DIMACS Technical Report 2003-17
April 2003

On the Complexity of Some Enumeration Problems for Matroids*

by

Endre Boros† Khaled Elbassioni† Vladimir Gurvich†
Leonid Khachiyan‡

*This research was supported in part by the National Science Foundation Grant IIS-0118635. The research of the first and third authors was also supported in part by the Office of Naval Research Grant N00014-92-J-1375. The second and third authors are also grateful for the partial support by DIMACS, the National Science Foundation's Center for Discrete Mathematics and Theoretical Computer Science.

---

†RUTCOR, Rutgers University, 640 Bartholomew Road, Piscataway NJ 08854-8003; ({boros,elbassio,gurvich}@rutcor.rutgers.edu).
‡Department of Computer Science, Rutgers University, 110 Frelinghuysen Road, Piscataway NJ 08854-8003; (leonid@cs.rutgers.edu).

ABSTRACT

We present an incremental polynomial-time algorithm for enumerating all circuits of a matroid or, more generally, all minimal spanning sets for a flat. We also show the NP-hardness of several related enumeration problems.

1 Introduction

Let M be a matroid on ground set S of cardinality $|S| = n$. We assume throughout the paper that M is defined by an *independence oracle*, i.e. an algorithm $\mathcal{I}$ which, given a subset X of S, can determine in unit time whether or not X is independent in M. This assumption implies that the rank of any set $X \subseteq S$,

$$r(X) = \max\{|I| \ : \ I \text{ independent subset of } X\},$$

and in particular, the rank of the matroid

$$r(M) \stackrel{\text{def}}{=} r(S)$$

can be determined in $O(n)$ time by the well-known greedy algorithm. Hence the rank of X in the dual matroid M^*

$$r^*(X) = r(S \setminus X) + |X| - r(M),$$

can also be computed in $O(n)$ time. In particular, $\mathcal{I}$ can be used as an independence oracle for the dual matroid.

Let $\mathcal{C}(M)$ be the family of all circuits of M, i.e., the family of all minimal dependent subsets of S, and let $\mathcal{B}(M)$ be the family of all bases of M, i.e., the collection of all maximal independent sets. By definition, $\mathcal{C}(M)$ and the family $\mathcal{B}(M^*) = \{X \ : \ S \setminus X \in \mathcal{B}(M)\}$ of bases of the dual matroid M^* are mutually transversal hypergraphs.

It is a folklore result that all bases of a matroid M can be enumerated with polynomial delay, i.e., in $poly(n)$ time per each generated base. This can be done, for instance, by traversing the connected "metagraph" $\mathcal{G} = (\mathcal{B}(M), \mathcal{E})$ in which two "vertices" $B, B' \in \mathcal{B}(M)$ are connected by an edge in $\mathcal{E}$ if and only if B and B' can be obtained from each other by exchanging a pair of elements, i.e. when $|B \setminus B'| = |B' \setminus B| = 1$. The connectivity of $\mathcal{G}$ then follows from the well-known *base axiom*:

If $B, B' \in \mathcal{B}(M)$ and $x \in B' \setminus B$ then $(B \cup y) \setminus x \in \mathcal{B}(M)$ for some $y \in B \setminus B'$.

When M is the cycle matroid of a given graph $G = (V, E)$ and consequently $\mathcal{C}(M)$ is the family of all simple cycles of G, all elements of $\mathcal{C}(M)$ can also be enumerated with polynomial delay (see e.g. [13]). This is also true for M^*, the cocycle matroid of G, when each element of $\mathcal{C}(M^*)$ is a minimal set of edges whose removal increases the number of connected components of G (see e.g. [12]). In general, however, we are not aware of any polynomial-delay algorithm for enumerating all circuits of an arbitrary matroid M. Intuitively, the circuit enumeration problem seems to be harder than the base enumeration due to the fact that $|C(M)| \leq (n - r(M))|\mathcal{B}(M)|$, whereas in general, $|\mathcal{B}(M)|$ cannot be bounded by a polynomial in n and $|\mathcal{C}(M)|$. In addition, there is a combinatorial construction which reduces the enumeration of all bases of a matroid to the enumeration of all circuits of another matroid (see Section 5).

In this paper we present a simple algorithm for enumerating all circuits of an arbitrary matroid M in *incremental polynomial time*, i.e. show that for each $k \leq |\mathcal{C}(M)|$, one can compute k circuits of M in $poly(n,k)$ time. This is done in Section 2. By duality, this results also gives an incremental polynomial time algorithm for enumerating all hyperplanes or, more generally, all flats of a given rank in M or M^*. Thus, any level of the lattice of flats of M can be produced in incremental polynomial time.

In Section 3 we consider the enumeration of all circuits of M which contain a given element of $a \in S$. Again, we show that all circuits through a can be enumerated in incremental polynomial time, and discuss some dual formulations of this result. We are not aware of an efficient algorithm for enumerating all circuits containing $t \geq 2$ elements of a given matroid M. In Section 4 we argue that this problem can be solved with polynomial delay for each fixed t when M is the cycle or cocycle matroid of a graph, but becomes NP-hard when t is part of the input.

