Matroids

1 Definition

A matroid is an abstraction of the notion of linear independence in a vector space. See Oxley [6], Welsh [7] for further information about matroids.

A *matroid* is a pair $(E, \mathscr{I})$, where E is a set and $\mathscr{I}$ a non-empty family of subsets of E (called *independent sets*) satisfying the conditions:

(a) If $I \in \mathscr{I}$ and $J \subseteq I$, the $J \in \mathscr{I}$.

(b) (the *Exchange Axiom*) If $I_1, I_2 \in \mathscr{I}$ and $|I_2| > |I_1|$, then there exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathscr{I}$.

The following are examples of matroids:

- E is the edge set of a graph G; a set of edges is independent if and only if it is a forest. (Such a matroid is a *graphic matroid*.)
- E is a set of vectors in a vector space V; a set of vectors is independent if and only if it is linearly independent. (Such a matroid is a *vector matroid*.)
- E is a subset of an algebraically closed field L; a set of field elements is independent if and only if it is algebraically independent over an algebraically closed subfield K of L. (Such a matroid is called an *algebraic matroid*.)
- E is a set with a family $(\mathscr{A} = (A_i : i \in I)$ of subsets; a subset of E is independent if and only if it is a partial transversal of $\mathscr{A}$. (Such a matroid is a *transversal matroid*.)
- Let $\mathscr{A}$ be a family of subsets of E such that $E \notin \mathscr{A}$ and $|A \cap A'| \leq k-2$ for all $A, A' \in \mathscr{A}$. A subset of size at most k is independent if and only if it is not contained in any member of $\mathscr{A}$. (Such a matroid is called a *paving matroid*. Examples include the case where $\mathscr{A}$ is the set of blocks of a Steiner system $S(k-1, l, n)$.)

The exchange axiom implies that all maximal independent sets have the same cardinality r; such sets are called *bases* of M, and r is the *rank* of M. More generally, for any subset A of E, the maximal independent subsets of A all have the same rank; this is the *rank* of A, and is denoted by $\rho(A)$. Other matroid concepts:

- a *circuit* is a minimal element of $\mathscr{P}(E) \setminus \mathscr{I}$;
- a *flat* is a subset F of E with the property that, for any $e \in E$, $\rho(F \cup \{e\}) = \rho(F)$ implies $e \in F$;
- a *hyperplane* H is a maximal proper flat of M (a flat satisfying $\rho(H) = \rho(E) - 1$).

Matroids can be axiomatised in terms of their bases, circuits, rank function, flats, or hyperplanes.

It is convenient to allow a vector matroid to have "repeated elements", just as a graphic matroid arising from a multigraph can. Thus, given a family $(v_1, \ldots, v_n)$ of vectors in a vector space V, we take $E = \{1, \ldots, n\}$, and define a subset I of E to be independent if the subfamily $(v_i : i \in I)$ of vectors is linearly independent. If $V = F^k$ for some field F, we regard the vectors as the columns of a $k \times n$ matrix over F. (A "matroid" is a generalisation of a "matrix" in this sense.)

The *dual* of a matroid M is the matroid M^* on the same ground set whose bases are the complements of the bases of M. Note that $(M^*)^* = M$.

The *uniform matroid* $U_{k,n}$ is the matroid on n elements whose independent sets are all the subsets of size k. It is easy to see that $(M_{k,n})^* = M_{n-k,n}$.

2 Geometric matroids

A *loop* in a matroid M on E is an element e with $\rho(\{e\}) = 0$ (that is, such that $\{e\}$ is dependent). Two non-loops e_1, e_2 are *parallel* if $\rho(\{e_1, e_2\}) = 1$ (that is, such that $\{e_1, e_2\}$ is a circuit). Parallelism is an equivalence relation on the set of non-loops.

A matroid is *geometric* if it has no loops and parallel elements are equal; that is, if all sets of size at most 2 are independent.

Classically, we obtain a projective space from a vector space by deleting the zero vector and identifying vectors which are scalar multiples of each other. The same procedure works in a general matroid: if we delete the loops, and then identify the elements in each parallel class, we obtain a geometric matroid.

Geometric matroids are sometimes called "combinatorial geometries".

3 Deletion and contraction

An element e of a matroid is a loop if and only if it is contained in no basis. Dually, we say that e is a *coloop* if it is contained in every basis; that is, if it is a loop in the dual matroid.

Note that in a graphic matroid, a loop is an edge which is a loop in the graph-theoretic sense, while a coloop is an edge which is a *bridge* or *isthmus* in the graph.

Let $M = (E, \mathscr{I})$ be a matroid, and e an element of M.

If e is not a coloop, we define the matroid obtained by *deleting* e to be

$$M \backslash e = (E \setminus \{e\}, \{I \in \mathscr{I} : e \notin I\}).$$

Dually, if e is not a loop, we define the matroid obtained by *contracting* e to be

$$M/e = (E \setminus \{e\}, \{I \setminus \{e\} : e \in I \in \mathscr{I}\}).$$

Clearly we have

$$(M/e)^* = M^* \backslash e$$

if e is not a loop.

