Notes on matroids and codes

Peter J. Cameron

Abstract

The following expository article is intended to describe a correspondence between matroids and codes. The key results are that the weight enumerator of a code is a specialisation of the Tutte polynomial of the corresponding matroid, and that the MacWilliams relation between weight enumerators of a code and its dual can be obtained from matroid duality. It also provides a general introduction to matroids, an introduction to trellis decoding, and an algebraic construction of the minimal trellis of a code.

Some of this material was presented in the QMW study group, although this version is my own re-working of it. I am grateful to Carrie Rutherford and Costas Papadopoulos for their contributions. Some of Carrie's are acknowledged in the text, while Costas taught me about trellis decoding.

1 Introduction

Matroids were invented by Whitney to generalise the notion of linear independence in vector spaces. They also describe in a natural way many other situations such as acyclic sets of edges of graphs, partial transversals of families of sets, and others. The purpose of these notes is to explain a connection between matroids and linear codes. In particular, the weight enumerator of a code is a specialisation of a two-variable polynomial called the Tutte polynomial of the corresponding matroid. Duality of codes corresponds to duality of matroids, and we easily obtain the MacWilliams relation between the weight enumerators of a code and its dual. We then consider trellis decoding, examine how the size of the minimal trellis for a code is determined by the matroid. A general reference for matroid theory is Welsh [6].

A *matroid* M is a pair (E,I), where E is the finite set of *elements* of the matroid, and I a family of subsets of E called the *independent sets* of the matroid, satisfying the following axioms:

(M1) any subset of an independent set is independent;

(M2) if I_1 and I_2 are independent and $|I_1| < |I_2|$, then there exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\}$ is independent.

There are two standard examples of matroids to which we often refer. These examples give rise to much of the terminology of the subject.

Graphs. Let E be the edge set of a graph (which is permitted to have loops and multiple edges). A set of edges is *independent* if it contains no circuit. Axiom (M1) is clear; we prove (M2).

For this, we use the fact that if a graph with n vertices, m edges and c connected components contains no circuits, then $n = m + c$. Now if $|I_1| < |I_2|$ and both I_1 and I_2 are independent, then the graph with edge set I_2 has fewer components then the graph with edge set I_1, so some edge e of I_2 must join vertices in different components of the latter graph; then adding e to I_1 creates no circuit.

This matroid is called the *cycle matroid* of the graph, for reasons that will appear shortly.

Sets of vectors. Let $v_1, v_2, \ldots, v_n$ be vectors in a vector space V. We take $E = \{1, \ldots, n\}$, and let the subset I be independent if and only if $\{v_i : i \in I\}$ is linearly independent in V. (This is slightly more clumsy than taking E to be the set of vectors and independence to mean linear independence; but it allows us to have 'repeated vectors'.) The proofs of (M1) and (M2) are given in any linear algebra text. If the vector space V is the set F^m of all m-tuples of elements of F (written as column vectors), then we can conveniently represent the elements of the matroid as the columns of an $m \times n$ matrix over F. A matroid of this form is a *vector matroid*.

We check the matroid axioms. Condition (M1) is clear. To prove (M2), suppose that $(v_1, \ldots, v_n)$ are linearly independent, as also are $(w_1, \ldots, w_{n+1})$. Assume that the conclusion is false, that is, that $(v_1, \ldots, v_n, w_i)$ is linearly dependent for all i. Then we have

$$w_i = a_{i1} v_1 + \cdots + a_{in} v_n$$

for $i = 1, \ldots, n+1$. Consider the system of equations

$$x_1 a_{1j} + \cdots + x_{n+1} a_{n+1\,j} = 0$$

for $j = 1, \ldots, n$. These comprise n homogeneous equations in $n+1$ unknowns, so they have a non-zero solution $(x_1, \ldots, x_{n+1})$. (This fact is the only 'algebra' required in the proof.) But then we have

$$x_1 w_1 + \cdots + x_{n+1} w_{n+1} + 0,$$

contrary to the assumption that $(w_1, \ldots, w_{n+1})$ is a linearly independent family.

Now the basic properties of linear independence, as developed in elementary linear algebra texts, can be proved using (M1) and (M2).

2 Bases and cycles

A *basis* is an independent set which is maximal with respect to inclusion. It follows from (M2) that all bases have the same size. In a connected graph G, a basis of the cycle matroid is the set of edges of a spanning tree of G.

The *rank* $\rho(A))$ of a set A of elements of a matroid is the cardinality of the largest independent set contained in A. Again, by (M2), all maximal independent subsets of A have the same size. In the cycle matroid of a graph, the rank of a set A of edges is $n-c$, where n is the number of vertices of the graph, and c the number of connected components of the subgraph with edge set A. The rank of a sunset of a vector matroid is the dimension of the subspace spanned by the corresponding vectors.

A *cycle* in a matroid is a set which is not independent but has the property that every proper subset is independent. A cycle in the cycle matroid of a graph is the edge set of a circuit (closed path) in the graph (possibly a loop at a vertex, or two parallel edges between the same two vertices) — hence the name.

A matroid is determined by its bases, its rank function, or its cycles. For a set I is independent if and only if it is contained in some basis, or if and only if it satisfies $\rho(A) = |A|$, or if and only if it contains no cycle. It is possible to axiomatise matroids in terms of their sets of bases, their rank functions, or their sets of cycles.

As examples, we treat the axiomatisation of matroids via bases and via cycles.

Theorem 2.1 *Let $\mathcal{B}$ be a non-empty family of subsets of E. Then $\mathcal{B}$ is the family of bases of a matroid on E if and only if the following condition holds:*

(MB) if $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then there exists $y \in B_2 \setminus B_1$ such that $B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$.

Proof All bases of a matroid have the same cardinality (since if $B_1, B_2 \in \mathcal{I}$ and $|B_1| < |B_2|$ then B_1 cannot be maximal independent). Then (MB) follows from (M2) since $|B_1 \setminus \{x\}| < |B_2|$.

Conversely, suppose that (MB) holds, and let $\mathcal{I}$ be the set of all subsets of E which are contained in some member of $\mathcal{B}$. Clearly (M1) holds.

To prove (M2), take $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$. Let B_1, B_2 be members of $\mathcal{B}$ containing I_1 and I_2 respectively. If B_1 contains an element x of $I_2 \setminus I_1$, then $I_1 \cup \{x\}$ is the set required by (M2). So suppose that no such point x occurs. Now, using (MB) repeatedly, we can replace points of $B_1 \setminus I_1$ by points of B_2. Since $|I_1| < |I_2|$, we are forced to use a point x of I_2 as the replacement point before we run out of points of $B_1 \setminus I_1$. Then $I_1 \cup \{x\}$ is contained in the basis produced at this step.

Finally, we observe that $\mathcal{B}$ is precisely the set of bases in the matroid $M = (E, \mathcal{I})$: for every member of $\mathcal{B}$ is a maximal independent set, and conversely a maximal independent set is contained in a member B of $\mathcal{B}$ but has the same cardinality as B, so is equal to it.

For later use, here is a further property of bases. You may have to read this carefully to see how it differs from (MB).

Lemma 2.2 *Let B_1, B_2 be bases of a matroid, and let $y \in B_2 \setminus B_1$. Then there exists $x \in B_1 \setminus B_2$ such that $B_1 \setminus \{x\} \cup \{y\}$ is a basis.*

Proof If the conclusion were that $B_2 \setminus \{y\} \cup \{x\}$ is a basis, this would just be (MB), with B_1 and B_2 interchanged. However, as it is, we have some work to do!