Section 5 deals with the enumeration of all minimal subsets X of a given set $D \subseteq S$ such that X spans a given flat A of M. Examples of such spanning sets include generalized Steiner trees and multiway cuts in graphs. We reduce the enumeration problem for minimal A-spanning sets to the generation of all circuits through a given element in some extended matroid, and hence obtain an incremental polynomial-time algorithm. All maximal subsets of a given set D which do not span A can also be enumerated in incremental polynomial time.

Section 6 discusses some variants of the circuit enumeration problem for two matroids on S. We also discuss generalized circuits whose definition is obtained by replacing some singletons of S by subsets, i.e., by performing the parallel extension of the rank function $r(X)$ for some sets $A_1, ..., A_n \subseteq S$. We show that the enumeration problems corresponding to these variants and generalizations of circuits are all NP-hard already for graphic and cographic matroids. By duality, this is also true for analogous problems stated in terms of generalized hyperplanes.

Finally, in Section 7 we discuss similar variants and generalizations of bases (or feedback sets) of an arbitrary matroid and show that all of them can be expressed in a natural way as minimal solutions to some systems of polymatroid inequalities. This implies that the corresponding enumeration problems for generalized bases, including spanning, packing, and the maximal independent set problems for several matroids, can all be solved in incremental *quasi-polynomial* time due to results obtained in [1] for general polymatroid inequalities.

2 Enumeration all circuits of a matroid.

Let M be a matroid defined by an independence oracle on ground set S of size n, and let $\mathcal{C}(M) \subseteq 2^S$ be the family of all circuits of M.

Theorem 1 *For each $k \le |\mathcal{C}(M)|$, computing k circuits of M can be carried out in $poly(n,k)$ time.*

Proof. If B is a base of M and $x \in S \setminus B$ then there exists a unique circuit $C = C(B,x)$ such that $x \in C \subseteq B \cup x$. This circuit $C(B,x)$, called the fundamental circuit of x in the base B, can be computed by querying the independence oracle on at most $|B|$ subsets of $B \cup x$. We start by constructing a base B^o of M and the system $\mathcal{F}(B^o) = \{C(B^o,x) \mid x \in S \setminus B^o\}$ of $n - r(M)$ fundamental circuits for B^o. This can be done in $poly(n)$ time. Next, the family $\mathcal{C}(M)$ of circuits of any matroid satisfies the *circuit axiom*:

If C_1 and C_2 are distinct circuits of M and $e \in C_1 \cap C_2$ there exists a circuit C_3 such that $C_3 \subseteq (C_1 \cup C_2) \setminus e$.

Given an arbitrary collection $\mathcal{C}'$ of k circuits of M we can check in $poly(n,k)$ time whether or not $\mathcal{C}'$ is closed with respect to the circuit axiom, i.e., for any two distinct circuits $C_1, C_2 \in \mathcal{C}'$ with a common element $e \in C_1 \cap C_2$ the given collection $\mathcal{C}'$ also contains a circuit $C_3 \subseteq (C_1 \cup C_2) \setminus e$. To enumerate all circuits in M we start with the fundamental system of circuits $\mathcal{C}' = \mathcal{F}(B^o)$ and repeatedly check whether $\mathcal{C}'$ is closed with respect to the circuit axiom. Since each violation of the circuit axiom produces a new circuit, it remains to show that if some system $\mathcal{C}'$ of circuits is closed with respect to the circuit axiom and $\mathcal{F}(B^o) \subseteq \mathcal{C}'$ then $\mathcal{C}' = \mathcal{C}(M)$. This follows from the fact that any set system $\mathcal{C}' \subseteq 2^S$ satisfying the circuit axiom and the Sperner condition

$$C_1, C_2 \in \mathcal{C} \Longrightarrow C_1 \not\subseteq C_2$$

defines a matroid M' on S, see [10, 15]. By definition, the bases of M' are all maximal independent sets for $\mathcal{C}'$, i.e. all those maximal subsets of S which contain no set in $\mathcal{C}'$. In our case $\mathcal{C}' \subseteq \mathcal{C}(M)$ and hence $\mathcal{C}'$ is Sperner by definition. Furthermore, since $\mathcal{C}'$ contains the fundamental system of circuits for $B^o \in \mathcal{B}(M)$, it follows that B^o is also a base of M', implying that the ranks of M and M' are equal. Let $C \in \mathcal{C}(M)$ be an arbitrary circuit of M, then C is the fundamental circuit for some base $B \in \mathcal{B}(M)$ and some element $x \in S \setminus B$, i.e. $C = C(B,x)$. Since B is independent in M' and $|B| = r(M) = r(M')$, we conclude that $B \in \mathcal{B}(M')$. Now M' must also contain a unique fundamental circuit $C' = C'(B,x)$. Since any circuit of M' is also a circuit of M, we conclude that $C = C(B,x) = C'(B,x)$, which shows that $C \in \mathcal{C}' = \mathcal{C}(M')$. □

For an integer threshold t, let

$$\mathcal{H}_t(M) = \{X \ : \ X \text{ maximal subset of } S \text{ such that } r(X) \le t\}$$

be the family of all flats of rank t in M. In particular, when $t = rank(M) - 1$ the family $\mathcal{H}_t(M)$ consists of all hyperplanes of M. Let also

$$\mathcal{C}_t(M) = \{X \ : \ X \text{ minimal subset of } S \text{ such that } r(X) \le |X| - t\},$$

so that $\mathcal{C}_1(M) = \mathcal{C}(M)$ is exactly the family of all circuits of M.

