Two remarks concerning balanced matroids

Mark Jerrum^{*} School of Informatics University of Edinburgh

February 20, 2018

Abstract

The property of balance (in the sense of Feder and Mihail) is investigated in the context of paving matroids. The following examples are exhibited: (a) a class of "sparse" paving matroids that are balanced, but at the same time rich enough combinatorially to permit the encoding of hard counting problems; and (b) a paving matroid that is not balanced. The computational significance of (a) is the following. As a consequence of balance, there is an efficient algorithm for approximating the number of bases of a sparse paving matroid within specified relative error. On the other hand, determining the number of bases exactly is likely to be computationally intractable.

1 Discussion

Let E be a finite ground set and $\mathcal{B} \subseteq 2^E$ a collection of subsets of E. We say that \mathcal{B} forms the collection of *bases* of a *matroid* $M = (E, \mathcal{B})$ if the following two conditions hold:

- 1. All bases (sets in \mathcal{B}) have the same size r, namely the rank of M.
- 2. For every pair of bases $X, Y \in \mathcal{B}$ and every element $e \in X$, there exists an element $f \in Y$ such that $X \cup \{f\} \setminus \{e\} \in \mathcal{B}$.

^{*}Postal address: School of Informatics, University of Edinburgh, The King's Buildings, Edinburgh EH9 3JZ, United Kingdom.

Several other equivalent axiomatisations of matroid are possible, but the above choice turns out to be the most appropriate for our needs. For other possible axiomatisations, and more on matroid theory generally, consult Oxley [10] or Welsh [14].

The above axioms for a matroid capture the notion of linear independence. Thus if $S = \{u_0, \ldots, u_{m-1}\}$ is a set of *n*-vectors over a field *K*, then the maximal linearly independent subsets of *S* form the bases of a matroid with ground set *S*. The bases in this instance have size equal to the dimension of the vector space spanned by *S*, and they clearly satisfy the second or "exchange" axiom. A matroid that arises in this way is *vectorial*, and is said to be *representable over K*. A matroid that is representable over every field is said to be *regular*. An important combinatorial example is provided by the collection of all spanning trees in an undirected graph *H*: these form the bases of a matroid, the *cycle matroid of G*, with ground set E(H), the edge set of *H*. A matroid that arises as the cycle matroid of some graph is called *graphic*. Graphic matroids form a proper subclass of regular matroids.

The matroid axioms given above suggest a natural walk on the set of bases of a matroid M. The bases-exchange graph G(M) of a matroid M has vertex set $\mathcal{B} = \mathcal{B}(M)$ and edge set

$$\{\{X,Y\}: X, Y \in \mathcal{B} \text{ and } |X \oplus Y| = 2\},\$$

where \oplus denotes symmetric difference. Note that the edges of the basesexchange graph G(M) correspond to the transformations guaranteed by the exchange axiom. Indeed, it is straightforward to check, using the exchange axiom, that the graph G(M) is always connected. By simulating a random walk on G(M) it is possible, in principle, to sample a basis almost uniformly at random (u.a.r.) from $\mathcal{B}(M)$. We'll return to this idea presently.

An intriguing feature of the bases-exchange graph is that it appears to have very high "edge expansion". For any matroid $M = (E, \mathcal{B})$, define the *edge expansion* of its bases-exchange graph to be

$$\alpha = \alpha(M) := \min\left\{ |\operatorname{cut}(\mathcal{A})| / |\mathcal{A}| : \emptyset \subset \mathcal{A} \subset \mathcal{B} \text{ and } |\mathcal{A}| \le \frac{1}{2} |\mathcal{B}| \right\},\$$

where $\operatorname{cut}(\mathcal{A})$ denotes the cut defined by \mathcal{A} , i.e., the set of edges in E with one endpoint in \mathcal{A} and one in $\mathcal{B} \setminus \mathcal{A}$. Whenever it has been possible to compute the edge expansion of the bases-exchange graph of a matroid M, it has been found that $\alpha(M) \geq 1$. The conjecture that $\alpha(M) \geq 1$ for all matroids is a special case of an even stronger one, called the "zeroone polytope conjecture" of Mihail and Vazirani [9, 8]. The circumstantial evidence in favour of the conjecture, even in its restricted matroid version, is far from overwhelming. Our ignorance concerning the edge expansion of matroids in general is almost total: it is perfectly possible that a sequence of matroids exists for which $\alpha(M)$ decays exponentially fast as a function of the size |E| of the ground set. Nevertheless there is an interesting class of matroids M, the "balanced" matroids, for which the lower bound $\alpha(M) \ge 1$ has been established. The definition of balanced matroid (given below) is due to Feder and Mihail [5], as is the proof that balance implies expansion.