We use induction on $k = |B_1 \setminus B_2| = |B_2 \setminus B_1|$. If $k = 0$, the result is vacuous, while if $k = 1$ it is trivial. So suppose that $k \geq 2$ and suppose that the result holds in all situations where B_1' and B_2' are bases with $|B_1' \setminus B_2'| < k$.

Since $k \geq 2$, we can choose $y' \in B_2 \setminus B_1$ with $y' \neq y$. Now by (MB), there exists $x' \in B_1 \setminus B_2$ such that $B_2' = B_2 \setminus \{y'\} \cup \{x'\}$ is a basis. Now $|B_1 \setminus B_2'| = k - 1$. By the induction hypothesis, there is a point $x \in B_1 \setminus B_2'$ such that $B_1 \setminus \{x\} \cup \{y\}$ is a basis, as required.

We now turn to cycles.

Theorem 2.3 *Let $\mathcal{C}$ be a family of subsets of a set E. Then $\mathcal{C}$ is the set of cycles of a matroid on E if and only if the following conditions hold:*

(MC1) No member of $\mathcal{C}$ contains another;

(MC2) If C_1, C_2 are distinct elements of $\mathcal{C}$ and $e \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq C_1 \cup C_2$ and $e \notin C_3$.

Proof Suppose first that $\mathcal{C}$ is the set of cycles (minimal dependent sets) of a matroid. Then a set is dependent if and only if it contains a member of $\mathcal{C}$. Condition (MC1) is obvious. So suppose that C_1, C_2 are cycles and $e \in C_1 \cap C_2$. If $C_1 \cup C_2 \setminus \{e\}$ does not contain a cycle, then $C_1 \cup C_2$ is a minimal dependent set, that is a cycle, contradicting minimality.

Conversely, suppose that $\mathcal{C}$ is a family of sets satisfying (MC1) and (MC2), and let $\mathcal{I}$ be the family of sets containing no member of $\mathcal{C}$. We must show that $\mathcal{I}$ is a matroid on E.

Condition (M1) is clear. To check (M2), let $I_1, I_2 \in \mathcal{I}$ with $|I_2| = |I_1| - 1$, and suppose, for a contradiction, that there is no point $y \in I_2 \setminus I_1$ such that $I_1 \cap \{y\}$ is independent. Let $I_1 \setminus I_2 = \{x_1, \ldots, x_k\}$, and $I_2 \setminus I_1 = \{y_1, \ldots, y_{k+1}\}$. We prove by induction on i that there exist at least $k - i + 1$ cycles contained in $I_1 \cup I_2$ but containing none of $x_12, \ldots, x_i$.

To start the induction for $i = 0$, observe that, because $I_1 \cup \{y_j\}$ is dependent, it contains a cycle $C(y_j)$; and $y_j \in C(y_j)$, since otherwise $C(y_j) \subseteq I_1$, contradicting the independence of I_1. So these cycles are distinct for $j = 1, \ldots, k+1$.

So suppose that the assertion holds for i. If none of the given $k - i = 1$ cycles contains x_{i+1}, then we are done. So suppose that x_{i+1} lies in m of these cycles, say $C_1, \ldots, C_m$. By (MC2), for $j = 1, \ldots, m-1$, we can find a cycle C'_j contained in $C_j \cup C_m$ but not containing x_{i+1}. Replacing C_j by C'_j and deleting C_m completes the induction step.

Now for $j = k$, the assertion we have proved says that there is at least one cycle contained in $I_1 \cup I_2$ but containing no point of $I_1 \setminus I_2$; that is, contained in I_2. But this contradicts the independence of I_2.

So $\mathcal{I}$ is a matroid on E.

Moreover, $\mathcal{C}$ is the family of all cycles in the matroid $\mathcal{I}$. For a set in $\mathcal{C}$ is not in $\mathcal{I}$, but all its proper subsets are (else it properly contains another member of $\mathcal{C}$. Conversely, if C is minimal with respect to containing no member of $\mathcal{I}$, then C contains a member of $\mathcal{C}$ but no proper subset of it does; that is, $C \in \mathcal{C}$.

An interesting interpretation of the matroid cycle axioms was pointed out to me by Dima Fon-Der-Flaass.

Consider the game of Bingo. Each player has a card with some numbers written on it. The caller announces in turn the numbers in a sequence. The first player all of whose numbers have been called is the winner. What conditions should the cards satisfy? Let C_i be the set of numbers on the ith card.

- If $C_i \subseteq C_j$ then the player holding the jth card can never win, which is unsatisfactory.

- We want to avoid the situation in which two players complete their cards at the same time and the prize is disputed. Suppose that C_1 and C_2 are the sets of numbers on any two cards, and $e \in C_1 \cap C_2$. If the numbers in $C_1 \cup C_2$ are called with e last, then both players 1 and 2 would claim the prize (contrary to what we want), unless the prize has already been claimed by, say player 3, where $C_3 \subseteq C_1 \cup C_2$ and $e \notin C_3$.

In other words, the sets C_i should be the cycles of a matroid!

More formally, this result can be stated as follows. We define a *clutter* (also known as an *antichain* or *Sperner family* to be a family of sets, none of which contains another.

Theorem 2.4 *Let $\mathcal{C}$ be a family of subsets of E. Then $\mathcal{C}$ is the family of cycles of a matroid if and only if it is a clutter with the following property: for any total ordering of E, there is a set $C \in \mathcal{C}$ whose greatest element is smaller than the greatest element of any other set in $\mathcal{C}$.*

3 The greedy algorithm

One important property of matroids is that they are precisely the structures in which the greedy algorithm works successfully.

The *greedy algorithm* is defined whenever we are trying to find the maximum value of a function. It operates in the most short-sighted way possible: it proceeds by taking steps, each of which increases the function by as much as possible. So it is prone to get trapped at a local maximum which is smaller than the absolute maximum.

More formally, suppose that we are given a set X of points with a *weight function* w from X to the set of non-negative real numbers. We are also given a non-empty family $\mathcal{B}$ of k-element subsets of X. The *weight* of a subset B is defined to be $\sum_{x \in B} w(x)$. The problem is to choose the member of $\mathcal{B}$ of maximum weight.

The greedy algorithm works as follows. Given that $e_1, \ldots, e_{i-1}$ have already been chosen. The next point e_i is chosen to maximise $w(e_i)$ subject to the condition that $\{e_1, \ldots, e_i\}$ is contained in some member of $\mathcal{B}$. Clearly the algorithm succeeds in choosing k points, which form a set in $\mathcal{B}$.

Theorem 3.1 *The non-empty family $\mathcal{B}$ is the family of bases of a matroid if and only if, for any weight function w, the greedy algorithm chooses a member of $\mathcal{B}$ of maximum weight.*

Proof Suppose that $\mathcal{B}$ is the set of bases of a matroid, and let w be any weight function. Suppose that the greedy algorithm chooses successively $e_1, e_2, \ldots, e_k$. Let us assume that there is a basis of greater weight than $\{e_1, \ldots, e_k\}$, say $\{f_1, \ldots, f_k\}$, where $w(f_1) \geq w(f_2) \geq \ldots \geq w(f_k)$. Thus, we have

$$w(e_1) + \cdots + w(e_k) < w(f_1) + \cdots + w(f_k).$$

Choose the index i as small as possible subject to the condition

$$w(e_1) + \cdots + w(e_i) < w(f_1) + \cdots + w(f_i).$$

Then

$$w(e_1) + \cdots + w(e_{i-1}) \geq w(f_1) + \cdots + w(f_{i-1}),$$

and so

$$w(f_1) \geq \ldots \geq w(f_i) > w(e_i).$$

(Note that $i > 1$, since e_1 is the element of largest weight which can occur in a basis.)