Corollary 1 *Given an integer parameter t, all flats in $\mathcal{H}_t(M)$ can be enumerated in incremental polynomial time. Similarly, all elements of $\mathcal{C}_t(M)$ can also be enumerated in incremental polynomial time.*

Proof. Since each hyperplane of M is the complement of a cocircuit of M and vice versa, the enumeration of all hyperplanes of M is equivalent with the circuit enumeration for the dual matroid M^*. Hence by Theorem 1 all hyperplanes of M can be enumerated in incremental polynomial time. Furthermore, the corollary also holds for the family $\mathcal{H}_t(M)$ of all flats of rank t, because $\mathcal{H}_t(M)$ consists of all hyperplanes of the truncated matroid M_{t+1} whose rank function is defined by $r_{t+1}(X) = \min\{r(X), t+1\}$. Finally, let $\tau = |S| - r(M) - t$ then enumerating all flats of rank τ for M^* is equivalent with the enumeration of all maximal solutions $Y \subseteq S$ to the inequality $r^*(Y) = r(S \setminus Y) + |Y| - r(M) \leq \tau$. The letter problem is in turn equivalent with the enumeration of all minimal solutions $X = S \setminus Y$ to the inequality $r(X) \leq |X| - t$. □

By Corollary 1 the lattice $\mathcal{L}(M)$ of flats of any matroid M can be computed in incremental polynomial time. It is known [9] that $|\mathcal{L}(M)| \geq 2^{r(M)}$.

3 Circuits through a given element

An important open question in linear programming is whether there exists an efficient way to enumerate all vertices of a given polytope

$$P = \{x = (x_1, \ldots, x_n) \in \Re^n \ : \ \sum_{i=1}^{n} a_i x_i = a, \quad x_1, \ldots, x_n \geq 0 \ \},$$

where $a, a_1, \ldots, a_n$ are given d-dimensional vectors. Each vertex of P can be identified with a minimal supporting set I of coordinates $\{1, \ldots, n\}$ for which the system of linear equations

$$\sum_{i \in I} a_i x_i = a \tag{1}$$

has a non-negative, and hence positive real solution. Dropping the non-negativity conditions we arrive at the problem of enumerating all minimal sets $I \subseteq \{1, \ldots, n\}$ for which (1) has a real solution. This is equivalent with the enumeration of all those circuits of the vectorial matroid $M = \{a, a_1, \ldots, a_n\} \subseteq \Re^d$ that contain a. When M is the cycle or cocycle matroid of some connected graph $G = (V, E)$ and $a = (uv) \in E$ is an edge with endpoints $u, v \in V$, enumerating all circuits through a calls for computing all simple uv-paths or all minimal uv-cuts in G, which can be done with polynomial delay [12, 13]. The following results indicates that all circuits through a given element a can be efficiently enumerated for any matroid M.

Theorem 2 *Let M be a matroid with ground set S, let $a \in S$, and let $\mathcal{C}(M, a)$ the set of circuits C of M such that $a \in C$. Assuming that M is defined by an independence oracle, all elements of $\mathcal{C}(M, a)$ can be enumerated in incremental polynomial time.*

Proof. Two elements $x, y \in S$ are said to be *connected* in M if either $x = y$ or there is a circuit $C \in \mathcal{C}(M)$ containing both x and y. It is well known that this definition results in an equivalence relation on S, each equivalence class of which is called a *connected component* of M. In particular, M is connected if S is the only connected component of M. Given an independence oracle for M, the connected components of M can be determined as follows:

(i) Compute a base B^o of M and the $n - r(M)$ fundamental circuits for B^o. Let $\mathcal{COMP}$ be the set system consisting of the fundamental circuits and $r(M)$ singletons of B^o;

(ii) Repeatedly replace any two intersecting sets in $\mathcal{COMP}$ by their union until all sets in $\mathcal{COMP}$ become disjoint;

(iii) Return the disjoint sets of $\mathcal{COMP}$ as connected components of M.

This procedure can be carried out in *poly*(n) time due to the fact that there may be at most $n - 1$ set unions in step (ii). It correctly identifies the connected components of M because the algorithm described in the proof of Theorem 1 generates all circuits of M. This means that whenever two distinct elements of S can be connected by a circuit of M they can also be connected by a sequence of steps (ii). We mention in passing that the above polynomial-time procedure can easily be extended to compute a connecting circuit for each pair of distinct connected elements.

Returning to the problem of enumerating all circuit of M through the given element a we observe that all such circuits must belong to the connected component of M which contains a. So we may replace S by this connected components and assume without loss of generality that M is connected.

