A Polynomial Time Algorithm to Find the Minimal Cycle Basis of a Regular Matroid

Alexander Golynski and Joseph D. Horton
Faculty of Computer Science
University of New Brunswick
http://www.cs.unb.ca
email: jdh@unb.ca

July 31, 2001

1 Introduction

The Minimal Cycle Basis Problem (MCB) is the following. Given a binary matroid with nonnegative weights assigned to its elements, what is the set of cycles with total smallest weight which generate all of the circuits of the matroid? The answer to this problem also answers in some cases the Sparsest Null Space Basis Problem (NSP) [CP87]. Given a $t \times n$ matrix A with $t < n$ and rank r, find a matrix N with the fewest nonzeros whose columns span the null space of A. Coleman and Pothen find solutions to the latter problem useful in solving the very general Linear Equality Problem: minimize a nonlinear objective function $f(x)$ subject to a matrix equation $Ax = b$. Many optimization problems are of this form. They are especially concerned when the matrix A is large and sparse. The algorithm given in this paper solves the NSP for totally unimodular matrices, that is matrices in which every square submatrix of A has a determinant of +1, -1 or 0. A matroid is regular if and only if it is representable by the columns of a totally unimodular matrix.

Seymour [Sey80] proved that any regular matroid can be decomposed in polynomial time into 1-sums, 2-sums, and 3-sums of graphic matroids, cographic matroids and the special ten element matroid R_{10}. Truemper [Tru90] gives an algorithm which finds such a decomposition in cubic time. An algorithm to solve the MCB problem for graphs is given in [Hor87]. The Gomory-Hu tree of [GH61] solves the MCB problem for cographic matroids. The main technical result of this paper is to show how the minimal cycle

bases of a decomposition can be glued together to form a minimal cycle basis of the k-sum.

2 Background

The symmetric difference of two sets is denoted by $X+Y = (X \setminus Y) \cup (Y \setminus X)$.

2.1 Matroids

Definition 2.1 *A matroid $M = (S, \mathcal{I})$ is a finite set S and a collection $\mathcal{I}$ of subsets of S, the independent sets of M, such that:*

(I1) the empty set is independent;

(I2) subset of an independent set is independent;

(I3) if X and Y are independent subsets, such that $|X| = |Y| + 1$, then there are exists $e \in X \setminus Y$ such that $Y \cup \{e\}$ is also independent.

The set S is called the ground set of the matroid and denoted $\mathcal{E}(M)$. A *weighted* matroid $M = (S, \mathcal{I}, w)$ is a matroid $(S, \mathcal{I})$ together with a weight function $w \mapsto \Re^+ \cup \{0\}$

A set $X \subseteq E$ is said to be *dependent* if $X \notin \mathcal{I}$.

A set $B \subseteq E$ is said to be a *base* if B is a maximally independent set, that is B is independent, but every proper superset X of B is dependent.

A set C is said to be a *circuit* if it is minimally dependent, that is C is dependent but every its proper subset $X \subset C$ is independent. The set of circuits is denoted by $\mathcal{C}(M)$.

A set C is said to be a *cycle* if it is a combination of circuits with respect to the + operation. The set of cycles is called the cycle space and denoted $\mathcal{C}(M)$. The cycle space forms a commutative group with respect to the + operation.

The *rank* function $r : P(E) \mapsto$ N specifies the cardinality of a maximally independent subset of X.

$$r(X) = max\{|Y| : Y \subset X \text{ and } Y \in \mathcal{I}\}$$

The dual matroid of $M = (E, \mathcal{I})$ is the matroid $M^* = (E, \mathcal{I}^*)$, where set of independent sets is $\mathcal{I}^* = \{X : \exists B \text{ base of } M, \text{ such that } B \cap X = \emptyset\}$.

2.2 Representations of a matroid

A matroid does not have to be defined by specifying its independent sets. Instead one can specify any one of the following:

1. the dependent sets;
2. the bases;
3. the circuits;
4. the rank function;
5. the cycle space;
6. the dual matroid.

The dual matroid in turn can be specified in any of the other ways.