Now $\{f_1, \ldots, f_i\}$ is an independent set with cardinality larger than that of $\{e_1, \ldots, e_{i-1}\}$; so, for some j with $1 \leq j \leq i$, the set $\{e_1, \ldots, e_{i-1}, f_j\}$ must be independent. But then the greedy algorithm should have chosen f_j rather than e_i at the ith stage, since $w(f_j) > w(e_i)$.

To show the reverse implication, we are given a family $\mathcal{B}$ which is not the set of bases of a matroid, and we must show how to choose a weight function which defeats the greedy algorithm. The statement that $\mathcal{B}$ is not a matroid means that there exist $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$ such that, for no $y \in B_2 \setminus B_1$ is it true that $B_1 \setminus \{x\} \cup \{y\}$ is a basis. Let $l = |B_1 \setminus B_2| = |B_2 \setminus B_1|$, and choose a number a satisfying $1 - (1/l) < a < 1$. Now define the weight function w as follows:

$$w(e) = \begin{cases} 1 & \text{if } x \in B_1 \setminus \{x\}; \\ a & \text{if } x \in B_2 \setminus B_1; \\ 0 & \text{otherwise.} \end{cases}$$

Now the greedy algorithm first chooses all the points of $B_1 \setminus \{x\}$. Then by assumption it cannot choose any point of $B_2 \setminus B_1$; so the last point chosen (which may be x) has weight zero, and the weight of the chosen set is $k - 1$. On the other hand, the set B_2 has weight

$$(k - l) + la > (k - l) + l(1 - (1/l)) = k - 1.$$

In the case of a graphic matroid, this result says that, if weights are assigned to the edges of the complete graph, then the greedy algorithm (in the form, ‘add the edge of largest weight subject to creating no cycle’ at each stage) is guaranteed to find a spanning tree of maximum weight. This result is usually stated in the form obtained by reversing the inequalities, (replacing weight $w(e)$ by $W-w(e)$ for all edges e, where W is greater than the greatest weight). In this form the problem is known as the *minimal spanning tree* or *minimal connector* problem.

Here is another characterisation of matroids, whose statement and proof look somewhat like those of the above result about the greedy algorithm.

Suppose that the set X is totally ordered. Now any k-subset of X can be written in non-increasing order: we write such a set as $\{e_1,\ldots,e_k\}_\geq$ to indicate that $e_1 \geq \ldots \geq e_k$. We say that the k-set $\{e_1,\ldots,e_k\}_\geq$ *dominates* $\{f_1,\ldots,f_k\}_\geq$ if $e_i \geq f_i$ for $i = 1,\ldots,k$.

Theorem 3.2 *The non-empty family $\mathcal{B}$ of k-subsets of X is the family of bases of a matroid if and only if, for any ordering of X, there is a member of $\mathcal{B}$ which dominates all others.*

Proof Suppose first that $\mathcal{B}$ is a matroid. Let X be ordered in any manner, say $X = \{x_1,\ldots,x_n\}_\geq$. Choose a weight function w which is an order-preserving map from X into the non-negative real numbers. Let B be the basis of greatest weight. We claim that B dominates all bases.

Let $B = \{e_1,\ldots,e_k\}_\geq$, and suppose for a contradiction that there is a base $B' = \{f_1,\ldots,f_k\}_\geq$ which is not dominated by B. Then $f_i > e_i$ for some i. Choose i as small as possible subject to this. Then

$$f_1 \geq \ldots \geq f_i > e_i.$$

We know that B is chosen by the Greedy Algorithm, which does not choose any of $f_1,\ldots,f_i$ at stage i, even though they all have greater weight than e_i. So $\{e_1,\ldots,e_{i-1},f_j\}$ is dependent for all $j \leq i$. Now we have the same contradiction as in the earlier argument: since $\{f_1,\ldots,f_i\}$ is an independent set with larger cardinality than $\{e_1,\ldots,e_{i-1}\}$, it must contain an element f_j such that $\{e_1,\ldots,e_{i-1},f_j\}$ is independent.

Conversely, suppose that $\mathcal{B}$ has the ordering property. We must prove the exchange axiom. Let $B_1,B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$. If $|B_1 \setminus B_2| = 1$, say $B_2 \setminus B_1 = \{y\}$, then $B_1 \setminus \{x\} \cup \{y\} = B_2$, and there is nothing to prove. So suppose that $|B_1 \setminus B_2| > 1$. Now order the points of X as follows:

- the greatest elements are those of $B_1 \cap B_2$ (in any order);
- then the points of $B_1 \setminus B_2$ other than x;
- then the points of $B_2 \setminus B_1$;
- next comes x;
- then the remaining points of X.

Now neither of B_1 and B_2 dominates the other, so there must be a set in $\mathcal{B}$ which dominates both. But the only sets dominating B_1 are those in which x is replaced by an element of $B_2 \setminus B_1$. So the exchange axiom holds.

Remark This theorem gives us more insight into what a matroid looks like. For example, the dominance order on 2-subsets of a 4-set is shown in Figure 1. We see that the only families of 2-sets of $\{1,2,3,4\}$ which are not matroids consist of $\{1,4\}$ and $\{2,3\}$ together with any subset of $\{\{1,2\},\{1,3\}\}$, or any permutation of one of these.

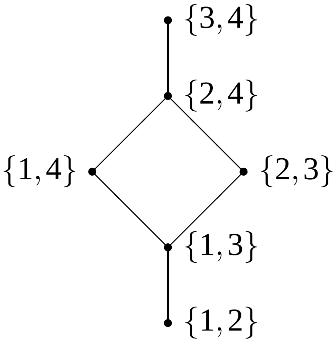

Figure 1: Dominance order

Remark The dominance condition looks very similar to our characterisation of matroid cycles in Theorem 2.4. Indeed, as Carrie Rutherford pointed out to me, the cycle property is a simple consequence. For take any ordering of the elements of the matroid, and let B be the unique base which dominates all others. Let e be the largest element which is not in B. (If no such e exists, there are no cycles.)

If B' is the set of elements greated than e, then $B' \cup \{e\}$ is dependent (else it is contained in a base not dominated by B), and so it contains a cycle includeing e. This is the unique cycle whose minimal element is greatest. This is just the dual of the property in Theorem 2.4.

Remark The second characterisation has led to a subtle but far-reaching generalisation of matroids by Borovik, Gel'fand, White and others, to the so-called *Coxeter matroids*. We do not discuss this here. See [1], for example.

4 The dual matroid

Let $M = (E, I)$ be a matroid, and let $\mathcal{B}$ be its set of bases.

The *dual matroid* M^* is the matroid on the set E whose bases are precisely the complements of the bases of M. (Thus a set is independent in M^* if and only if it is disjoint from some basis of M.) Checking that it is a matroid requires a little care.

The set of all complements of bases of a matroid M satisfies (MB): Lemma 2.2 is exactly what is needed to show this. For let $B_1^* = E \setminus B_1$ and $B_2^* = E \setminus B_2$, where B_1 and B_2 are bases of M. If $x \in B_1^* \setminus B_2^*$, then $x \in B_2 \setminus B_1$; so there exists $y \in B_1 \setminus B_2$ such that $B_1 \setminus \{y\} \cup \{x\}$ is a basis; its complement is $B_1^* \setminus \{x\} \cup \{y\}$.

For what comes later, we need to prove a technical result about the rank function of the dual of a matroid.