Aside from its intrinsic appeal, the expansion conjecture for matroids (and even more so the zero-one polytope conjecture) has important algorithmic consequences, which arise from the following considerations. Suppose we simulate an unbiased random walk on the bases-exchange graph G(M), with uniform transition probabilities (which could be taken as 1/rm, where m = |E| is the size of the ground set and r the rank). The walk is ergodic and converges to a stationary distribution on bases which is uniform. It is possible, in principle, to use the walk to sample a basis (almost) u.a.r. from $\mathcal{B}(M)$. From there it is a short step (see, e.g., [6, §3.2] for the general principle) to estimating the number $|\mathcal{B}(M)|$ of bases within arbitrarily small relative error. The efficiency of this approach depends crucially on the "mixing time" (number of steps to convergence to near-stationarity) of the random walk. As far as we know, this mixing time could be exponential in m. However, the mixing time is short whenever $\alpha(M) \geq 1$ (or something somewhat weaker) holds. For example, in the case of balanced matroids, the mixing time is known to be $O(rm \log r)$:¹ see Jerrum and Son [7], which improves quantitatively on Feder and Mihail [5].

The standard examples of balanced matroids are regular matroids, which were shown to be balanced by Feder and Mihail [5], and uniform matroids, which are trivially balanced. (The bases of the uniform matroid of rank ron E are all r-element subsets of E.) From an algorithmic point of view, this is unfortunate, since the bases of a regular matroid may be counted exactly via linear algebra, and the number of bases of a uniform matroid is trivially $\binom{m}{r}$. (It can be shown that the bases of a regular matroid are in 1-1 correspondence with the non-singular $r \times r$ submatrices of an $r \times m$ unimodular matrix, and that the number of these can be computed using the Binet-Cauchy formula. Refer to Dyer and Frieze [4, §3.1] for a discussion of this topic.)

The first observation in this paper is that paving matroids from a certain class, which will be called "sparse", are all balanced. (Definitions of "paving matroid", and "sparse paving matroid" will be given in §2.) The

¹To avoid trivialities, assume $r \ge 2$.

class of sparse paving matroids is combinatorially rich and it is easy to express one's favourite computationally hard counting problem in terms of counting the bases of a sparse paving matroid. This shows that balance is a concept that is not entirely devoid of algorithmic interest: specifically, there exists a class of matroids M for which (a) exact calculation of $|\mathcal{B}(M)|$ is as hard as counting satisfying assignments to a Boolean formula, and hence is almost certainly computationally intractable, whereas (b) $|\mathcal{B}(M)|$ may be approximated within arbitrarily small relative error in polynomial time by simulating random walks on bases-exchange graphs.²

The second observation resolves an obvious question raised by the first: namely, are all paving matroids balanced? It transpires that the answer is no, but the construction of a counterexample requires non-trivial effort. The counterexample is based on the Steiner system S(5, 8, 24). Welsh [14, §12.6] has noted the special position that this Steiner system holds in the theory of matroids.

A closing historical remark. Dirk Vertigan (personal communication) has described a class of balanced matroids, unrelated to paving matroids, whose bases are hard to count in the sense we have in mind in this note (and which will be clarified in §3). His result was presented during the DIMACS Special Year on Graph Theory and Algorithms (1991–2), but was never published. Aside from applying to a different class of matroids, his construction was apparently more complicated than the one given here. So even if the result is not completely new, it seems worthwhile to record it here.