Given a set $X \subseteq S$ let

$$D(X) = X \setminus \bigcap \{C \in \mathcal{C}(M, a) \ : \ C \subseteq X\},$$

where as before $\mathcal{C}(M, a)$ denotes the set of all circuits containing a.
Lehman's theorem [10, 15] asserts that for any connected matroid M the circuits of M not containing a are precisely the minimal sets of the form $D(C_1 \cup C_2)$ where C_1 and C_2 are distinct members of $\mathcal{C}(M, a)$. Hence for any connected matroid M we have the following bound:

$$|\mathcal{C}(M)| \leq |\mathcal{C}(M, a)|\big(|\mathcal{C}(M, a)| + 1\big)/2.$$

This bound and Theorem 1 readily imply that all circuits in $\mathcal{C}(M, a)$ can be enumerated in output polynomial time *poly*$(|\mathcal{C}(M, a)|)$ by simply generating all circuits in $\mathcal{C}(M)$ and discarding those of them that do not pass through a. In fact, since our enumeration problem is self-reducible, the above bound also implies an incremental polynomial-time algorithm. To see this, assume that we wish to enumerate a given number k of circuits in $\mathcal{C}(M,a)$, or list all of them if $k \geq |\mathcal{C}(M,a)|$. Since for each integer $k' \leq |\mathcal{C}(M)|$ we can obtain k' circuits in $\mathcal{C}(M)$ in $poly(n,k')$ time, we can decide whether or not $k \geq |\mathcal{C}(M,a)|$ by attempting to generate $k' = k(k+1)/2$ circuits in $\mathcal{C}(M)$, in time bounded by a polynomial in n and k. If we discover that $|\mathcal{C}(M)| \leq k(k+1)/2$ by producing all circuits in $\mathcal{C}(M)$ then we also have the entire set $\mathcal{C}(M,a)$. Suppose now that we have computed $k(k+1)/2$ circuits in $\mathcal{C}(M)$ but fewer than k of them pass through a. Let $b \neq a$ be another element of S. Delete b and compute the connected component S' which contain a in the matroid M restricted to $S \setminus b$. Note that any circuit of $\mathcal{C}(M,a)$ which do not contain b must belong to S'. So we may apply the same procedure to the connected matroid M' obtained by restricting M on S', and either obtain all circuits of $\mathcal{C}(M,a)$ which avoid b, or conclude that the number of such circuits exceeds k. Since in the latter case we can reduce the size of S by removing b for good (as long as we are not required to produce more than k circuits of $\mathcal{C}(M,a)$), we may now assume without loss of generality that for each element $b \neq a$ we have obtained all the circuits in $\mathcal{C}(M,a)$ which avoid b. This means that in time polynomial in n and k we can produce all circuits in $\mathcal{C}(M,a)$ which skip some element of S. Unless S itself is the only element of $\mathcal{C}(M,a)$, this gives the entire set $\mathcal{C}(M,a)$. □

As an application of Theorem 2, consider a system of equations

$$Ax = b, \qquad x \in \Re^d, \tag{2}$$

where $A \in \Re^{n \times d}$ is a given $n \times d$-matrix and $b \in \Re^n$ is an n-vector. Suppose that the system is infeasible. If $A'x = b'$ is an infeasible subsystem of (2), then the rows of the augmented matrix $[A'|\ b']$ must contain the vector $a \stackrel{\text{def}}{=} (0,\ldots,0,1) \in \Re^{d+1}$ in their linear hull. In particular, the minimal infeasible subsystems of (2) correspond to the circuits containing a in the vectorial matroid defined by the rows of the matrix $[A|\ b]$. Thus, all minimal infeasible subsystems of (2) can be enumerated in incremental polynomial time.

By duality, Theorem 1 gives an incremental polynomial-time algorithm for enumerating all hyperplanes (or, more generally, all flats of a given rank t) which *do not contain* a. Needless to say that all hyperplanes (or flats of rank t) which *contain* an arbitrary set of elements $A \subseteq S$ can be enumerated in incremental polynomial time because this is equivalent with enumerating all circuits of the (truncated) matroid M restricted to $S \setminus A$.

It is also worth mentioning that $\{C \setminus \{a\} \mid C \in \mathcal{C}(M,a)\}$ and $\{C' \setminus \{a\} \mid C' \in \mathcal{C}(M^*,a)\}$ form a pair of mutually transversal Sperner hypergraphs. For instance, these hypergraphs consist of all uv-paths and all uv-cuts respectively, when M is a cycle matroid of a connected graph $G = (V,E)$ in which edge $a = (uv)$ connects vertices $u, v \in V$.

4 Circuits through t elements

It is natural to ask what is the complexity of enumerating all circuits of M which contain a given set $A = \{a_1, \ldots, a_t\}$ of $t \geq 2$ elements of S. As we argue below, this problem is NP-hard when t is part of the input but can be solved with polynomial delay if $t = |A|$ is fixed and M is the cycle or cocycle matroid of a given graph $G = (V, E)$. However, we are not aware of an efficient algorithm for listing all circuits through $t = const \geq 2$ elements of arbitrary matroids.

Let M be the cycle matroid of G so that the circuits of M are the simple cycles of G. An edge set A may be contained in a simple cycle only if A itself is a simple cycle or A is a union of k pairwise vertex disjoint simple paths $P_1, \ldots, P_k$ for some integer positive $k \leq t$. All simple cycles containing $P_1, \ldots, P_k$ can be enumerated with polynomial delay via lexicographic backtracking [13] by growing and merging these partial paths (so that their number continually decreases). Hence backtracking listing algorithms reduce the enumeration of simple cycles containing $a_1, \ldots, a_t$ to the following decision problem:

> Does there exist a simple cycle in G which contain k given disjoint paths $P_1, \ldots, P_k$?