Lemma 4.1 *Let M^* be the dual of the matroid M on E, and let A be a subset of E and $A^* = E \setminus A$. If ρ and ρ^* are the rank functions of M and M^* respectively, we have*

$$|A^*| - \rho^*(A^*) = \rho(E) - \rho(A) \quad \textit{and} \quad \rho^*(E^*) - \rho^*(A^*) = |A| - \rho(A).$$

Proof Let I be a maximal independent subset of A (in M). Extend I to a basis $I \cup J$ of M, so that $J \subseteq A^*$. If $K = A^* \setminus J$, then K is an independent subset of A^* (in M^*), since it is contained in the basis $E \setminus (I \cup J)$. Hence

$$\rho^*(A^*) \geq |K| = |A^*| - |J| = |A^*| - \rho(E) + \rho(A).$$

Dualising the argument gives

$$\rho(A) \geq |A| - \rho^*(E) + \rho^*(A^*).$$

But we have

$$|A| + |A^*| = |E| = \rho(E) + \rho^*(E),$$

so the two inequalities are equalities, and the equations of the lemma follow.

A cycle in a matroid M is a set minimal with respect to being contained in no basis. Thus, a cycle in the dual M^* is a set minimal with respect to being disjoint from no basis of M, that is, meeting every basis.

What does the dual of the cycle matroid of a graph G look like? Its cycles are easily described. Assuming that G is connected, a cycle of M^* is a set of edges minimal with respect to meeting every spanning tree of G, that is, a set minimal with respect to the property that its removal disconnects G. Such a set is a *cutset* of G; so the dual of the cycle matroid of G is called the *cutset matroid* of G.

What about the dual of a vector matroid? Suppose that the vectors representing M are the columns of an $m \times n$ matrix A. We may suppose that these vectors span F^m; in other words, A has rank m, and is the matrix of a linear transformation T from F^n onto F^m. Let U be the kernel of T, and B the matrix of a linear embedding of U into F^n. (Thus B is an $n \times (n-m)$ matrix whose columns form a basis for U; the matrix B has rank $n-m$, and we have $B^\top A = 0$. Consider the $(n-m) \times n$ matrix $B^\top$. The columns of $B^\top$ are indexed by the same set as the columns of A, and we claim that $B^\top$ represents the dual matroid M^*.

To see this, take a set of m columns which form a basis for the space F^m. For convenience of notation, we suppose that they are the first m columns. Then we can apply elementary row operations to A (these do not affect the linear independence or dependence of sets of columns, and so don't change the matroid represented by A) so that the first m columns form an $m \times m$ identity matrix I. Thus, A has the form $[I\ X]$, where X is $m \times (n-m)$.

Consider the matrix $B = [-X\ I]^\top$, of size $n \times (n-m)$. Clearly B has rank $n-m$. Also, $B^\top A = O$, so B the columns of B lie in the null space of A; considering dimensions, we see that the columns of B form a basis for the null space of A. Also, it is clear that the last $n-m$ columns form a basis for the matroid represented by $B^\top$.

We have shown that the complement of any basis of M is a basis in the matrix represented by $B^\top$. Reversing the argument shows the converse implication, So $B^\top$ represents the dual matroid M^*.

5 Restriction and contraction

A *loop* is an element e of a matroid such that $\{e\}$ is not independent. Equivalently, e which lies in no independent set, or in no maximal independent set. The terminology arises from the cycle matroid of a graph, where loops are just loops in the graph-theoretic sense. In a vector matroid, the index i is a loop if and only if the ith vector (or column of the matrix) is zero.

If e is not a loop, we define the *contraction* M/e as follows: the elements are those of $E \setminus \{e\}$, and a set I is independent in M/e if and only if $I \cup \{e\}$ is independent in M. The name arises from the interpretation in cycle matroids: if M is the cycle matroid of G, then M/e is the cycle matroid of the graph G/e obtained by *contracting* the edge e (that is, removing it and identifying the two distinct vertices which were its ends).

If e is a non-loop in a vector matroid (corresponding to a non-zero vector v), then M/e is a vector matroid obtained by projecting the other vectors onto the factor space $V/\langle v\rangle$. In matrix terms, assuming that e is the first coordinate, apply elementary row operations to convert the first column to $(1\ 0\ \ldots 0)^\top$, and then delete the first row and column to obtain a matrix representing M/e.

These concepts dualise. An element e is a *coloop* if it is contained in every basis of M. A coloop in a connected graph is an edge whose removal disconnects the graph. (Such an edge is commonly called a *bridge* or *isthmus*.)

If e is not a coloop, we define the *restriction* $M\backslash e$ to have element set $E \setminus \{e\}$, a set being independent in $M\backslash e$ if and only if it is independent in M. In the cycle matroid of G, this operation simply corresponds to deleting the edge e; in a vector matroid, to deleting the corresponding vector or column.

Proposition 5.1 *(a) e is a loop in M if and only if e is a coloop in M^*, and* vice versa.

(b) If e is not a loop in M, then $(M/e)^* = M^*\backslash e$.

(c) If e is not a coloop in M, then $(M\backslash e)^* = M^*/e$.

Proof We see that e lies in every basis of M (that is, e is a coloop in M) if and only if it lies in no basis of M^* (that is, e is a loop in M^*), and dually.

Suppose that e is a non-loop in M. The bases of M/e are the bases of M containing e, with e removed. Their complements (in $E \setminus \{e\}$) are the bases of M^* not containing e, that is, the bases of $M^*\backslash e$. So $(M/e)^* = M^*\backslash e$. The other statement is proved dually.

6 The Tutte polynomial

The Tutte polynomial of a matroid can be regarded as a generalisation of the chromatic polynomial of a graph. We sketch this in order to see the issues involved in its definition.

Let G be a graph. A *vertex-colouring* of G is a map f from the vertex set of G to a set C of colours with the property that, if v and w are joined, then $f(v) \neq f(w)$. Let $P(g;\lambda)$ denote the number of vertex-colourings of G using a set of λ colours. It is clear that $P(G;\lambda)$ does not depend on the set of colours. What is less clear is that it is the evaluation at λ of a polynomial with integer coefficients. To see this, we observe:

- If G has n vertices and no edges, then $P(G;\lambda) = \lambda^n$.
- If G contains a loop, then $P(G;\lambda) = 0$.
- If e is an edge which is not a loop, then

  $$P(G;\lambda) = P(G\backslash e;\lambda) - P(G/e;\lambda),$$

  where $G\backslash e$ and G/e are the graphs obtained from G by deleting and contracting e, respectively.

The first and second assertions are clear. For the third, we consider all colourings of $G\backslash e$, where $e = \{x,y\}$, and observe that it can be partitioned into two subsets: colourings f with $f(x) = f(y)$ (counted by $P(G/e;\lambda)$), and those with $f(x) \neq f(y)$ (counted by $P(G;\lambda)$).

Now the fact that $P(G;\lambda)$ is polynomial in λ follows by an easy induction on the number of edges.

The point here is that the three conditions above enable us to calculate $P(G;\lambda)$, by applying a sequence of edge deletions and contractions; but they give no guarantee that a different sequence of deletions and contractions will lead to the same value. The guarantee comes from the fact that $P(G;\lambda)$ counts something, independently of the recurrence.

Similar considerations apply to the Tutte polynomial. Its most important properties are those which allow us to calculate it by means of a recurrence similar to that for $P(G;\lambda)$. But we must adopt a different definition in order to show that it is well-defined. In what follows, as in most enumeration theory, we adopt the conventions that $u^0 = 1$ for any u (including $u = 0$), and $0^n = 0$ for any positive integer n.