2 A class of balanced paving matroids

Suppose $M = (E, \mathcal{B})$ is a matroid of rank r. A subset of E is called an *independent set* if it a subset of some basis in \mathcal{B} . A subset of E that is not an independent set is a *dependent set*. A minimal (with respect to set inclusion) dependent set is a *circuit*. The matroid M is said to be *paving* if all (r-1)-element subsets of E are independent sets. Alternatively, one could say that all circuits of M are of size either r or r+1. Every r-element subset of M is thus either a basis or a circuit.

A element of E that is contained in no basis of M is a *loop*, and one that is contained in every basis is a *coloop*. Two absolutely central operations on

²The issue of balance is not in fact crucial here, as Chávez Lomelí and Welsh [2] have presented a polynomial-time algorithm for approximately counting bases of an arbitrary paving matroid.

matroids are contraction and deletion. Assume that $e \in E(M)$ is neither a loop nor a coloop. If e is an element of the ground set of M then the matroid $M \setminus e$ obtained by *deleting* e has ground set $E(M \setminus e) = E(M) \setminus \{e\}$ and bases $\mathcal{B}(M \setminus e) = \{X \subseteq E(M \setminus e) : X \in \mathcal{B}(M)\}$; the matroid M/eobtained by *contracting* e has ground set $E(M/e) = E(M) \setminus \{e\}$ and bases $\mathcal{B}(M/e) = \{X \subseteq E(M/e) : X \cup \{e\} \in \mathcal{B}(M)\}$. Any matroid obtained from M by a series of contractions and deletions is a *minor* of M.

The matroid M is said to possess the negative correlation property if the inequality $\Pr(e \in X \mid f \in X) \leq \Pr(e \in X)$ holds for all pairs of distinct elements $e, f \in X$, where we assume that $X \in \mathcal{B}$ is chosen u.a.r. In other words the knowledge that f is present in X makes the presence of e less likely.³ Further, the matroid M is said to be balanced if all minors of M (including M itself) possess the negative correlation property. For more on balanced matroids in a general matroidal context, refer to Choe and Wagner [3].

Let (E, \mathcal{B}) be a paving matroid of rank r on ground set E. We have seen that such a matroid is defined by the set C_r of circuits with r elements. Oxley [10, Prop. 1.3.10] provides the following useful characterisation of paving matroids.

Lemma 1. Let $C_r \subset 2^E$ be a collection of r-element subsets of E. Then C_r defines (in the above sense) a paving matroid on E precisely if the following condition holds: for all $C, C' \in C_r$, if $|C \oplus C'| = 2$ then every r-element subset of $C \cup C'$ is in C_r .

We say that a paving matroid is $sparse^4$ if

$$|C \oplus C'| > 2$$
 for all distinct circuits $C, C' \in \mathcal{C}_r$. (1)

Note that, by Lemma 1, any collection C_r of r-element subsets of E satisfying (1) defines a (sparse) paving matroid.

Lemma 2. Sparse paving matroids are balanced.

Proof. We first verify that every minor of a sparse paving matroid is a sparse paving matroid. This is routine. Suppose $M = (E, C_r)$ is a sparse paving matroid, and $e \in E$ is arbitrary. Note that e cannot be a coloop (except in the trivial case $r \geq |E| - 1$) and so the rank of $M \setminus e$ is r. The circuits of size r in $M \setminus e$ are simply all the sets in C_r that avoid e [10, Eq. (3.1.14)].

³We assume here that $Pr(f \in X) > 0$, i.e., that f is not a loop.

 $^{^4 \}rm Clearly,$ the qualifier "sparse" is intended to refer to the circuits and not the bases of the matroid.

This subcollection of C_r clearly continues to satisfy (1). Furthermore, e cannot be a loop (except in the trivial case r = 1), and so the rank of M/e is r - 1. The circuits of size r - 1 in M/e are all r - 1 element subsets $C \subseteq E \setminus \{e\}$ satisfying $C \cup \{e\} \in C_r$ [10, Prop. 3.1.11]. Again, it is clear that this collection of circuits satisfies (1).

