_r, i_{r+1}$ such that $A = \{i_1, \ldots, i_{r-1}, i_r\}$ and $B = \{i_1, \ldots, i_{r-1}, i_{r+1}\}$. This gives $\vec{i_1} \oplus \cdots \oplus \vec{i_{r-1}} = \vec{i_r} = \vec{i_{r+1}}$. But since i_r and i_{r+1} are distinct, this is a contradiction.

Thus if we take any subset $\mathcal{V} \subseteq \mathcal{U}(r,n)$, and then insert into $\mathcal{V}$ all those $r-1$ element subsets of S_n which are not contained in any member of $\mathcal{V}$, the resulting collection will be a $(r-1)$-partition of S_n and hence represents the hyperplanes of a rank-r paving matroid on S_n. There are $2^{|\mathcal{U}(r,n)|}$ choices for $\mathcal{V}$, hence we have $|\mathbb{M}_r^{r-1}(S_n)| \geqslant 2^{|\mathcal{U}(r,n)|}$. It is now required to find $|\mathcal{U}(r,n)|$,

$$\begin{aligned}
&|\mathcal{U}(r+1,n)| \\
&= |\{\{i_1, \cdots, i_{r+1}\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_{r+1}} = \vec{0}\}| \\
&= \frac{1}{r+1}|\{\{i_1, \cdots, i_r\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_r} = \vec{z},\ z \in S_n - \{i_1, \ldots, i_r\}\}| \\
&= \frac{1}{r+1}\big(|\{\{i_1, \cdots, i_r\} \subset S_n\}| \\
&\quad -|\{\{i_1, \cdots, i_r\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_r} = \vec{z},\ z \in \{0, i_1, \ldots, i_r\}\}|\Big) \\
&= \frac{1}{r+1}\left(\binom{n}{r} - |\{\{i_1, \cdots, i_r\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_r} = \vec{0}\}|\right. \\
&\quad \left. -|\{\{i_1, \cdots, i_r\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_r} = \vec{z},\ z \in \{i_1, \ldots, i_r\}\}|\right) \\
&= \frac{1}{r+1}\left(\binom{n}{r} - |\mathcal{U}(r,n)|\right. \\
&\quad \left. -(n-(r-1))|\{\{i_1, \cdots, i_{r-1}\} \subset S_n : \vec{i_1} \oplus \cdots \oplus \vec{i_{r-1}} = \vec{0}\}|\right) \\
&= \frac{1}{r+1}\left(\binom{n}{r} - |\mathcal{U}(r,n)| - (n-r+1)|\mathcal{U}(r-1,n)|\right).
\end{aligned}$$

The initial conditions for this recursion are $|\mathcal{U}(3,n)| = \binom{n}{3}/(n-2)$ and $|\mathcal{U}(4,n)| = \binom{n}{4}/(n-2)$. $\mathcal{U}(3,n)$ of course corresponds to certain 2-partitions of S_n, which are the hyperplanes of rank-3 paving matroids. □

4. Concerning the points-lines-planes conjecture

The following conjecture is stated in Seymour [20]. Originally Welsh [21, p.289] introduced the phrase 'Points-lines-planes conjecture' for the $k = 2$ instance of Mason [16, Conjecture 1C]. In the current form it is actually the $k = 2$ instance of the slightly more general Mason [16, Conjecture 1D].

Conjecture 4.1 (Points-Lines-Planes)**.** *For all $M \in \mathbb{M}_4^2(S_n)$,*

$$W_2(M)^2 \quad \geqslant \quad \frac{3(W_1(M)-1)}{2(W_1(M)-2)} W_1(M) W_3(M),$$

with equality if and only if $\mathcal{F}_3(M) = \binom{S_n}{3}$.

The most general case proven so far is:

Theorem 4.2 (Seymour [20])**.** *The points-lines-planes conjecture is true for all $\{M \in \mathbb{M}_4^2(S_n) \ : \ |F| \leqslant 4$ for all $F \in \mathcal{F}_2(M)\}$.*

Let us also mention that in related work, Kung [14] proved that if M is a simple matroid of rank at least 5, in which all lines contain the same number of points, then $W_2(M) \leqslant W_3(M)$.

The purpose of this section is to prove that the points-lines-planes conjecture is true for all simple rank-4 matroids if and only if it is true for a special subcollection of them.