Let $M = (E, I)$ be a matroid, with rank function ρ. The *Tutte polynomial* $T(G;x,y)$ is the polynomial in x and y (with integer coefficients) given by

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

Proposition 6.1 *(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 $T(M;x,y) = T(M\backslash e;x,y) + T(M/e;x,y)$.

Proof (a) is trivial; the other parts are proved by careful analysis of the definition. All the arguments are similar and similarly tedious. We prove (b) here and leave the rest as an exercise.

Suppose that e is a loop, Every subset A of $E \setminus \{e\}$ corresponds to a pair of subsets $A, A \cup \{e\}$ of E. So each term in the sum for $T(M\backslash e)$ gives rise to two terms in the sum for $T(M)$. Let ρ' denote the rank function of $M\backslash e$. Then the following hold:

- $|(E \setminus \{e\}| = |E| - 1$;
- $\rho'(E \setminus \{e\}) = \rho(E)$;
- $|A \cup \{e\}| = |A| + 1$;
- $\rho(A) = \rho(A \cup \{e\}) = \rho'(A)$.

Let t be the term in $T(M\backslash e)$ corresponding to the set A. Then the term in $T(M)$ corresponding to A is t, while the term corresponding to $A \cup \{e\}$ is $(y-1)t$, giving a contribution of yt to $T(M)$. So $T(M) = yT(M\backslash e)$.

As an application, we show that the chromatic polynomial of a graph is, up to normalisation, a specialisation of the Tutte polynomial.

Proposition 6.2 *For any graph G,*

$$P(G;\lambda) = (-1)^{\rho(G)}\lambda^{\kappa(G)}T(G;1-\lambda,0),$$

where $\kappa(G)$ is the number of connected components of G and $\rho(G) + \kappa(G)$ the number of vertices.

Proof Let $f(G;\lambda)$ denote the expression on the right-hand side in the theorem. We verify that it satisfies the same recurrence relation and initial conditions as the chromatic polynomial. If G has n vertices and no edges, then $\kappa(G)=n$, $\rho(G)=0$, and $T(G;x,y)=1$, so the initialisation is correct. If G has a loop, then $f(G;\lambda)=0$ by (b), which is also correct. If e is neither a loop nor a coloop, then contracting e reduces ρ by one without changing κ, while deleting e changes neither ρ nor κ, so the inductive condition holds.

The most interesting case is that where e is a coloop or bridge, so that $G\backslash e$ has one more component than G. Let $e=\{x,y\}$. Then a fraction $1/\lambda$ of the colourings of $G\backslash e$ put any given colour on x, and the same proportion on y; these events are independent, since x and y lie in different components of this graph. Thus, a proportion of $1/\lambda$ of the colourings give x and y the same colour (and induce colourings of G/e), while the remaining proportion $(\lambda-1)/\lambda$ give x and y different colours (and so give colourings of G). Thus, $P(G;\lambda)=(\lambda-1)P(G/e;\lambda)$. This agrees with the recurrence for f in this case, since contracting e reduces ρ by one without changing κ.

Many other graph invariants related to trees and forests, flows, percolation, reliability, and knot polynomials, are evaluations or specialisations of the Tutte polynomial. Two of these are obvious from the definition:

Proposition 6.3 *(a) $T(M;1,1)$ is the number of bases of M;*

(b) $T(M;2,1)$ is the number of independent sets in M.

Proof The only terms contributing to $T(M;1,1)$ are those with $|A|=\rho(A)=\rho(E)$, that is, bases of M. Similarly, the only terms contributing to $T(M;2,1)$ are those with $|A|=\rho(A)$, that is, independent sets.

A useful tool for identifying specialisations of the Tutte polynomial is obtained by considering a more general form of the Tutte polynomial. We could ask whether there exists a polynomial $\tilde{T}(M;x,y,u,v)$ satisfying the recurrence relation

(a) $\tilde{T}(\emptyset;x,y,u,v)=1$.

(b) If e is a loop, then $\tilde{T}(M;x,y,u,v)=y\tilde{T}(M\backslash e;x,y,u,v)$.

(c) If e is a coloop, then $\tilde{T}(M;x,y,u,v)=x\tilde{T}(M/e;x,y,u,v)$.

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

$$\tilde{T}(M;x,y,u,v)=u\tilde{T}(M\backslash e;x,y,u,v)+v\tilde{T}(M/e;x,y,u,v).$$

As before, it is clear that there is at most one solution to this recurrence. In fact there is one, which can be obtained from the usual Tutte polynomial by a simple renormalisation:

Proposition 6.4 *The unique solution to the above recurrence is given by*

$$\tilde{T}(M;x,y,u,v) = u^{|E|-\rho(E)} v^{\rho(E)} T\left(\frac{x}{v}, \frac{y}{u}\right).$$

Proof This is easily checked using the facts that

- if e is a non-loop, then the passage from M to M/e reduces both the number of elements and the rank by 1;
- if e is a non-coloop, then the passage from M to $M\backslash e$ reduces the number of elements by 1 but doesn't change the rank.

The Tutte polynomial of the dual matroid is obtained very simply:

Proposition 6.5 $T(M^*;x,y) = T(M;y,x)$.

Proof Lemma 4.1 shows that the contribution of a set A to $T(M;y,x)$ is identical to the contribution of the complementary set $A^* = E \setminus A$ to $T(M^*;x,y)$.

7 Codes

We have seen that an $m \times n$ matrix A over a field F gives rise to a vector matroid on the set $\{1,\ldots,n\}$. We may assume that the matrix has rank m (so that the vectors span the space V in which they live). We examine the effect of various operations on A.

- *Elementary row operations* have the effect of changing the basis in the space V without altering the vectors used for the representation. So the matroid is unchanged.
- *Column permutations* simply re-name the vectors, and so replace the matroid by an isomorphic one.

- *Multiplying columns by non-zero scalars* changes the vectors by scalar multiples; this does not affect whether a collection of vectors is linearly independent, so again the matroid is unchanged.

From the matrix A, we can also obtain an m-dimensional subspace of F^n, namely the row space of A. Such a subspace is called a *linear code,* or *code* for short. We do not here go into the applications of codes to information transmission (in the case where F is a finite field), though some of the most important concepts will be defined shortly (and there is further discussion in Section 9. A code, then, is not a subspace of an arbitrary vector space, but a subspace of F^n (that is, a subspace of a vector space with a prescribed basis).

How do the operations on A affect the code?

- *Elementary row operations* just change the basis for the code.
- *Column permutations, and multiplication of columns by scalars*, have the effect of changing the prescribed basis for F^n in a limited way: we can permute basis vectors or multiply them by non-zero scalars. As we will see, the important properties of the code are not changed. So we call two codes *equivalent* if they are related in this way.

These operations generate a certain equivalence relation on the set of all $m \times n$ matrices of rank m over F. We see that each equivalence class of matrices corresponds to a unique vector matroid (up to re-labelling and change of basis in the ambient space), and also to a unique code (up to a natural notion of equivalence). So vector matroids and linear codes (up to the appropriate equivalence) correspond bijectively.

Thus, it comes as no surprise that properties of the codes and matroids are very closely related.

We now define a few important concepts from coding theory. The motivation is that the field F is regarded as an alphabet, and elements (or words) in the code are used for sending messages over a noisy communication channel. We require that any two codewords differ in sufficiently many positions that even if a few errors occur, the correct codeword can be recovered (as the codeword which resembles the received word most closely). Since the number of positions in which v and w differ is equal to the number of positions where $v-w$ has a non-zero entry, we are led to the following definitions.