It remains to show that the events $e \in X$ and $f \in X$ are negatively correlated for all distinct $e, f \in E$, assuming X is a basis selected u.a.r. Partition $\mathcal{B} = \mathcal{B}_{ef} \cup \mathcal{B}_{e\bar{f}} \cup \mathcal{B}_{\bar{e}f} \cup \mathcal{B}_{\bar{e}\bar{f}}$ into the sets of bases (respectively) including e and f, including e but excluding f, including f but excluding e, and excluding both e and f. Consider the bipartite subgraph of the bases exchange graph G(M) induced by vertex sets \mathcal{B}_{ef} and $\mathcal{B}_{e\bar{f}}$. Each vertex (basis) $X \in \mathcal{B}_{ef}$ is adjacent to at least m - r - 1 vertices in $\mathcal{B}_{e\bar{f}}$. (Consider the collection of r-elements sets $\{X \cup \{g\} \setminus \{f\} : g \in E \setminus X\}$. Condition (1) ensures that this collection contains at most one circuit.) On the other hand, each vertex (basis) in $X \in \mathcal{B}_{e\bar{f}}$ is adjacent to at most r - 1 vertices in \mathcal{B}_{ef} . (The vertices adjacent to X are all of the form $X \cup \{f\} \setminus \{g\}$ for some $g \in X \setminus \{e\}$.) It follows that

$$(m-r-1)\left|\mathcal{B}_{ef}\right| \le (r-1)\left|\mathcal{B}_{e\bar{f}}\right|.$$
(2)

Likewise, consider the bipartite subgraph induced by vertex sets $\mathcal{B}_{\bar{e}\bar{f}}$ and $\mathcal{B}_{\bar{e}f}$. Every vertex $X \in \mathcal{B}_{\bar{e}\bar{f}}$ is adjacent to at least r-1 vertices in $\mathcal{B}_{\bar{e}f}$. (Consider the collection of *r*-elements sets $\{X \cup \{f\} \setminus \{g\} : g \in X\}$. As before, this collection contains at most one circuit.) On the other hand, each vertex (basis) in $X \in \mathcal{B}_{\bar{e}f}$ is adjacent to at most m-r-1 vertices in $\mathcal{B}_{\bar{e}\bar{f}}$. It follows that

$$(r-1)\left|\mathcal{B}_{\bar{e}\bar{f}}\right| \le (m-r-1)\left|\mathcal{B}_{\bar{e}f}\right|.$$
(3)

(Inequality (3) does not rely on sparseness, and holds in fact for any paving matroid.)

Multiplying inequalities (2) and (3) yields

$$|\mathcal{B}_{ef}| imes |\mathcal{B}_{\bar{e}\bar{f}}| \le |\mathcal{B}_{e\bar{f}}| imes |\mathcal{B}_{\bar{e}f}|.$$

A little algebraic manipulation reveals that this inequality is equivalent to $\Pr(e \in X \mid f \in X) \leq \Pr(e \in X)$ where X is selected u.a.r. from the bases of M.

It is interesting to note that a simple bound on the density of bases of a matroid is sufficient to establish the negative correlation property. Specifically, it suffices that $|\mathcal{B}| \ge (1 - \frac{m-r}{2m^2})\binom{m}{r}$. (Martin Dyer, personal communication.) However, since balance requires negative correlation to hold for all

minors, it is likely that bases need to be somewhat uniformly distributed as well as dense. The sparse paving definition is a convenient way of ensuring these conditions.

3 Counting bases is hard, even in balanced matroids

In discussing algorithms for matroids, the issue of representation is necessarily problematic, not least because the number of matroids on a ground set of size m is doubly exponential in m. Indeed, it is easy to see that the number of sparse paving matroids is already doubly exponential.⁵ We may note, in passing, that regular matroids form only a tiny fraction of all balanced matroids, since the number of regular matroids is only singly exponential in m.

In this section, we avoid the issue of representing instances of paving matroids by not providing a formal definition of the bases counting problem. Instead we indicate a simple method of encoding hard counting problems in sparse paving matroids, which hopefully will seem quite natural. A "hard" counting problem in this context is one that is #P-complete. The class #P was introduced by Valiant as a counting analogue of the more familiar class NP of decision problems. He showed [12] that many natural counting problems are complete for #P with respect to polynomial-time Turing reducibility, and hence almost certainly computationally intractable. In particular, #P-completeness provides strong evidence against the existence of a polynomial-time algorithm.