Many matroids can be represented as sets of vectors. A matroid is said to be *representable* over a field $\mathcal{F}$ if there is a mapping m of E into a finite dimensional vector space V over $\mathcal{F}$ such that $I \subset E$ is independent if and only if $m(I) \subset V$ is an independent set of vectors. Often the elements of the matroid are specified to be the column vectors of a matrix. Then the circuits correspond to a minimal set of columns which are dependent. There is some linear combination of these columns which is in the null space of the matrix.

A matroid which is representable over any field is said to be *regular*; a matroid representable over $\mathcal{GF}(2)$ is said to be *binary*. The symmetric difference operator $+$ on the subsets of E of a binary matroid corresponds to vector addition in the corresponding vector space $m(E)$. The cycle space $\mathcal{C}(M)$ is a subspace of this vector space. For the rest of this paper we are concerned only with binary matroids.

2.3 Graphic and cographic matroids

A matroid M is called *graphic* if there exists a graph $G = (V, E)$, where V is the vertex set and E is the edge set, such that $\mathcal{E}(M) = E$ and a set $I \subset E$ is independent iff I does not contain a circuit. We denote the graph by $G(M)$. A matroid M is called *cographic* if its dual is graphic. We denote the corresponding graph by $G^*(M)$.

A set C is a cocycle (cut) in a graph if and only if there is a 2-coloring of the vertex set V, A and $V \setminus A$, such that $C = C_A$, where

$$C_A = \{e = \{s, t\} | e \in E, s \in A \text{ and } t \in V \setminus A\}$$

A cocycle C is a cocircuit iff it is minimal with respect to set inclusion. Thus circuits of a cographic matroid M are cuts in the graph $G^*(M)$. The cycle space of a cographic matroid consists of the sets C_A for each $A \subseteq V$.

3 Minimal Cycle Bases

A cycle basis $\mathcal{B}$ of a binary matroid M is a subset of the cycle space of the matroid $\mathcal{C}(M)$, in which every cycle C of $\mathcal{C}(M)$ has a unique representation over $\mathcal{B}$, that is $C = C_1 + C_2 + \ldots + C_k$ where $C_1, C_2, \ldots, C_k \in \mathcal{B}$. The dimension of the cycle space of a binary matroid M is $m - r$, where m is the number of elements of the matroid and r is the rank of the matroid.

Let w be a nonnegative *weight function* defined on S, that is $w : S \mapsto \Re^+ \cup \{0\}$. Define the weight of a set $E \subseteq S$ to be $w(E) = \sum_{e \in E} w(e)$. The weight of a cycle basis is defined to be the sum of the weights of all cycles in the basis. A *minimal cycle basis* is a cycle basis which has the minimum weight among all cycle bases.

3.1 A characterization of cycles in the MCB

To simplify the presentations in this paper, we assume that every cycle has a different weight. One can always force this by perturbing the weights on the elements, at the cost of some time and space. Then there is a unique minimal cycle basis. It is possible instead to choose one cycle in preference to another if they are the same weight and are dependent on each other, but this becomes somewhat cumbersome. One good way to handle such ties is to use families of relevant cycles, as developed in [Vis97] for graphs. The following lemma characterizes cycles in a minimal cycle basis under this uniqueness assumption.

Lemma 3.1 *A cycle C is in a minimal cycle basis if and only if it satisfies the following property. Whenever $C = C_1 + C_2 + \ldots + C_k$ where the C_i differ from C, then there is an i such that $w(C) < w(C_i)$.*

Proof Assume that cycle C satisfies this property, and let $\mathcal{B}$ be a cycle basis not containing C. Then $C = C_1 + C_2 + \ldots + C_k$ where $C_1, C_2, \ldots, C_k \in \mathcal{B}$. By the above property, there is an i such that $w(C) < w(C_i)$. But then $\mathcal{B}' = \mathcal{B} \setminus \{C_i\} \cup \{C\}$ is a basis of weight less than $\mathcal{B}$. Hence a minimal basis must contain C.

Conversely, assume that C is a cycle in a minimal cycle basis $\mathcal{B}$. Suppose that $C = C_1 + C_2 + \ldots + C_k$. Each C_i can be expressed uniquely as the

sum of members of the cycle basis, some of which may not include C and at least one of which does include C. That is, there is a j such that C_j can be expressed as the sum of cycles in $\mathcal{B}$ including C. Then C_j can replace C in $\mathcal{B}$ and still form a cycle basis $\mathcal{B}' = \mathcal{B} \setminus \{C_j\} \cup \{C\}$. Because $\mathcal{B}$ is a minimal cycle basis, $w(\mathcal{B}) < w(\mathcal{B}')$. Hence $w(C) < w(C_j)$. ∎

In other words, a cycle is not in the minimum cycle basis if and only if it can be written as the sum of smaller cycles.