When k is fixed, by considering all possible permutations and reversals of $P_1, ..., P_k$ the latter problem can in turn be polynomially reduced to the well-known *disjoint-path problem*:

> Given k pairs of vertices $\{u_i, v_i\}$, $i = 1, \ldots, k$ of a graph, can these pairs be connected by k pairwise vertex disjoint paths?

Even though the disjoint path problem is NP-complete when k is part of the input (see [7]), it is known [14] to be solvable in polynomial time for each fixed k. Hence all simple cycles through $t = const$ edges can be enumerated with delay bounded by a polynomial in the size of the input graph.

As we mentioned earlier, if $t = |A|$ is part of the input then the problem of enumerating all simple cycles through t edges of a graph becomes NP-complete. In fact, given a graph $G = (V, E)$ and a (large) matching $A \subset E$ it is NP-hard to decide whether G has *any* simple cycle containing A. This can be seen from the following argument. Given a graph $H = (U, E)$, substitute an edge e_u for each vertex $u \in U$. Then, unless G consists of a single edge, the resulting graph $G = P_2 \times H$ has a simple cycle through the matching $A = \{e_u \ : \ u \in U\}$ if and only if the original graph H is Hamiltonian, a condition which is NP-complete to verify.

Now, let M be the cocycle matroid of a connected graph $G = (V, E)$ and accordingly, let the circuits of M be the minimal cuts of G. It is well-known and easy to see that an edge set $C \subseteq E$ forms a minimal cut in G if and only if there is a partition $V = U \cup W$ such that C is the set of all edges between U and W and the induced subgraphs $G[U]$ and $G[W]$ are both connected. In particular, this means that C (and each subset of C) must form a bipartite graph.

Given an edge set $A = \{a_1, \ldots, a_t\} \subseteq E$ which forms a bipartite graph $G_A = (V_A, A)$, let us split G_A into connected components $G_{A_i} = (V_{A_i}, A_i),\ i = 1, \ldots, k$ for some $k \leq t$. Then the problem of enumerating all minimal cuts containing A can be solved with polynomial delay via lexicographic backtracking [13] by growing and merging these connected components in all possible ways (so that their number can only decrease). Specifically, backtracking listing algorithms reduce the enumeration of minimal cuts containing $a_1, \ldots, a_t$ to the following decision problem:

> Given two disjoint vertex sets $U', W' \subseteq V$ can they be extended to a partition U, W which defines a minimal cut, that is $U' \subseteq U$, $W' \subseteq W$, $U \cap W = \emptyset$, $U \cup W = V$, and the induced subgraphs $G[U]$ and $G[W]$ are both connected ?

If t, and hence $|U'| + |W'|$, is bounded this problem can be solved in polynomial time. In fact, this is true for the following more general problem:

> Given a graph $G = (V, E)$ and r pairwise disjoint vertex sets $U'_1, \ldots U'_r \subseteq V$, are there vertex sets $U_1 \ldots U_r \subseteq V$ which are still pairwise disjoint, $U'_i \subseteq U_i$ and the induced subgraph $G[U_i]$ is connected (i.e. spans U_i) for each $i = 1, \ldots, r$?

Robertson and Seymour [14] proved that for bounded $|U'_1| + \ldots + |U'_r|$ the above problem can be solved in polynomial time. Obviously, without loss of generality one can assume that the extended sets $U_1 \ldots U_r$ form a partition of V and hence for $r = 2$ the above problem includes the previous one.

Finally, similarly to minimal cycles, the enumeration of all minimal cuts through t edges becomes NP-hard when t is part of the input. Indeed, given a graph $G = (V, E)$ and a matching $A = \{a_1 = (u_1, w_1), \ldots, a_t = (u_t, w_t)\} \subseteq E$, it may be NP-hard to tell whether G has a minimal cut containing A. The latter claim can be shown as follows. Let $U' = \{u_1, \ldots, u_t\}$, $\quad W' = \{w_1, \ldots, w_t\}$, and $V' = V \setminus (U' \cup W')$. Consider the family $\mathcal{G}$ of all graphs $G = (V, E)$ such that

(i) the induced subgraph $G[V']$ is complete,
(ii) $G[U']$ and $G[W']$ are edge-free,
(iii) there are no edges between U' and W' except A, and
(iv) the edges between V' and U' and between V' and W' are symmetric in the sense that $(v, u_i) \in E \quad \Leftrightarrow \quad (v, w_i) \in E$ for all $v \in V'$ and all $i = 1, \ldots, t$.

Note that condition (iv) makes irrelevant any reversals in A, and that the decision problem:

> Given a graph $G \in \mathcal{G}$, is it possible to split V' between U' and W' to obtain two connected induced subgraphs ?

is polynomially equivalent with the special case of the CNF satisfiability problem in which all clauses are either strictly positive or strictly negative, and the clauses in the positive and negative halves are symmetric. It remains to notice that this special case of the satisfiability problem is NP-complete since it is equivalent to the identification of *self-compliment saturated hypergraphs*, a problem whose NP-completeness was shown in [4].