In a graphic matroid, deletion and contraction of an edge coincide with the usual graph-theoretic operations with the same names.

4 Matroids and codes

Let C be a linear code of length n and dimension k over $\mathrm{GF}(q)$ (see the topic essay on codes). Let G be a generator matrix for C, and associate with C the vector matroid M formed by the columns of G. In other words, $E = \{1, \ldots, n\}$; and a set $I \subseteq E$ is independent if and only if the family of columns of G with indices in I is linearly independent.

The correspondence between matroid and code is preserved by the "natural" equivalences on each of them. For elementary row operations applied to G leave C unchanged and simply change the representation of M; while column permutations and multiplication of columns by non-zero scalars don't affect M and simply replace C by a *monomial-equivalent* code.

We see that a set I of coordinate positions is independent in M if and only if all possible $|I|$-tuples of field elements occur in these positions in codewords of C;

in other words, I does not contain the support of a non-zero element of the dual code $C^{\perp}$.

The operations of deletion and contraction on M correspond precisely to the operations of puncturing and shortening C at a coordinate position. The matroid associated with the dual code $C^{\perp}$ of C is the dual M^* of M.

The *weight* $\mathrm{wt}(c)$ of a codeword c is the number of non-zero coordinates of c. The *minimum weight* of a code C is the smallest weight of a non-zero codeword of C, and the *weight enumerator* of C is the homogeneous polynomial

$$W_C(X,Y) = \sum_{c\in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where A_i is the number of codewords of C of weight i. The *MacWilliams relation* gives the weight enumerator of $C^{\perp}$ in terms of that of C:

$$W_{C^{\perp}}(X,Y) = \frac{1}{|C|} W_C(X+(q-1)Y, X-Y).$$

5 Tutte polynomial

The *Tutte polynomial* of a matroid $M = (E,\mathscr{I})$ with rank function ρ is the two-variable polynomial $T(M)$ given by the formula

$$T(M;x,y) = \sum_{A\subseteq E} (x-1)^{\rho E-\rho A} (y-1)^{|A|-\rho A}.$$

There is also a convenient recursive expression for the Tutte polynomial in terms of deletion and contraction:

(a) $T(\emptyset;x,y) = 1$, where $\emptyset$ is the empty matroid.

(b) If e is a loop, then $T(M;x,y) = yT(M\backslash e;x,y)$.

(c) If e is a coloop, then $T(M;x,y) = xT(M/e;x,y)$.

(d) If e is neither a loop nor a coloop, then

$$T(M;x,y) = T(M\backslash e;x,y) + T(M/e;x,y).$$

It is not hard to show that the Tutte polynomials of a matroid and its dual are related by $T(M^*;x,y) = T(M;y,x)$.

The Tutte polynomial has many important specialisations. For example:

- $T(M;1,1)$ is the number of bases of M, $T(M;2,1)$ is the number of independent sets, and $T(M;1,2)$ the number of spanning sets. (Of course, $T(M;2,2) = 2^n$.)

- If M is the graphic matroid associated with the graph G, then the chromatic polynomial of G (which counts the proper colourings of the vertices of G with k colours) is given by

$$P_G(k) = (-1)^{\rho(G)} k^{\kappa(G)} T(M(G); 1-k, 0),$$

  where $\kappa(G)$ is the number of connected components of G and $\rho(G) + \kappa(G)$ the number of vertices. Several other graph polynomials, such as those counting nowhere-zero flows with values in an abelian group of order k, or the probability that the graph remains connected if edges are removed independently with probability p, are also specialisations of the Tutte polynomial.

- If M is associated with a linear code C over $\mathrm{GF}(q)$, then the weight enumerator of C is given by

$$W_C(X,Y) = Y^{n-\dim(C)} (X-Y)^{\dim(C)} T\left(M; \frac{X+(q-1)Y}{X-Y}, \frac{X}{Y}\right)$$

  (a theorem of Greene [3]).

From Greene's Theorem and the fact that dual codes are associated with dual matroids and $T(M^*;x,y) = T(M;y,x)$, it is a simple matter to deduce the MacWilliams relation.

Since the Tutte polynomial carries so much information, it is not surprising that it is difficult to compute in general: see Welsh [8]. We will see below a class of matroids for which the Tutte polynomial can be computed more easily, the *perfect matroid designs*.

6 IBIS groups

Let G be a permutation group on the set E. A *base* for G is a sequence $(e_1, \ldots, e_b)$ of points of E whose pointwise stabiliser (in G) is the identity. A base is *redundant* if some point e_i is fixed by the pointwise stabiliser of the preceding points in the base (such a point can be omitted without affecting the defining property of a base); it is *irredundant* if this doesn't happen. Note that the property of redundancy may depend on the order of the base points.

Cameron and Fon-Der-Flaass [1] showed that the following three conditions on a permutation group G are equivalent:

- all irredundant bases contain the same number of elements;
- irredundant bases are preserved by re-ordering;
- the irredundant bases are the bases of a matroid.

They called a group satisfying these properties an *IBIS group* (for **I**rredundant **B**ases of **I**nvariant **S**ize).