3.2 MCB in graphic matroids

The algorithm to find the minimal cycle basis for a weighted graph in [Hor87] is based on the following:

Lemma 3.2 *Let C be a cycle in a minimal cycle basis of a graph G, and let x be a vertex of C. Then there is an edge $e \in C$, say $e = \{u, v\}$, such that C consists of a shortest path from u to x and a shortest path from v to x and the edge e.*

Therefore the following finds the minimal cycle basis:

- Find the shortest path P_{uv} in G between each pair of verticies $\{u, v\}$.
- List all *candidate* circuits of the form

$$\mathcal{X} = \{P_{uw} + P_{vw} + \{u, v\} | u, v, w \in V, P_{uw} \cap P_{vw} = \{w\}\}$$

- Use a greedy algorithm to extract a minimal cycle basis from $\mathcal{X}$.

3.3 MCB in cographic matroids

To find the minimal cycle basis of a cographic matroid, one can use the Gomory-Hu algorithm from [GH61]. Given a weighted graph, they find a weighted tree on the same set of vertices for which the weights of the minimal cuts (cocycles in matroid terminology) between any pair of nodes is the same in both the tree and the graph. Each edge of this Gomory-Hu tree corresponds to the minimal cut in the graph separating its two endpoints. If any minimal cut separating two vertices v and u is written as the sum of other cuts, the sum must contain a cut which separates v and u. This cut cannot be smaller than the minimal one. Hence by Lemma 3.1 these minimal cuts must all be in the minimal cycle basis. The $n-1$ cuts corresponding to edges of the Gomory-Hu tree number exactly the dimension of the cocycle space and hence must form the minimal cycle basis.

3.4 Sums of binary matroids

The sum of two binary matroids $M_1 \oplus M_2$ is defined to be a matroid M on the ground set $S = S_1 + S_2$, where S_1 and S_2 are the ground sets of M_1 and M_2 respectively. The sum is given by its cycle space

$$\mathcal{C}(M) = \{C_1 + C_2 : C_1 \in \mathcal{C}(M_1), C_2 \in \mathcal{C}(M_2), C_1 + C_2 \subseteq S\}$$

The members of $Z = S_1 \cap S_2$ are called the *connecting* elements.

We are concerned about three special cases of this operation, namely:

1-sum or direct sum when $Z = \emptyset$;

2-sum when $Z = \{z\}$;

3-sum when $|Z| = 3$, Z is a *triangle* (circuit of three elements) of M_1 and M_2 and Z includes no cocircuit of either M_1 or M_2.

In these cases it is required that $|S_1|, |S_2| < |S|$.

A set A of M_1 or M_2 is called *good* with respect to the decomposition $M = M_1 \oplus M_2$ if $|A \cap Z| \leq 1$, otherwise A is called *bad*. Note that in the 1- and 2-sum cases, all sets are good. In the 3-sum case every cycle $A \in \mathcal{C}(M)$ is the sum of two good cycles. Suppose that $A = C + D$ where C is a cycle of M_1 and D is a cycle of M_2, and C and D are bad. Then $|C \cap Z| > 1$, so $|(C + Z) \cap Z| \leq 1$. Therefore $A = (C + Z) + (D + Z)$ where $C + Z$ and $D + Z$ are both good.

4 The Algorithm

The first phase of the algorithm is based on the decomposition theorem [Sey80] for regular matroids. A regular matroid M can be decomposed into 1-, 2- and 3-sums of graphic, cographic matroids and copies of the special matroid of ten elements R_{10}. The algorithm of [Tru90] finds such a decomposition in cubic time.

Given a decomposition $M = M_1 \oplus M_2$ and minimal cycle bases for M_1 and M_2, how can we construct a minimal cycle basis for M? In fact, before we can even find the minimal cycle bases for the M_i, appropriate weights have to be found for the connecting elements. So the remaining algorithm consists of three more phases: determine the weights of connecting elements; calculate the minimal cycle bases of the constituent graphic, cographic and R_{10} matroids; last, glue together the minimal cycle bases.