We mention in closing that the results of this section also indicate that it may be NP-complete to decide whether a cycle or cocycle matroid M has a hyperplane avoiding a given set A of elements.

5 Minimal spanning sets for a flat

Let as before M be a matroid on S. Each circuit C containing a given element $a \in S$ can be identified with a minimal (independent) set I such that $a \in Span(I)$, where

$$Span(I) = \{x \in S \; : \; r(I \cup x) = r(I)\}$$

is the closure operator. In this section we consider the problem of enumerating all minimal sets I spanning a given collection of elements $A \subseteq S$. In fact, we will consider a slightly more general problem of generating all minimal subsets $I \subseteq D$ which span A, where D and A are two (not necessarily disjoint) given nonempty sets of elements of M. We denote the family of all such minimal spanning sets I by $\mathcal{SPAN}(D, A)$. Note that since $A \subseteq Span(I)$ implies $Span(A) \subseteq Span(I)$, we could assume that A is a flat, i.e. $A = Span(A)$.

Example 1 (Generalized Steiner trees and point-to-point connections) Let $G = (V, E)$ be a graph with k given disjoint vertex sets $V_1, \ldots, V_k \subseteq V$. A *generalized Steiner tree* is a minimal set of edges $I \subseteq E$ connecting all vertices within each set V_i, i.e., for each $i = 1, \ldots, k$, all vertices of V_i must belong to a single connected component of (V, I). In particular, for $k = 1$ we obtain the usual definition of Steiner trees. When each set V_i consists of two vertices $\{u_i, v_i\}$, generalized Steiner trees are called *point-to-point* connections. Let $T_1, \ldots, T_k$ be arbitrary spanning trees on $V_1, \ldots, V_k$ composed of "new" edges, and let M the cycle matroid of the multigraph $(V, E \cup T_1 \cup \ldots \cup T_k)$ with a total of $|E| + |V_1| + \ldots + |V_k| - k$ edges. Then $\mathcal{SPAN}(E, T_1 \cup \ldots \cup T_k)$ is the family of all generalized Steiner trees for $V_1, \ldots, V_k$.

Example 2 (Multiway cuts) For a connected graph $G = (V, E)$ with k pairs of vertices $\{u_i, v_i\}$, $i = 1, \ldots, k$, a *multiway cut* is a minimal collection of edges whose removal disconnects each u_i from v_i. Letting $A = \{(u_i v_i) \; : \; i = 1, \ldots, t\}$ and assuming without loss of generality that $A \cap E = \emptyset$, the family of all multicuts of G can be identified with the family $\mathcal{SPAN}(E, A)$ for the cocycle matroid of $(V, E \cup A)$.

Theorem 3 *Given a matroid M with ground set S and two non-empty sets $D, A \subseteq V$, all elements of $\mathcal{SPAN}(D, A)$ can be enumerated in incremental polynomial time. All maximal subsets of D which do not span A can also be enumerated in incremental polynomial time.*

Proof. Let α be a new element representing A, and let M_α be the matroid on $D \cup \alpha$ with the following rank function:

$$\rho(X) = \begin{cases} r(X), \text{ if } \alpha \notin X \\ \max\{r((X \setminus \alpha) \cup a) \ : \ a \in A\}, \quad \text{otherwise.} \end{cases} \tag{3}$$

It is easy to check that M_α is indeed a matroid. When M is a vectorial matroid over a large field, α can be interpreted as the "general linear combination" of all elements of A; in general, $\rho(X)$ is the so-called *principal extension of* $r(X)$ *on* A *with value* 1 (see e.g. [11]).

When $I \in \mathcal{SPAN}(D, A)$ then $I \cup \alpha$ is a circuit in M_α and conversely, for any circuit C in M_α containing α, the set $C \setminus \alpha$ belongs to $\mathcal{SPAN}(D, A)$. Hence the enumeration problem for $\mathcal{SPAN}(D, A)$ is equivalent with that for the set of all circuits through α in M_α. Given an independence oracle for M, the rank function (3) of the extended matroid can be trivially evaluated in oracle-polynomial time. Therefore the first claim of Theorem 3 directly follows from Theorem 2. To see the second claim note that the maximal subsets of D which do not span A are in one-to-one correspondence with the hyperplanes of M_α which avoid α. □

We close this section with the observation that since $\mathcal{SPAN}(S, S)$ is the set of bases of M, the proofs of Theorems 2 and 3 show that the enumeration of all bases of a matroid can be reduced to the enumeration of all circuits of another matroid.

6 Circuits in two matroids. Generalized circuits.

Let M_1 and M_2 be two matroids on S, with rank functions $r_1(X)$ and $r_2(X)$. It is known that the minimum of the submodular function $r_1(X) + r_2(S \setminus X)$ for all $X \subseteq S$ gives the maximum cardinality of a set I independent in both M_1 and M_2, and that this minimum can be computed in polynomial time [3]. In particular, when the ranks of M_1 and M_2 are equal one can determine in polynomial time whether M_1 and M_2 share a common base, i.e. $\mathcal{B}(M_1) \cap \mathcal{B}(M_2) \neq \emptyset$. In fact, using this as a subroutine for backtracking on matroids obtained by deleting and contracting elements of S, all bases in $\mathcal{B}(M_1) \cap \mathcal{B}(M_2)$ can be enumerated with polynomial delay.