A *word* of length n over F is an element of F^n. The *weight* $\mathrm{wt}(c)$ of a word c is the number of coordinates in which c has non-zero entries. An important parameter of a code C is its *minimum weight*, the smallest weight of a non-zero word in C.

The *weight enumerator* of a code C of length n is the 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 words of weight i in C. It is really a polynomial in one variable, since we lose no information by putting $x = 1$; the form given is homogeneous (every term has degree n).

We now come to the theorem of Curtis Greene [3] asserting that the weight enumerator of a code is a specialisation of the Tutte polynomial of the corresponding matroid.

Theorem 7.1 *Let C be a code over a field with q elements, and M the corresponding vector matroid. Then*

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

Proof This result is an application of Proposition 6.4. We have to describe the codes C' and C'' corresponding to deletion and contraction of the ith coordinate in the matroid, and verify the following.

(a) $W_C(x,y) = 1$, if C is the 'empty code'.

(b) If the ith coordinate is a loop, then $W_C(x,y) = xW_{C'}(x,y)$.

(c) If the ith coordinate is a coloop, then $W_C(x,y) = (x+(q-1)y)W_{C''}(x,y)$.

(d) If the ith coordinate is neither a loop nor a coloop, then $W_C(x,y) = yW_{C'}(x,y) + (x-y)W_{C''}(x,y)$.

Then Proposition 6.4 shows that

$$\begin{aligned} W_C(x,y) &= \tilde{T}(M; x+(q-1)y, x, y, x-y) \\ &= y^{n-\dim(C)}(x-y)^{\dim(C)} T\left(M; \frac{x+(q-1)y}{x-y}, \frac{x}{y}\right) \end{aligned}$$

as required.

Clearly, the ith coordinate of C is a loop in M if and only if the ith column of the matrix A is zero (that is, every codeword has 0 in the ith position). Dually, the ith coordinate is a coloop if and only if, applying elementary row operations so that the ith column of A is $(1\ 0\ \ldots\ 0)^\top$, all other entries in the first row of A are zero. Put another way, this means that C is the direct sum of the code F^1 and a code of length $n-1$.

If the ith coordinate is not a coloop, we define the *punctured code* C' to be the code obtained from C by deleting the ith coordinate from every codeword in C. If the ith coordinate is not a loop, we define the *shortened code* C'' to be obtained as follows: take all codewords which have entry 0 in the ith coordinate (these will form a subcode of codimension 1 in C) and then delete the ith coordinate. It is easily checked that the punctured and shortened codes correspond to the restriction M/i and contraction $M\backslash i$ respectively.

Now we check the recurrence relations. Part (a) is trivial. Consider (b). If the ith coordinate is a loop, then every codeword c has zero there, and the contribution of c to $W_C(x,y)$ is just x times its contribution to $W_{C'}(x,y)$. So (b) holds.

Suppose that the ith coordinate is a coloop. Then each codeword c of C'' corresponds to q codewords of C, obtained by putting each possible symbol of the alphabet in the ith coordinate. Of these, one (obtained by writing in 0) has the same weight as c, and the remaining $q-1$ have weight one greater. So (c) holds.

Finally, suppose that the ith coordinate is neither a loop nor a coloop. Write $W_C = W_C^{(1)} + W_C^{(2)}$, where $W_C^{(1)}$ is the sum of terms $x^{n-\mathrm{wt}(c)}y^{\mathrm{wt}(c)}$ corresponding to words c having zero in the ith coordinate, and $A_C^{(2)}$ to words having non-zero entry in the ith coordinate. Then by definition

$$W_{C''} = W_C^{(1)}/x,$$

and

$$W_{C'} = W_C^{(1)}/x + W_C^{(2)}/y,$$

from which we deduce that

$$W_C = W_C^{(1)} + W_C^{(2)} = yW_{C'} + (x-y)W_{C''},$$

as required for (d).

Note that, if $X = (x+(q-1)y)/(x-y)$ and $Y = x/y$, then

$$(X-1)(Y-1) = q.$$

So the weight enumerator is an evaluation of the Tutte polynomial along a particular hyperbola in the ‘Tutte plane’.

From this result, we can deduce the MacWilliams relation which shows that the weight enumerator of the dual code $C^\perp$ can be calculated from that of C.

Theorem 7.2

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

Proof Since $C^\perp$ has dimension $n - \dim(C)$ and corresponds to the dual matroid M^*, we have

$$W_{C^\perp}(x,y) = y^{\dim(C)}(x-y)^{n-\dim(C)} T\left(M; \frac{x}{y}, \frac{x+(q-1)y}{x-y}\right).$$

On the other hand, we have

$$\begin{aligned} \frac{1}{|C|} W_C(x+(q-1)y, x-y) &= q^{-\dim(C)}(x-y)^{n-\dim(C)}(qy)^{\dim(C)} \times \\ &\qquad \times T\left(M; \frac{qx}{qy}, \frac{x+(q-1)y}{x-y}\right). \end{aligned}$$

The two expressions are equal.

8 Tutte polynomial and bases

The Tutte polynomial $T(M;x,y)$ of a matroid M has the property that $T(M;1,1)$ is the number of bases of the matroid. (This is clear from the formula for T as a sum over subsets. When we substitute $x = y = 1$, all those terms which have a factor $(x-1)$ or $(y-1)$ vanish, and we are left only with subsets A such that $|A| = \rho(A) = \rho(E)$, that is, bases.) This means that the sum of all the coefficients in the Tutte polynomial is equal to the number of bases.

Crapo [2], who first extended Tutte's definition from graphs to matroids, observed that the Tutte polynomial has an alternative definition as a sum over bases. The definition is somewhat complicated, however, depending on a total ordering of E. Let B be any base of M. For each $y \notin B$, there is a unique cycle containing y and contained in $\{y\} \cup B$, called the *fundamental cycle* of y (with respect to the base B). To show this, note that $B \cup \{y\}$ contains a cycle (since it is not independent), whereas B contains no cycle; so there is at least one cycle in $B \cup \{y\}$ containing y. If there were more than one, say C_1 and C_2, then (MC2) would give the existence of a cycle contained in $C_1 \cup C_2$ not containing y, hence contained in B, a contradiction.

Dually, for all $x \in B$, there is a unique cocycle (that is, cycle of the dual matroid) containing x and contained in $\{x\} \cup (E \setminus B)$, called the *fundamental cocycle* of x (with respect to B); it is just the fundamental cycle of x with respect to the base $E \setminus B$ of the dual matroid.

For example, if the matroid M is graphic and comes from a connected graph G, then a base B is the edge set of a spanning tree of G. The fundamental cycle containing an edge $y \notin B$ is the unique cycle in the graph with edge set $B \cup \{y\}$. Dually, if $x \in B$, then removal of x disconnects the spanning tree B into two components; the fundamental cocycle consists of all edges of G which have one end in each component.

Now suppose that the ground set E is totally ordered, and let B be any base. We say that $x \in B$ is *internally active* if it is the greatest element in its fundamental cocycle; and $y \notin B$ is *externally active* if it is the greatest element in its fundamental cycle. The *internal activity* of B is the number of internally active elements, and the *external activity* is the number of externally active elements. Now Crapo showed:

Theorem 8.1 *The coefficient of $x^i y^j$ in $T(M;x,y)$ is equal to the number of bases of M with internal activity i and external activity j.*

A remarkable feature of this theorem is that the number of bases with given internal and external activity is independent of the ordering of the elements, although of course the internal and external activity of any given base will change.