4.1 Connecting Weights

Let Z be the set of connecting elements for the sum $M = M_1 \oplus M_2$. Let C_z be the circuit of minimal weight in M_1 such that $Z \cap C_z = \{z\}$, and let $P_z = C_z \setminus \{z\}$. Call P_z the z-path in M_1. Similarly let D_z be a minimal weight circuit in M_2 containing z and no other element of Z, and call $Q_z = D_z \setminus \{z\}$ the z-path in M_2.

Assume that w is the weight function on M. Define weight functions w_i on M_i to be the same as w on the set $S_i \cap S$. Define the weight of a connecting element z from Z in M_1, $w_1(z)$, to be the weight of z-path Q_z in M_2. Similarly define the weight of a connecting element z from Z in M_2, $w_2(z)$, to be the weight of z-path P_z in M_1. These weights are the only information about each part of a sum embedded in the other part.

For any subset A of S_1 we define its *correspondent* $\bar{A}$, a subset of S, by replacing every connecting element z with the corresponding shortest path Q_z. In other words

$$\bar{A} = A + \sum_{z \in Z \cap A} D_z \tag{1}$$

We list some properties of this correspondence:

- Since D_z are fixed, $A \mapsto \bar{A}$ is a linear transformation, therefore

$$\text{If } C = C_1 + \ldots + C_k \text{ then } \bar{C} = \bar{C}_1 \ldots + \bar{C}_k$$

- $w_1(\bar{A}) \leq w(A)$, moreover if A is good then $w_1(\bar{A}) = w(A)$.
- If $C \in \mathcal{C}(M_1)$, then $\bar{C} \in \mathcal{C}(M)$.

Similarly for $B \subset S_2$, define its correspondent by $\bar{B} = B + \sum z \in Z \cap BC_z$.

Finding the connecting weights can be reduced to the following more general (M, T)-problem. Given a regular weighted matroid M defined on a ground set S with weight function w and a set $T \subset S$, for each $t \in T$, find a shortest circuit C_t including t in M which is otherwise disjoint from T. For our purposes it suffices to restrict the set T to being a single edge or a circuit of three elements.

In the base cases when the matroid is graphic, cographic or R_{10}, the (M, T)-problem can be solved. For the graphic case, delete the elements of T from the graph and solve the shortest path problem between the endpoints of the edge t. The path together with the edge of T is the answer. For the cographic case, contract the edges of T (except for t) and solve the min-cut

problem between the endpoints of t. All possible circuits can be considered for R_{10}.

Otherwise there is a decomposition $M = M_1 \oplus M_2$ and we can apply recursion. Let Z be the set of connecting elements. Weight the elements in M_1 and M_2, other than the elements of T and Z, the same as in M. If the sum is a 1-sum, $Z = \emptyset$, and then each circuit of M is either a circuit of M_1 or a circuit of M_2. The problem can be solved in either M_1 or M_2, depending upon which submatroid the elements of T are in.

The cases of a 2-sum or a 3-sum are considered together. Suppose that T is contained in either S_1 or S_2, say $T \subset S_1$. Then all the elements e of M_2 have defined weights $w_2(e) = w(e)$ other than those in Z. Let $w_2(z)$ be an arbitrarily large number for each element z in Z. We apply the algorithm to the (M_2, Z)-problem, find the circuits D_z, and let Q_z be the shortest z-paths obtained. Assign weights $w_1(z) = w_2(Q_z)$ for every $z \in Z$. Next invoke the algorithm for the (M_1, T)-problem for each element t to find the circuit C_t, the minimal circuit containing t but no other element of T. Each circuit C_t contains at most one element from Z.

If C_t contained two elements from Z, say z_1 and z_2, then we are dealing with a 3-sum, and $Z = \{z_1, z_2, z_3\}$ is a 3-element circuit. Then z_3 can replace z_1 and z_2 in P_t to make a lighter path thru t. Note that the triangle inequality $w_1(z_3) \leq w_1(z_1) + w_1(z_2)$ holds for the elements of Z, because $Q_1 + Q_2 + \{z_3\} = D_1 + D_2 + Z$ is a cycle in M_2 and so $w_2(Q_3) \leq w_2(Q_1) + w_2(Q_2)$. Thus the correspondent of C_t, $\bar{C}_t$ is the solution to the (M, T)-problem in the case when T is only on one side of the decomposition.