In contrast to this result, deciding whether M_1 and M_2 contain a common circuit is NP-hard already when M_1 is the cycle matroid of some graph $G = (V, E)$ and M_2 is the uniform matroid on E whose bases are all subsets of size $r = |V| - 1$. In this case, $\mathcal{C}(M_1) \cap \mathcal{C}(M_2) \neq \emptyset$ if and only if G is Hamiltonian. A similar argument for the NP-complete maximum cut problem shows that testing if $\mathcal{C}(M_1) \cap \mathcal{C}(M_2) \neq \emptyset$ remains NP-hard when M_1 is the cocycle matroid of a graph $G = (V, E)$ and M_2 is again a uniform matroid on E.

Of course, given two matroids M_1 and M_2 on S one can always enumerate all elements of $\mathcal{C}(M_1) \cup \mathcal{C}(M_2)$ in incremental polynomial time due to Theorem 1. Note, however, that deciding whether a given set $C \in \mathcal{C}(M_1) \cup \mathcal{C}(M_2)$ is *maximal* in $\mathcal{C}(M_1) \cup \mathcal{C}(M_2)$ may be NP-hard. This is because for any set $A \subseteq S$ we may choose M_2 to be the matroid for which A is the only circuit, and then deciding whether A is maximal becomes equivalent with determining if M_1 has a circuit containing A (see Section 4). Perhaps more surprisingly, for two matroids M_1 and M_2 on S enumerating all *minimal* elements of $\mathcal{C}(M_1) \cup \mathcal{C}(M_2)$ may also be hard.

Proposition 1 *Let M_1 and M_2 be the cycle matroids of two graphs $G_1 = (V_1, E)$ and $G_2 = (V_2, E)$ with identical sets of edges, and let $\mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\}$ be the collection of all minimal edge sets which form a cycle in G_1 or G_2. Then, given a set family $\mathcal{M} \subseteq \mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\}$, it is NP-complete to tell whether $\mathcal{M}$ can be extended, i.e. $\mathcal{M} \neq \mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\}$.*

Proof. We reduce our problem from the CNF satisfiability problem: Is there a truth assignment of N binary variables satisfying a given conjunctive normal form $\phi(x_1, \ldots, x_N) = D_1 \wedge \ldots \wedge D_m$, where each D_j is a disjunction of some literals in $\{x_1, \bar{x}_1, \ldots, x_N, \bar{x}_N\}$. We denote by $n = |D_1| + \ldots + |D_m|$ the total number of literals in ϕ, and assume that (i) $m \geq 3$ and (ii) each variable x_i and its negation $\bar{x}_i$ occur in ϕ, i.e., ϕ is not monotone or anti-monotone with respect to some variable.

We start by replacing each variable x_i in disjunction D_j by a new variable Y_{ij}, and we also replace each negation $\bar{x}_k$ in D_j by another new variable Z_{kj}. Let E be the set of n variables Y_{ij} and Z_{ij} obtained after these substitutions. Now we construct two graphs $G_1 = (V_1, E)$ and $G_2 = (V_2, E)$, both with edge sets in one-to-one correspondence with E. The first of these graphs G_1 is a collection of m disjoint cycles $C_1, ..., C_m$ where $|C_j| = |D_j|$, and the edges of C_j are labeled by the variables Y_{ij}, Z_{kj} coming from D_j, $j = 1, \ldots, m$. The second graph is

$$G_2 = v_0 \ P_1 \ v_1 \ P_2 \ v_2 \ldots \ v_{N-1} \ P_N \ v_0,$$

where $v_0, v_1, \ldots, v_{N-1}, v_0$ are vertices the first and last of which are identified to form a ring, and each P_i consists of two parallel chains $Y_i = E \cup \{Y_{i1}, \ldots, Y_{im}\}$ and $Z_i = E \cup \{Z_{i1}, \ldots, Z_{im}\}$ between v_{i-1} and v_i. Due to our assumptions (i) and (ii), G_2 is connected and has two types of cycles: 1) N trivial cycles of the form $\{Y_i, Z_i\}$, $i = 1, \ldots, N$, and 2) 2^N additional cycles in one-to-one correspondence with the truth assignments of $x_1, \ldots, x_N$. Now let $\mathcal{M}$ be the collection of all those cycles among $C_1, \ldots, C_m$ and all those cycles of type 1 which belong to $\mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\}$. Then $|\mathcal{M}| \leq m + N$ and all other cycles in $\mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\} \setminus \mathcal{M}$ must be of type 2. However, it is easy to see that any cycle of type 2 in $\mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\}$ is equivalent with the satisfiability of ϕ. $\square$

We close this section with yet another generalization of the notion of circuit in a matroid. Let M be a matroid defined by an independence oracle on some ground set U, and let $A_1, \ldots, A_n$ be given (not necessarily disjoint) subsets of U. We define a *generalized circuit* as a minimal subset X of $S = \{1, \ldots, n\}$ such that $\bigcup_{i \in X} A_i$ is a dependent set in M.