One of the original problems on Valiant's list of #P-complete problems is counting Hamiltonian cycles in an undirected graph. Suppose H = ([r], E)is an undirected graph on r vertices with edge set E. Let C_r be the collection of all Hamilton cycles in H. Since any pair of Hamilton cycles differ in at least four edges, the collection C_r satisfies (1), and hence defines a sparse paving matroid (E, \mathcal{B}) of rank r on E. Furthermore, it is clear that the number of Hamiltonian cycles in H is equal to $|C_r| = {m \choose r} - |\mathcal{B}|$. This gives a natural — in a general combinatorial, though not specifically matroidal sense — encoding of a #P-complete problem as a sparse paving matroid.

It is interesting to observe that the number $|\mathcal{B}|$ of bases of the matroid just constructed can be efficiently approximated (by virtue of balance, or

⁵Piff and Welsh's lower bound on combinatorial geometries [11] is essentially based on counting sparse paving matroids.

by appeal to [2]) whereas the number $|\mathcal{C}_r|$ of non-bases cannot (since even deciding emptiness of \mathcal{C}_r is hard).

4 A paving matroid that is not balanced

Given that a relatively large subset of paving matroids are balanced, it is natural to ask whether all paving matroids are balanced. The answer is "no", but one has to work a little to obtain a counterexample. The problem is to squeeze in enough circuits to violate the negative correlation property.

We construct a paving matroid of rank six on a ground set E of size 24 containing two distinguished elements e, f, and prove that e and f are positively correlated. The construction is based on the Steiner system S(5, 8, 24). Denote by E the ground set of S(5, 8, 24) and by $\mathcal{V} \subset 2^E$ its set of blocks. (The ground sets of the Steiner system and of the paving matroid will coincide, so it is notationally convenient to confuse the two.) The salient features of S(5, 8, 24) are the following $[1, \S 3.6]$:

- |E| = 24;
- each block in \mathcal{V} is of size eight;
- each subset of five elements of E is contained in a unique block of \mathcal{V} .

We'll define the desired paving matroid (E, \mathcal{B}) of rank six by specifying its circuits of size six. Let e, f be distinguished elements of E. We'll declare a subset $C \subset E$ of size six to be a circuit of the matroid if there exists a block $V \in \mathcal{V}$ with $|V \cap \{e, f\}| = 1$ and $V \supset C$. Note that two distinct blocks can have at most four elements in common, and the same is true of circuits coming from different blocks. Hence, by Lemma 1, these circuits define a paving matroid. The bases of this paving matroid are simply all six-element sets that are not circuits.

Recall the partition $\mathcal{B} = \mathcal{B}_{ef} \cup \mathcal{B}_{e\bar{f}} \cup \mathcal{B}_{\bar{e}f}$. We'll calculate the sizes of the various sets occurring in this partition, and show that $|\mathcal{B}_{ef}| \times |\mathcal{B}_{\bar{e}\bar{f}}| > |\mathcal{B}_{e\bar{f}}| \times |\mathcal{B}_{\bar{e}\bar{f}}|$. It follows directly that the events $e \in X$ and $f \in X$ are positively correlated, assuming $X \in \mathcal{B}$ is selected u.a.r.

- $|\mathcal{B}_{ef}| = 7315$. By construction, there are no circuits of size six containing both e and f. In other words, every six-element set containing e and f is a base, and $|\mathcal{B}_{ef}| = \binom{22}{4} = 7315$.
- $|\mathcal{B}_{e\bar{f}}| = |\mathcal{B}_{\bar{e}f}| = 22638$. Denote by $\mathcal{V}_e \subset \mathcal{V}$ the blocks of the Steiner system containing e, and by $\mathcal{V}_{e\bar{f}}$ the blocks containing e but excluding f,