Now suppose that T intersects both ground sets. Without loss of generality, let $T \cap S_1 = \{r, s\}$ and $T \cap S_2 = \{t\}$. By the definition of the matroid sum, there exist two good cycles $C \in \mathcal{C}(M_1)$ and $D \in \mathcal{C}(M_2)$ such that $C + D = T$, and $C \cap Z = D \cap Z = \{z\}$. Then $D = \{t, z\}$, in other words z is parallel to t. The circuits thru t in M_2 are the same as the circuits thru z, with t replacing z. Hence z can act as a surrogate for t in M_2. As z is also in M_1, z can act as a surrogate for t in M_1 as well.

Delete t from M_2, removing all circuits in M_2 which include t, to form a new smaller matroid M_2'. Solve the (M_2', Z)-problem. Let D_z' be the minimal weight circuit containing z, and let $Q_z' = D_z' \setminus \{z\}$. If this is a 3-sum case, let the other elements of Z be x and y, and define Q_x' and Q_y' similarly. Weight the elements of Z in M_1 with the weight of these "paths" in M_2'. Next solve the $(M_1, \{z, r, s\})$-problem, finding minimal circuits C_z, C_r and C_s for z, r and s respectively.

The answer to the (M, T)-problem can now be found, but it is not quite as simple as the case when T is all on one side of the sum. There are two

possible answers for each element of T. The weight for both possibilities can be checked as the final step of this phase of the algorithm. The shortest circuit including t can be either $D'_z + \{z,t\}$ or the correspondent of $C_z + \{z,t\}$. The shortest circuit including r is either $\bar{C}_r$ or $C_s + \{r\} + Q'_z$. The shortest circuit including s is either $\bar{C}_s$ or $C_r + \{s\} + Q'_z$.

4.2 Gluing minimal cycle bases together

Finally we discuss how to glue cycle bases from the parts of a sum. The gluing algorithm is based on the observation that the set of correspondents for all cycles in $\mathcal{B}_1$ and $\mathcal{B}_2$ spans the cycle space of M. At the same time no other cycle of M can satisfy the property of Lemma 3.1. Thus the minimal cycle basis of M must be included in this set of cycles.

Theorem 4.1 *Let $M = M_1 \oplus M_2$, where M_1 and M_2 are binary matroids with ground sets S_1 and S_2 respectively, and $\oplus$ is a 1-, 2- or 3-sum. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be their minimal cycle bases respectively, with weights of the connecting elements as previously defined. Then the set*

$$\mathcal{B}_t = \{\bar{C} : C \in \mathcal{B}_1\} \cup \{\bar{D} : D \in \mathcal{B}_2\}$$

includes a minimal cycle basis for M.

Proof Let A be a cycle of M and not in $\mathcal{B}_t$. It is representable as a sum of two good cycles, say $A = C + D$, where C is a cycle of M_1 and D is a cycle of M_2. Two cases are possible.

Suppose A is contained in one of the ground sets S_i, say $A \subseteq S_1$. Then $D = \emptyset$ and let

$$C = C_1 + \ldots + C_k \tag{2}$$

be the representation of C over $\mathcal{B}_1$. Then by lemma 4.1

$$A = C = \bar{C} = \bar{C}_1 + \ldots + \bar{C}_k \tag{3}$$

is a representation of A over $\mathcal{B}_t$. Note that A is heavier than the heaviest cycle C_i in (3), since the property of lemma (3.1) holds for the heaviest $\bar{C}_i$. Hence A cannot be in the minimal cycle basis of M.