Let us briefly outline Knuth's [13] algorithm for constructing all matroids on the finite set S_n (i.e., for constructing the class $\cup_{r=1}^{n} \mathbb{M}_r^1(S_n)$). We restate the algorithm in a slightly different way to the original paper. Let $\mathcal{T}$ be a collection of subsets of S_n. Let $\textsc{Expand}(\mathcal{T}) := \{A \cup a : A \in \mathcal{T} \text{ and } a \in S_n - A\}$. Let $\textsc{Random}(\mathcal{T})$ be a collection of random sets where each random set properly contains some member of $\mathcal{T}$. Let $\textsc{Refine}(\mathcal{T}, \mathcal{T}')$ be the collection of sets $\mathcal{T}$ obtained after applying the following:

> Repeat until $A \cap B \subseteq C$ for some $C \in \mathcal{T}'$ for all $A, B \in \mathcal{T}$: if $A, B \in \mathcal{T}$, $A \neq B$ and $A \cap B \not\subseteq C$ for any $C \in \mathcal{T}'$ then replace A and B in $\mathcal{T}$ by the set $A \cup B$.

Knuth's random matroids algorithm

(1) Let $r = 0$ and $\mathcal{F}_0 = \{\emptyset\}$.
(2) Let $\mathcal{A} = \textsc{Expand}(\mathcal{F}_r) \cup \textsc{Random}(\mathcal{F}_r)$.
(3) Let $\mathcal{F}_{r+1} = \textsc{Refine}(\mathcal{A}, \mathcal{F}_r)$.
(4) If $S_n \in \mathcal{F}_{r+1}$ then let $\mathcal{F} = \mathcal{F}_0 \cup \ldots \cup \mathcal{F}_{r+1}$ and Stop. Otherwise let $r = r + 1$ and go to step (2).

Theorem 4.3 (Knuth [13]).

(i) *The resulting collection $\mathcal{F}$ is the collection of flats of a matroid on S_n.*
(ii) *The resulting matroid obtained from the algorithm does not depend on the order of replacements in* $\textsc{Refine}(\mathcal{A}, \mathcal{F}_r)$.
(iii) *Every matroid in $\cup_{r=1}^{n} \mathbb{M}_r^1(S_n)$ is obtainable using this algorithm.*

Let M be a simple rank-$(r + 1)$ matroid on S_n with hyperplanes $\mathcal{F}_r$, and let $\mathcal{F}'_{r+1} = \textsc{Refine}(\textsc{Expand}(\mathcal{F}_r) \cup \textsc{Random}(\mathcal{F}_r), \mathcal{F}_r)$. The matroid M' with flats $\mathcal{F}(M) \cup \mathcal{F}'_{r+1}$ is an erection of M. If $M' = M$ (this happens if $\mathcal{F}'_{r+1} = \{S_n\}$) then M' is the *trivial erection*. If $\textsc{Random}(\mathcal{F}_r) = \emptyset$, then the resulting matroid M' is termed the *free erection* of M, denoted $\mathrm{Free}(M)$.

The free erection was first defined in Crapo [6] and an alternative construction of it can be found in Nguyen [17]. We prove the following result using the operations defined above. An alternative proof may be given using the results and terminology of [6, 17].

Theorem 4.4. *The points-lines-planes conjecture is true if and only if it is true for the class of rank-4 matroids that are the free erection of some rank-3 matroid.*

Proof. If the points-lines-planes conjecture is true, then clearly it is true for all those rank-4 matroids that are the free erection of some rank-3 matroid, i.e. $\{\mathrm{Free}(M) : M \in \mathbb{M}_3^2(S_n),\ \mathrm{Free}(M) \neq M\} \subset \mathbb{M}_4^2(S_n)$.

Conversely, suppose the points-lines-planes conjecture is true for all $\{\mathrm{Free}(M) : M \in \mathbb{M}_3^2(S_n),\ \mathrm{Free}(M) \neq M\}$. Every matroid $N \in \mathbb{M}_4^2(S_n)$ is the erection of some $M \in \mathbb{M}_3^2(S_n)$, that is to say, if $M = U_3(N)$ then there exists a collection $\textsc{Random}(\mathcal{F}_2(M))$ (not necessarily unique) such that

$$\mathcal{F}_3(N) \;=\; \textsc{Refine}(\textsc{Expand}(\mathcal{F}_2(M)) \cup \textsc{Random}(\mathcal{F}_2(M)), \mathcal{F}_2(M)).$$