etc. First we count the blocks $\mathcal{V}_{e\bar{f}} \subset \mathcal{V}$ containing e but not f. (Every circuit of size six that contains e but not f must be a subset of a unique such block.) Consider any set $A \subset E \setminus \{e\}$ of size four. Observe that $A \cup \{e\}$ defines a unique block in \mathcal{V}_e , and moreover that every such block is defined by exactly $\binom{7}{4}$ such sets A. Thus $|\mathcal{V}_e| = \binom{23}{4}/\binom{7}{4} = 253$. Similarly each set $A \subset E \setminus \{e, f\}$ of size three defines a unique block in \mathcal{V}_{ef} , and every such block is defined by exactly $\binom{6}{3}$ such sets A. Thus $|\mathcal{V}_{ef}| = \binom{22}{3}/\binom{6}{3} = 77$. Subtracting, $|\mathcal{V}_{e\bar{f}}| = 176$. As we observed, each circuit of size six containing e but not f is contained in a unique block in $\mathcal{V}_{e\bar{f}}$. The number of such circuits is thus $176 \times \binom{7}{5} = 3696$. Every six-element set containing e but excluding f is a basis unless it is one of these 3696 circuits. Thus $|\mathcal{B}_{e\bar{f}}| = \binom{22}{5} - 3696 = 22638$. Naturally, $|\mathcal{B}_{\bar{e}\bar{f}}| = |\mathcal{B}_{e\bar{f}}|$ by symmetry.

• $|\mathcal{B}_{\bar{e}\bar{f}}| = 72149$. Every six-element set avoiding both e and f is a base unless it is contained in a block in $\mathcal{V}_{e\bar{f}}$ or $\mathcal{V}_{\bar{e}f}$. Thus $|\mathcal{B}_{\bar{e}\bar{f}}| = \binom{22}{6} - 2 \times 176 \times \binom{7}{6} = 72149$.

In summary,

$$|\mathcal{B}_{ef}| \times |\mathcal{B}_{\bar{e}\bar{f}}| = \frac{89015}{86436} \times |\mathcal{B}_{e\bar{f}}| \times |\mathcal{B}_{\bar{e}f}|.$$

This example is perhaps a little larger than necessary, but there are limits to how much it can be simplified. For example, Wagner [13] shows that any matroid that is not balanced must have rank at least four. Furthermore, in order to violate the negative correlation property, it is necessary to achieve a high density of circuits of size r.

Acknowledgement

I thank Martin Dyer for enlightening and encouraging remarks on an early version of this note.

References

- N. L. Biggs and A. T. White. Permutation groups and combinatorial structures, volume 33 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1979.
- [2] Laura Chávez Lomelí and Dominic Welsh. Randomised approximation of the number of bases. In *Matroid theory (Seattle, WA, 1995)*, volume

197 of *Contemp. Math.*, pages 371–376. Amer. Math. Soc., Providence, RI, 1996.

- [3] Young-Bin Choe and David G. Wagner. Rayleigh matroids. arXiv:math.CO/0307096.
- [4] Martin Dyer and Alan Frieze. Random walks, totally unimodular matrices, and a randomised dual simplex algorithm. *Math. Programming*, 64(1, Ser. A):1–16, 1994.
- [5] Tomás Feder and Milena Mihail. Balanced matroids. In Proceedings of the 24th Annual ACM Symposium on Theory of Computing (STOC), pages 26–38. ACM Press, 1992.
- [6] Mark Jerrum. Counting, sampling and integrating: algorithms and complexity. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 2003.
- [7] Mark Jerrum and Jung-Bae Son. Spectral gap and log-Sobolev constant for balanced matroids. In Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science (FOCS'02), pages 721–729. IEEE Computer Society Press, 2002.
- [8] Volker Kaibel. On the expansion of graphs of 0/1-polytopes. arXiv:math.CO/0112146.
- [9] Milena Mihail. On the expansion of combinatorial polytopes. In Mathematical foundations of computer science 1992 (Prague, 1992), volume 629 of Lecture Notes in Comput. Sci., pages 37–49. Springer, Berlin, 1992.
- [10] James G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1992.
- [11] M. J. Piff and D. J. A. Welsh. The number of combinatorial geometries. Bull. London Math. Soc., 3:55–56, 1971.
- [12] Leslie G. Valiant. The complexity of enumeration and reliability problems. SIAM J. Comput., 8(3):410–421, 1979.
- [13] David G. Wagner. Rank three matroids are Rayleigh. arXiv:math.CO/0403216.
- [14] D. J. A. Welsh. *Matroid theory*. Academic Press [Harcourt Brace Jovanovich Publishers], London, 1976. L. M. S. Monographs, No. 8.