Otherwise $D \neq \emptyset$ and $C \cap D = \{z\}$ for some connecting element $z \in Z$. Then

$$A = (\bar{C} + C_z) + (\bar{D} + D_z) = \bar{C}_1 + \ldots + \bar{C}_k + \bar{D}_1 + \ldots + \bar{D}_l \tag{4}$$

for some C_i in $\mathcal{B}_i$ and D_j in $\mathcal{B}_2$. Thus A is the sum of elements of $\mathcal{B}_t$, so $\mathcal{B}_t$ spans the cycle space of M. Also A must be no lighter than C, since

$$w(A) = w(C \setminus \{z\}) + w_2(D \setminus \{z\}) \geq w_1(C \setminus \{z\}) + w_2(Q_z) = w_1(C) = w(\bar{C})$$

Similarly $w(A) \geq w_2(D)$. Also note that $w(C_z + D_z) = w_1(C_z) \leq w_1(C)$. Hence A is the sum of three cycles $\bar{C}$, $\bar{D}$ and $C_z + D_z$ which are lighter than itself. Thus A is not in the minimal cycle basis. ∎

The set of cycles $\mathcal{B}_t$ may not form a basis because there can be too many cycles in the set. The greedy algorithm can be used to obtain a basis from $\mathcal{B}_t$, since $\mathcal{C}(M)$ taken as the ground set constitutes a binary matroid itself with respect to cycle dependency. The same method as in [Hor87] can be used. Sort the cycles of $\mathcal{B}_t$ and represent them as columns of a matrix, the rows of which are indexed by the elements of M. Then use Gaussian elimination, processing columns from the lightest to the heaviest until we find $\dim(\mathcal{C}(M)) = |\mathcal{E}(M)| - r(M)$ independent cycles.

5 Complexity

Let m be the number of elements in a regular matroid M. Truemper finds a complete decomposition in $\Theta(m^3)$ time [Tru92], down to only graphic matroids, cographic matroids and copies of R_{10}.

Finding the weight of the connecting elements in the decomposition requires solving the (M,T)-problem in a 1-, 2-, or 3-sum. This requires at most $O(m)$ time to decide what subproblems have to be solved, and those subproblems need to be solved at most once on each side of the sum. The solution for the graphic and cographic cases requires solving a shortest path problem or a network flow problem respectively. In either case the problem is easier than solving the MCB problem itself for the component, which must be done in a later phase.

The Gomory-Hu tree for a graph can be constructed by solving $n-1$ network flow problems, n is the number of vertices in the graph. The network flow problem can be solved in $O(mn \log_{m/n \log n} n)$ [KRT94], so the MCB problem for cographic matroids can be solved in $O(mn^2 \log n)$ time. This is considerably faster than any known algorithm for graphic matroids.

Thus the slowest step in the algorithm is solving the MCB in the graphic case, for which the best published algorithm is $\Theta(m^3 n)$ in the worst case [Hor87]. The difficulty is extracting the independent set of shortest candidate cycles. In practise when implemented, the minimal cycle basis circuits

of a graph are usually found very quickly because they are usually all very short. But this is not guaranteed. Indeed it is possible for the largest circuit of $\mathcal{X}$ to be in the circuit basis.

The more general MCB problem for binary matroids is known to be NP-hard. Indeed just the problem of finding the shortest circuit in a binary matroid is NP-hard, and by Lemma 3.1, the shortest circuit must be in any minimal cycle basis.

References

[CP87] T. Coleman and A. Pothen. The null space problem I. Complexity. *Journal of Algebraic Discrete Meth*, 7:527–537, 1987.

[GH61] R. E. Gomory and T. C. Hu. Multi-terminal network flows. *Journal of the Society for Industrial and Applied Mathematics*, 9(4):551–570, 1961.

[Hor87] J. D. Horton. A polynomial-time algorithm to find the shortest cycle basis of a graph. *SIAM Journal on Computing*, 16(2):358–366, 1 1987.

[KRT94] King, Rao, and Tarjan. A faster deterministic maximum flow algorithm. *Journal of Algorithms*, 1994.

[Sey80] P. Seymour. Decomposition of regular matroids. *Journal of Combinatorial Theory (B)*, 28:305–359, 1980.

[Tru90] K. Truemper. A decomposition theory for matroids. V. Testing of matrix total unimodularity. *Journal of Combinatorial Theory (B)*, 49:241–281, 1990.

[Tru92] K. Truemper. *Matroid Decomposition.* Academic Press, Boston, 1992.

[Vis97] P. Vismara. Union of all minimum cycle bases of a graph. *Electronic Journal of Combinatorics*, 4(R9), 1997.