We now show that for all matroids $M \in \mathbb{M}_3^2(S_n)$,

$$|\textsc{Refine}(\textsc{Expand}(\mathcal{F}_2(M)) \cup \textsc{Random}(\mathcal{F}_2(M)), \mathcal{F}_2(M))| \;\leqslant\; |\mathcal{F}_3(\mathrm{Free}(M))|.$$

Let $M \in \mathbb{M}_3^2(S_n)$ with $\mathcal{F}_2(M) = \mathcal{F}_2$, so that

$$\mathcal{F}_3(N) \;:=\; \textsc{Refine}(\textsc{Expand}(\mathcal{F}_2) \cup \textsc{Random}(\mathcal{F}_2), \mathcal{F}_2).$$

Consider the collections $\textsc{Refine}(\textsc{Expand}(\mathcal{F}_2) \cup \textsc{Random}(\mathcal{F}_2), \mathcal{F}_2)$ and $\textsc{Refine}(\textsc{Expand}(\mathcal{F}_2), \mathcal{F}_2)$. Let $\textsc{Expand}(\mathcal{F}_2) = \{E_1, \ldots, E_m\}$ and define $E'_i = E_i$

for all $1 \leqslant i \leqslant m$. For each $1 \leqslant i \leqslant m$, if $X \in \textsc{Random}(\mathcal{F}_2)$ and $X \supseteq E_i$, then let $E_i' = E_i' \cup X$ and remove X from $\textsc{Random}(\mathcal{F}_2)$. Once $\textsc{Random}(\mathcal{F}_2)$ is empty, we have $E_i \subseteq E_i'$ for all i.

Recall from Theorem 4.3 that if $\mathcal{A}$ is a well defined collection in terms of $\mathcal{F}_2$, then $\textsc{Refine}(\mathcal{A} - \{A_1, A_2\} \cup \textsc{Refine}(\{A_1, A_2\}, \mathcal{F}_2), \mathcal{F}_2) = \textsc{Refine}(\mathcal{A} - \{A_3, A_4\} \cup \textsc{Refine}(\{A_3, A_4\}, \mathcal{F}_2), \mathcal{F}_2)$ for all $A_1, A_2, A_3, A_4 \in \mathcal{A}$ s.t. $A_1 \neq A_2$ and $A_3 \neq A_4$.

For each $E_i, E_j \in \textsc{Expand}(\mathcal{F}_2)$, if $\textsc{Refine}(\{E_i, E_j\}, \mathcal{F}_2) = \{E_i \cup E_j\}$ then $\textsc{Refine}(\{E_i' \cup E_j'\}, \mathcal{F}_2) = \{E_i' \cup E_j'\}$ since $E_i \cap E_j \subseteq E_i' \cap E_j'$. Hence, $\textsc{Refine}(\{E_1, \ldots, E_m\}, \mathcal{F}_2)$ has at least as many sets as

$$\textsc{Refine}(\{E_1', \ldots, E_m'\}, \mathcal{F}_2) \quad = \quad \textsc{Refine}(\textsc{Expand}(\mathcal{F}_2) \cup \textsc{Random}(\mathcal{F}_2), \mathcal{F}_2)$$

and so

$$\begin{aligned} W_3(N) &= |\textsc{Refine}(\textsc{Expand}(\mathcal{F}_2(M)) \cup \textsc{Random}(\mathcal{F}_2(M)), \mathcal{F}_2(M))| \\ &\leqslant |\textsc{Refine}(\textsc{Expand}(\mathcal{F}_2(M)), \mathcal{F}_2(M))| \\ &= W_3(\mathrm{Free}(M)). \end{aligned}$$

Since $W_2(M) = W_2(N)$ and $W_1(M) = W_1(N)$, the result follows. □

Let us also observe that since every plane (rank-3 flat) is determined by two unique lines (rank-2 flats), $W_3(M) \leqslant W_2(M)^2/2$. The benefit of Theorem 4.4 is apparent by considering the number of simple rank-3 matroids having non-trivial erections relative to the number of simple rank-4 matroids. Using Theorem 2.5 we have

$$|\mathbb{M}_4^2(S_n)| \geqslant |\mathbb{M}_4^3(S_n)| \geqslant 2^{\binom{n}{4}/2n}$$

and

$$|\{\mathrm{Free}(M) : M \in \mathbb{M}_3^2(S_n),\ \mathrm{Free}(M) \neq M\}| \leqslant |\mathbb{M}_3^2(S_n)| \leqslant 2^{\binom{n}{3}},$$

since all rank-3 matroids are uniquely expressible by their collection of bases, a subset of $\binom{S_n}{3}$. Hence

$$\frac{|\{\mathrm{Free}(M) : M \in \mathbb{M}_3^2(S_n),\ \mathrm{Free}(M) \neq M\}|}{|\mathbb{M}_4^2(S_n)|} \quad \leqslant \quad 2^{-(7n+3)(n-1)(n-2)/48}.$$