We saw in Theorem 3.2 that, for any ordering of E, there is a unique base B which dominates all others, in the sense that for all $i \leq \rho(E)$, the ith greatest element of B is at least as large as the ith greatest element of any other base. We call it the *last base*. Dually, there is a *first base*, whose ith smallest element is at least as small as the ith smallest element of any other base. Now the internal and external activity of these bases can be calculated:

Proposition 8.2 *(a) The internal activity of the first base is the number of coloops of M, while its external activity is equal to $|E| - \rho(E)$.*

(b) The internal activity of the last base is $\rho(E)$, while its external activity is equal to the number of loops of M.

Proof (a) Let B be the first base and $y \notin B$. We show that y is the greatest element in its fundamental cycle C. Suppose not: that is, there exists $x \in B \cap C$ with $x > y$. We can assume that x is the greatest element in C. Let X consist of all elements of B smaller than x, together with y. Then X is independent, since it contains no cycle; so X is contained in a base B'. Now we have a contradiction, since the elements of B and B' less than y agree, but y is smaller than the corresponding element of B.

Dually, if $x \in B$, then x is the smallest element in its fundamental cocycle. This follows on dualising and reversing the order, when $E \setminus B$ is the new first base, since then x is the greatest element in its fundamental cycle with respect to $E \setminus B$ in the reversed order.

Now it is clear that, with respect to the first base B, every element outside B is externally active, while an element of B is internally active if and only if it is both smallest and largest in its fundamental cocycle, that is, its fundamental cocycle consists of a single element, that is, it is a coloop.

(b) Dual.

For a trivial example, the matroid on $\{1,2,3\}$ with two bases of size 2 has no loops and one coloop, so its Tutte polynomial is x^2+xy. This matroid is representable over $\mathrm{GF}(2)$, by the matrix $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$; Theorem 7.1 shows that the weight enumerator of the corresponding code is

$$y(x-y)^2\left[\left(\frac{x+y}{x-y}\right)^2+\left(\frac{x+y}{x-y}\right)\left(\frac{x}{y}\right)\right]=x^3+x^2y+xy^2+y^3.$$

In fact, we see directly that the code has one word of each possible weight $0,1,2,3$.

9 Trellis decoding

We discuss trellis decoding here for two reasons. First, it provides a general method of decoding, which has some advantages over conventional methods such as syndrome decoding. Second, it poses some questions which have a tantalising similarity to aspects of the Tutte polynomial, which we don't yet understand.

Conventional coding works as follows. Let C be a linear code of length n and dimension k over a field F. In order to transmit information (which we suppose is presented in 'blocks' or k-tuples of elements of F), we first encode it by a one-to-one linear transformation from F^k to the subspace C of F^n. The information will be transmitted more slowly, since it will take n units of time to send a block, rather than k if we sent the information unencoded. (We say that the code has *rate* k/n.) We employ this redundancy for error correction.

Classically, we assume that the received information is an n-tuple of elements of F (but not necessarily a codeword, since errors may have occurred). Assuming that only a small number of errors are likely, the received word will hopefully be nearer to the transmitted codeword than to any other codeword. (Precisely, this is the case if at most $\lfloor (d-1)/2 \rfloor$ symbols are received incorrectly, where d is the minimum distance of the code.) So we search through the codewords and select the one nearest to the received word (in terms of Hamming distance). This strategy is *nearest-neighbour decoding*.

For example, suppose that $F = \mathrm{GF}(2)$, and let C be the *repetition code* of length 3, consisting of the two codewords 000 and 111. Assuming that at most one bit is altered during transmission, we may conclude that if a word with more zeros than ones is received, then 000 was sent, while if the received word has more ones than zeros, then 111 was transmitted.

In practice, however, what is received is an electrical voltage which varies continuously, and is sampled at appropriate time intervals to determine the symbols of the received word. The simplest strategy is to round each voltage level to the nearest value which corresponds to a symbol in F. For example, suppose that the symbols 0 and 1 are represented by voltages 0 and 1 respectively. Using the above repetition code, suppose that we received the voltages 0.4, 0.4. 1.4. If we round and then decode, we obtain 000. But it appears that 111 might be a better choice. Indeed, the Euclidean distance from the received vector to $(0,0,0)$ is

$$\sqrt{0.4^2 + 0.4^2 + 1.4^2} = 1.51,$$

whereas the Euclidean distance to $(1,1,1)$ is

$$\sqrt{0.6^2 + 0.6^2 + 0.4^2} = 0.94.$$

(The choice of Euclidean distance is not arbitrary. Under certain technical assumptions on the errors, namely that they are independent Gaussian random variables with mean zero and constant variance, minimum Euclidean distance corresponds to maximum likelihood.)

Trellis decoding is a method of decoding which finds the codeword at minimum Euclidean distance from the received word directly, avoiding the errors caused by rounding as above.

A *trellis* for a code C of length n is a graph with the following properties:

- The vertices lie in $n+1$ disjoint *layers* $L_0,\dots,L_n$, where L_0 and L_n each contain just one vertex (the *source* s and *target* t respectively).
- The edges are directed, and each edge goes from a vertex in layer L_i to one in layer L_{i+1}, for some i.
- Each edge has a *label*, which is an element of F.
- There is a bijection between the codewords of C and the paths from s to t, so that the n-tuple of edge labels on any path is equal to the corresponding codeword.

For example, Figure 2 is a trellis for the repetition code of length 3. We assume that edges are directed from left to right.

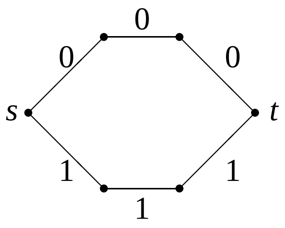

Figure 2: A trellis

Now suppose that $\alpha(c)$ is the voltage level corresponding to the symbol $c\in F$. Assume that $(x_1,\dots,x_n)$ is the 'received n-tuple' of voltage levels. An edge between levels L_{i-1} and L_i which carries the label c is assigned a *length* $(x_i-\alpha(c))^2$. Now the total length of a path from s to t with edge labels $(c_1,\dots,c_n)$ is

$$(x_1-\alpha(c_1))^2+\cdots+(x_n-\alpha(c_n))^2,$$

which is just the square of the Euclidean distance from $(x_1,\dots,x_n)$ to the point $(\alpha(c_1),\dots,\alpha(c_n))$ representing the codeword $(c_1,\dots,c_n)$. So nearest-neighbour decoding is achieved by finding the shortest path from s to t in the trellis. This can be done by standard algorithms such as Dijkstra's algorithm.

There is an added benefit. Dijkstra's algorithm works in two passes. First, the shortest distances from s to the vertices in L_i are computed by induction on i: if v_i is such a vertex, then

$$d(s,v_i)=\min\{d(s,v_{i-1})+l(v_{i-1},v_i),$$

where the minimum is over all vertices $v_{i-1} \in L_{i-1}$ for which (v_{i-1}, v_i) is an edge. This calculation can be done layer by layer as the components of $(x_1, \ldots, x_n)$ are received, since $l(v_{i-1}, v_i)$ depends only on x_i. When the entire word has been received, $d(s,t)$ is known, and the path realising this distance is found by a simple backtracking.

For example, consider the trellis for the repetition code shown above, with $\alpha(c) = c$ for $c \in \{0, 1\}$. When we receive the value 0.4, we assign $d(s, v) = 0.16, 0.36$ for the two nodes in L_1. When 0.4 is received again, we assign 0.32 and 0.72. Finally, when 1.4 is received, we assign $d(s,t) = \min\{2.28, 0.88\} = 0.88$. The backtracking in this case is trivial.