Cameron and Fon-Der-Flaass showed that, if G is an IBIS group whose associated matroid is uniform $U_{k,n}$, so that every k-tuple is an irredundant base for G, with $k > 1$, then G is $(k-1)$-transitive (see the topic essay on permutation groups for this concept). In particular:

- if $k = 2$, then G is a *Frobenius group,* and a lot is known about its structure (theorems of Frobenius, Zassenhaus and Thompson);
- if $k > 2$, then G is explicitly known.

Another case where a classification is known is the following. The permutation group G is *base-transitive* if it permutes its irredundant bases transitively. Clearly in this case all the bases have the same size, and so G is an IBIS group. Such groups were completely determined by Maund [4], using the Classification of Finite Simple Groups; those whose associated matroid has rank at least 7 were found by an "elementary" (but by no means easy) argument by Zil'ber [9].

Any code gives rise to an IBIS group, whose matroid is an "inflation" of that of the code, as follows. Let C be a linear code of length n over $\mathrm{GF}(q)$. The additive group of C acts as a permutation group G on $\{1,\ldots,n\} \times \mathrm{GF}(q)$ by the rule

$$c = (c_1,\ldots,c_n) : (i,a) \mapsto (i,a+c_i).$$

Then G is an IBIS group whose rank is equal to the dimension of C. The projection $(i,a) \mapsto i$ collapses classes of parallel elements and takes the matroid of G to the matroid of C.

7 Perfect matroid designs

A *perfect matroid design*, or *PMD*, is a matroid M, of rank r say, for which there exist integers $f_0, f_1, \ldots, f_r$ such that, for $0 \le i \le r$, any flat of rank i has cardinality f_i. The tuple $(f_0, f_1, \ldots, f_r)$ is the *type* of M. Note that $f_r = n$ is the cardinality of the set of elements.

It is clear that the matroid arising from a base-transitive permutation group is a PMD: any two independent sets of the same size are equivalent under an automorphism, and hence so are their spans.

If M is a PMD of type $(f_0, f_i, \ldots, f_r)$, then the geometrisation of M is a PMD of type $(f_0', f_1', \ldots, f_r')$, where $f_i' = (f_i - f_0)/(f_1 - f_0)$. In particular, $f_0' = 0$, $f_1' = 1$.

The most familiar examples of geometric PMDs are (possibly truncated) projective and affine spaces over finite fields: we have

- $f_i = (q^i - 1)/(q-1)$ for projective spaces over $\mathrm{GF}(q)$;
- $f_0 = 0$ and $f_i = q^{i-1}$ for $i > 0$ for affine spaces over $\mathrm{GF}(q)$.

A Steiner system $S(t,k,v)$ is a PMD: the i-flats are the i-sets for $i < t$, the t-flats are the blocks, and the rank of the matroid is $t+1$.

Apart from these examples, the only known PMDs arise from the *Hall triple systems*. A Hall triple system is a Steiner triple system, not an affine space over $\mathrm{GF}(3)$, in which any three non-collinear points lie in a subsystem of size 9 (isomorphic to the affine plane over $\mathrm{GF}(3)$). The smallest example of such a system has 81 points, and was constructed by Marshall Hall Jr. The number of points in a Hall triple system is necessarily a power of 3, and all powers of 3 greater than 27 occur. Now we obtain a PMD of rank 4 by taking the flats of ranks 1, 2, 3 to be the points, triples, and 9-point subsystems respectively.

In a PMD of type $(f_0, f_1, \ldots, f_r)$, if $i < j$, then the number of j-flats containing a given i-flat is equal to

$$\frac{(f_r - f_i)(f_r - f_{i+1}) \cdots (f_r - f_{j-1})}{(f_j - f_i)(f_j - f_{i+1}) \cdots (f_j - f_{j-1})}.$$

In particular, in a geometric PMD, the points and i-flats form a 2-design for $1 \le i \le r-1$. This construction includes the familiar construction of designs from the subspaces of projective and affine spaces.

Mphako [5] showed that the Tutte polynomial of a PMD can be calculated explicitly if the type is known.

See Deza [2] for a general reference on PMDs.

References

[1] P. J. Cameron and D. G. Fon-Der-Flaass, Bases for permutation groups and matroids, *Europ. J. Combinatorics* **16** (1995), 537–544.

[2] M. Deza, Perfect matroid designs, *Encycl. Math. Appl.* **40** (1992), 54–72.

[3] C. Greene, Weight enumeration and the geometry of linear codes, *Studia Appl. Math.* **55** (1976), 119–128.

[4] T. C. Maund, D.Phil. thesis, University of Oxford, 1989.

[5] E. G. Mphako, Tutte polynomials of perfect matroid designs, *Combinatorics, Probability and Computing* **9** (2000), 363–367.

[6] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[7] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

[8] D. J. A. Welsh, *Complexity: Knots, Colourings and Counting*, London Mathematical Society Lecture Notes **186**, Cambridge University Press, Cambridge, 1993.

[9] B. I. Zil'ber, The structure of models of uncountably categorical theories, pp. 359–368 in *Proc. Internat. Congr. Math.* Vol. 1 (Warsaw 1983).

Peter J. Cameron

April 12, 2005