5. Numerical values

As mentioned in Section 2, the tables for $|\mathcal{M}_r^2(S_n)|$ and $|\mathcal{M}_r^0(S_n)|$ were first given in Blackburn, Crapo and Higgs [4] and Acketa [3], respectively. These two tables along with the tables for $|\mathbb{M}_r^0(S_n)|$, $|\mathbb{M}_r^1(S_n)|$, $|\mathcal{M}_r^1(S_n)|$ and $|\mathbb{M}_r^2(S_n)|$ were given in Dukes [11]. A modification to the program used to generate these gives the two new tables for the number of paving matroids, $|\mathbb{M}_r^{r-1}(S_n)|$, and non-isomorphic paving matroids, $|\mathcal{M}_r^{r-1}(S_n)|$ on at most eight elements.

$|\mathbb{M}^0_r(S_n)|$

$r \setminus n$	0	1	2	3	4	5	6	7	8
0	1	1	1	1	1	1	1	1	1
1		1	3	7	15	31	63	127	255
2			1	7	36	171	813	4012	20891
3				1	15	171	2053	33442	1022217
4					1	31	813	33442	8520812
5						1	63	4012	1022217
6							1	127	20891
7								1	255
8									1
$\lvert\mathbb{M}^0(S_n)\rvert$	1	2	5	16	68	406	3807	75164	10607540

$|\mathcal{M}^0_r(S_n)|$

$r \setminus n$	0	1	2	3	4	5	6	7	8
0	1	1	1	1	1	1	1	1	1
1		1	2	3	4	5	6	7	8
2			1	3	7	13	23	37	58
3				1	4	13	38	108	325
4					1	5	23	108	940
5						1	6	37	325
6							1	7	58
7								1	8
8									1
$\lvert\mathcal{M}^0(S_n)\rvert$	1	2	4	8	17	38	98	306	1724

$|\mathbb{M}^1_r(S_n)|$

$r \setminus n$	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2		1	4	14	51	202	876	4139
3			1	11	106	1232	22172	803583
4				1	26	642	28367	8274374
5					1	57	3592	991829
6						1	120	19903
7							1	247
8								1
$\lvert\mathbb{M}^1(S_n)\rvert$	1	2	6	27	165	2135	55129	10094077

$|\mathcal{M}^1_r(S_n)|$

$r \setminus n$	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2		1	2	4	6	10	14	21
3			1	3	9	25	70	217
4				1	4	18	85	832
5					1	5	31	288
6						1	6	51
7							1	7
8								1
$\lvert\mathcal{M}^1(S_n)\rvert$	1	2	4	9	21	60	208	1418

$|\mathbb{M}^2_r(S_n)|$

$r \setminus n$	2	3	4	5	6	7	8
2	1	1	1	1	1	1	1
3		1	5	31	352	8389	433038
4			1	16	337	18700	7642631
5				1	42	2570	907647
6					1	99	16865
7						1	219
8							1
$\lvert\mathbb{M}^2(S_n)\rvert$	1	2	7	49	733	29760	9000402

$|\mathcal{M}^2_r(S_n)|$

$r \setminus n$	2	3	4	5	6	7	8
2	1	1	1	1	1	1	1
3		1	2	4	9	23	68
4			1	3	11	49	617
5				1	4	22	217
6					1	5	40
7						1	6
8							1
$\lvert\mathcal{M}^2(S_n)\rvert$	1	2	4	9	26	101	950

	$\lvert\mathbb{M}^{r-1}_r(S_n)\rvert$							$\lvert\mathcal{M}^{r-1}_r(S_n)\rvert$						
$r \setminus n$	2	3	4	5	6	7	8	2	3	4	5	6	7	8
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3		1	5	31	352	8389	433038		1	2	4	9	23	68
4			1	6	82	6149	4464328			1	2	5	18	322
5				1	7	239	239173				1	2	5	39
6					1	8	772					1	2	6
7						1	9						1	2
8							1							1
Total	1	2	7	39	443	14787	5137322	1	2	4	8	18	50	439

The program is freely available by e-mailing the author. It is written in the C-programming language and is easily compiled on FreeBSD and Linux platforms.