10 Minimal trellises

Any code C, not necessarily linear, can be represented by a trellis. We can simply take $|C|$ disjoint paths from s to t, one for each codeword, and label the edges on the path corresponding to the codeword c with the symbols of c in order.

However, it is clear from the description of trellis decoding in the last section that, the smaller the trellis, the more efficient the decoding algorithm will be. The size of the trellis can be measured in various ways (for example, number of vertices, number of edges, cycle rank); for simplicity we will use the number of vertices in this section.

For example, let C be the dual of the binary repetition code of length 3. This is a code with four codewords, so the simple construction above gives a trellis with 10 vertices and 12 edges. But there is a trellis with only 6 vertices and 8 edges for this code, as shown in Figure 3.

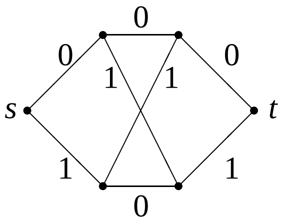

Figure 3: A minimal trellis

It is not hard to see that this is the smallest trellis which represents the code.

The following result of Muder [5] settles the question of existence of a 'best' trellis for a linear code in a strong way.

Theorem 10.1 *Let C be a linear code of length n. Then there is a trellis T for C, with layers $L_0,\ldots,L_n$, having the property that, if T' any other trellis for C, having layers $L'_0,\ldots,L'_n$, we have $|L_i| \le |L'_i|$ for $i = 1,\ldots,n$.*

We call L a *minimal trellis* for C. For the proof, see the next result, which also shows how the sizes of the layers in the minimal trellis are determined by the first and last base of the corresponding matroid.

Theorem 10.2 *Let C be a linear code over a field of order q. Let A and B be the first and last base of the corresponding matroid on the set $\{1,2,\ldots,n\}$. Let $a_i = |A\cap\{1,\ldots,i\}|$ and $b_i = |B\cap\{1,\ldots,i\}|$ for $i = 0,\ldots,n$. Then the cardinality of the ith layer of the minimal trellis for C is $q^{a_i-b_i}$, and the number of edges between the ith and $(i+1)$st layers is $q^{a_{i+1}-b_i}$.*

Proof We construct a trellis whose layers have the sizes claimed in the theorem. Then we show that it represents the code and is minimal.

Let P_i denote the subcode of C consisting of words which have entries 0 in positions $i+1,\ldots,n$, and let F_i denote the subcode consisting of words which have entries 0 in positions $1,\ldots,i$. (These are called the ith *past and future subcodes* of C.) We have $\dim(F_i) = k-a_i$ and $\dim(P_i) = b_i$, where $k = \dim(C)$. (To see the first equation, take a generator matrix for C in reduced echelon form. Then the first base consists of the coordinate positions where the leading ones occur. Also, a codeword c is zero in the first i positions if and only if the a_i rows with leading 1s in the first i positions do not occur in the expression for c as a linear combination of rows. The second equation is proved similarly by reversing the order.)

Now we construct the trellis as follows. By definition, $P_i\cap F_i = \{0\}$, so $\dim(P_i+F_i) = k-a_i+b_i$. We let L_i be the vector space $C/(P_i+F_i)$; then L_i has dimension a_i-b_i, and so has cardinality $q^{a_i-b_i}$ as claimed.

For each word $c\in C$, we associate the vertex of L_i which is the coset $(P_i+F_i)+c$. Join these vertices by a path from s to t, labelling the edges with the coordinates of c. We identify edges which have the same start and end vertices and the same label. This produces a trellis in which every codeword is represented by a path. We must show that every path arises in this way.

First, note that there is at most one edge with any given label entering or leaving any vertex of the trellis. For two edges with the same label leaving a vertex of L_i would arise from two codewords c, c' lying in the same coset of $P_i + F_i$ and having the same entry in position $i+1$. Write $c - c' = p + f$ with $p \in P_i$ and $f \in F_i$. Then p and $c - c'$ both have zero in the $i+1$ position, and hence so does f. Thus $f \in F_{i+1}$. Clearly $p \in P_{i+1}$ since $P_i \subseteq P_{i+1}$. So $c - c' \in P_{i+1} + F_{i+1}$, and the two edges have the same end, and are equal (by our convention).

Now we see that a vertex in layer L_i has q edges leaving it if $i+1 \in A$, and just one edge otherwise. So the number of paths in the trellis is equal to $q^{|A|} = |C|$; so every path corresponds to a codeword.

Finally we show that the trellis is minimal. Let T' be any trellis for C. We prove that two paths containing the same vertex in the ith layer L_i correspond to codewords in the same coset of $P_i + F_i$. So $|L_i'| \geq |C/(P_i + F_i)| = |L_i|$, and we are done.

So let $c = (c_1, \ldots, c_n)$ and $d = (d_1, \ldots, d_n)$ be two codewords represented by paths containing the same vertex of the ith layer. Then $e = (c_1, \ldots, c_i, d_{i+1}, \ldots, d_n) \in C$. So $e - d = (c_1 - d_1, \ldots, c_i - d_i, 0, \ldots, 0) \in C$ (as C is linear); so, in fact, $e - d \in P_i$. Similarly, $c - e \in F_i$, and so $c - d \in P_i + F_i$, as required.

Exercise Show that the minimal trellis for the code with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

has five vertices and six edges, whereas the minimal trellis for the equivalent code with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

has six vertices and eight edges.

As this exercise shows, equivalent codes can have different minimal trellises. We say that a trellis is a *minimal equivalent trellis* (or ME-trellis) for a code C if it is a minimal trellis for a code equivalent to C. Since the size of the minimal trellis depends on the ordering, it cannot be calculated from data about the matroid alone. However, it may be that some weighted average of the sizes of the ME-trellises for C can be derived from the matroid (perhaps even from the Tutte polynomial). This is unknown.

Another problem is to find the smallest ME-trellis for a code. Jain *et al.* [4] have shown that this problem is NP-hard for codes over large fields. Its status for binary codes seems to be unknown.

Example Consider the two generator matrices

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

for the dual Hamming code of length 7, differing by a transposition of the third and fourth columns. For the first matrix, the first and last bases are $\{1,2,4\}$ and $\{5,6,7\}$, giving a minimal trellis with 26 vertices and 32 edges. For the second matrix, the first and last bases are $\{1,2,3\}$ and $\{5,6,7\}$, giving a minimal trellis with 30 vertices and 36 edges.

Exercise A $k \times n$ matrix A is in *trellis-oriented form* or TOF if

(a) no row of A is zero;

(b) the first non-zero entries in the rows occur in different columns;

(c) the last non-zero entries in the rows occur in different columns.

Prove that any $k \times n$ matrix of rank k can be put into TOF by elementary row operations.

Note that the columns referred to in (b) and (c) comprise the first and last bases of the corresponding matroid respectively.

Find generator matrices in TOF corresponding to the two codes equivalent to the dual Hamming code of length 7 given above.

Exercise Show that the minimal trellises for a code and its dual have the same number of vertices in layer i for each i.

References

[1] A. V. Borovik and I. M. Gel'fand, WP-matroids and thin Schubert cells, *Advances Math.* **103** (1994), 162–179.

[2] H. Crapo, The Tutte polynomial, *Aequationes Math.* **3** (1969), 211–229.

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

[4] K. Jain, I. Măndoiu and V. Vazirani, The “art of trellis decoding” is computationally hard—for large fields, *IEEE Trans. Inform. Theory* **44** (1998), 1211–1214.

[5] D. J. Muder, Minimal trellises for block codes, *IEEE Trans. Inform. Theory* **34** (1988), 1049–1053.

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