Acknowledgments

The author would like to thank Francesco Brenti and the anonymous referee for helpful comments, and Christian Krattenthaler for an interesting suggestion. This work was funded by the Research Training Network 'Algebraic Combinatorics in Europe', grant HPRN-CT-2001-00272.

References

[1] D. M. Acketa, On the enumeration of matroids of rank-2, *Zbornik radova Prirodno-matematickog fakulteta – Univerzitet u Novom Sadu.*, **8** (1978), 83–90.

[2] D. M. Acketa, On the construction of all matroids on 7 elements at most, *Zbornik radova Prirodno-matematickog fakulteta – Univerzitet u Novom Sadu.*, **8** (1979), 133–152.

[3] D. M. Acketa, A construction of non-simple matroids on at most 8 elements, *J. Combin. Inform. System Sci.* **9** (1984), 121–132.

[4] J. E. Blackburn, H. Crapo and D. A. Higgs, A catalogue of combinatorial geometries, *Math. Comp.* **27** (1973), 155–166.

[5] H. Crapo, Single-Element Extensions of Matroids, *J. Res. Nat. Bur. Stand.* **69B** (1965), 57–65.

[6] H. Crapo, Erecting Geometries, *Proc. 2^{nd} Chapel Hill Conf. on Comb. Math.* (1970), 74–99.

[7] H. Crapo and G.-C. Rota, Combinatorial Geometries, Preliminary edition, MIT Press, Cambridge, 1970.

[8] H. Crapo and W. Schmitt, The free product of matroids, *European J. Combin.*, to appear.

[9] W. M. B. Dukes, On a unimodality conjecture in matroid theory, *Discrete Math. Theor. Comput. Sci.* **5**(1) (2002), 181–190.

[10] W. M. B. Dukes, Bounds on the number of generalized partitions and some applications, *Australas. J. Comb.* **28** (2003), 257–262.

[11] W. M. B. Dukes, Counting and Probability in Matroid Theory, Ph.D. thesis, Trinity College Dublin, 2000.

[12] D. E. Knuth, The Asymptotic Number of Geometries, *J. Combin. Theory Ser. A* **16** (1974), 398–400.

[13] D. E. Knuth, Random Matroids, *Discrete Math.* **12** (1975), 341–358.

[14] J. P. S. Kung, On the lines-planes inequality for matroids, *J. Combin. Theory Ser. A* **91** (2000), 363–368.

[15] M. Lemos, On the number of non-isomorphic matroids, *Adv. Appl. Math.* **33** (2004), 733–746.

[16] J. H. Mason, Matroids: Unimodal conjectures and Motzkin's theorem, *Combinatorics* (D. J. A. Welsh and D. R. Woodall, eds.), Institute of Math. and Appl. (1972), 207–221.

[17] H. Q. Nguyen, Constructing the free erection of a geometry, *J. Combin. Theory Ser. B* **27** (1979), 216–224.

[18] J. G. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

[19] M. J. Piff and D. J. A. Welsh, On the number of combinatorial geometries, *Bull. London. Math. Soc.* **3** (1971), 55–56.

[20] P. D. Seymour, On the points-lines-planes conjecture, J. Combin. Theory Ser. B **33** (1982), 17–26.

[21] D. J. A. Welsh, Matroid Theory, Academic Press, 1976.

[22] D. J. A. Welsh, Combinatorial problems in matroid theory, in *Combinatorial Mathematics and its Applications* (ed. D. J. A. Welsh), Academic Press, London, 1971, 291–306.

[23] D. J. A. Welsh, A bound for the number of matroids, *J. Comb. Theory* **6** (1969), 313–316.

[24] M. Wild, The asymptotic number of inequivalent binary codes and nonisomorphic binary matroids, *Finite Fields Appl.*, **6** (2000), 192–202.

E-mail address: `dukes@labri.fr`

LaBRI, Université Bordeaux 1, 351 cours de la Libération, 33405 Talence Cedex, France.