Proposition 2 *Enumerating all generalized circuits for the cycle matroid of a graph is NP-hard even when $A_1, \ldots, A_n$ are disjoint sets of edges of size 2 each.*

Proof. Let $G = G_1 \cup G_2$ be the disjoint union of the graphs G_1 and G_2 constructed in the proof of Proposition 1. Each of these graphs has n edges labeled by n elements of E. Let $A_1, ..., A_n$ be the n pairs of edges labeled by identical elements of E in G_1 and G_2. Then $A_1, \ldots, A_n$ are disjoint and the set of generalized circuits of $G_1 \cup G_2$ can be identified with $\mathcal{MIN}\{\mathcal{C}(M_1) \cup \mathcal{C}(M_2)\}$. □

It is easy to see that in Propositions 1 and 2 the cycle matroids of G_1 and G_2 can be replaced by the cocycle matroids of some graphs (e.g., the planar duals of G_1 and G_2). Also, by matroid duality, Proposition 1 shows that it may be NP-hard to enumerate all *generalized hyperplanes* of M, i.e., all those maximal subsets X of $S = \{1, \ldots, n\}$ for which $Span(\cup_{i \in X} A_i) \neq S$.

In the next section we consider *generalized bases* and argue that their enumeration is a much easier task even when they are defined for two or more matroids.

7 Generalized bases. Spanning and packing in matroids. Systems of polymatroid inequalities

Let M be a matroid on ground set U, and let $A_1, \ldots, A_n$ be given subsets of U. We define a *generalized base* as a minimal subset X of $S = \{1, \ldots, n\}$ for which the sets $A_i,\ i \in X$ span the matroid, i.e.,

$$r(\bigcup_{i \in X} A_i) \geq r(M). \tag{4}$$

Note that when $n = |U|$ and the sets A_i are the n disjoint singletons of U, this definition leads to the standard notion of a base of M. On the other hand, if each set A_i is a subset of elements of some fixed base B then

$$r(\bigcup_{i \in X} A_i) = |\bigcup_{i \in X} A_i|,$$

and accordingly each generalized base is a minimal set cover of B. Another interesting special case of generalized bases deals with minimal spanning collections of subspaces $A_1, \ldots, A_n$ in a given linear space M, see Example 3 below.

It will be convenient to further extend the definition of generalized bases. First, we can replace the right-hand side of inequality (4) by a given integer threshold $t \in \{1, \ldots, r(M)\}$. This is equivalent with replacing M by the truncated matroid with the rank function $r_t(\cdot) = \min\{r(\cdot), t\}$ and leads us to the notion of a *minimal t-spanning set*, i.e. a minimal set $X \subseteq \{1, \ldots, n\}$ for which

$$r(\bigcup_{i \in X} A_i) \geq t.$$

Naturally, for $t = r(M)$ we return to the definition of generalized bases.

Secondly, we may consider a number m of matroids $M_1, \ldots, M_m$ defined by independence oracles on ground sets $U_1, \ldots, U_m$. Suppose that for each of the matroids M_j we are given a collection of n sets $A_{j1}, \ldots, , A_{jn} \subseteq U_j$ along with an integer threshold $t_j \in \{1, \ldots, r(M_i)\}$, and consider the family $\mathcal{F}$ of all minimal solutions $X \subseteq S = \{1, \ldots, n\}$ to the system of m inequalities

$$r_j(\bigcup_{i \in X} A_{ji}) \geq t_j, \quad j = 1, \ldots, m. \tag{5}$$

Note that the rank function of any matroid is *polymatroid*, i.e. monotone, submodular, with minimum 0. It is also easy to see if $A_1, \ldots, A_n$ are arbitrary subsets of the ground set U of a matroid with rank function r, then the function $f(X) = r(\cup_{i \in X} A_i)$ is also polymatroid, i.e.

(i) $X \subseteq Y \subseteq S \implies f(X) \leq f(Y)$;
(ii) $f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y)$ for all $X, Y \subseteq S$, and
(iii) $f(\emptyset) = 0$.

The polymatroid function $f(X) = r(\cup_{i \in X} A_i)$ is called the *parallel extension* of r *with respect to* $A_1, \ldots, A_n$, see e.g. [11]. It is known [6] that any polymatroid function $f(X)$ can be obtained in this way from some matroid.

Returning to the minimal spanning subfamilies for (4) or, more generally, to the family $\mathcal{F}$ of all minimal feasible solutions for (5), we conclude that $\mathcal{F}$ is the family of all minimal feasible solutions $X \subseteq S = \{1, \ldots, n\}$ to the system of polymatroid inequalities

$$f_j(X) \geq t_j, \quad j = 1, \ldots, m, \tag{6}$$

where $f_j(X) = r_j(\bigcup_{i \in X} A_{ji})$. Since we assume that each of the input matroids is given by an independence oracle, each of the functions f_j can be evaluated at any set $X \subseteq S$ in polynomial oracle time. As shown in [1], given a system of polymatroid inequalities (6) defined by a polynomial-time evaluation oracle, we can compute any given number $k \leq |\mathcal{F}|$ of minimal solutions $X \in \mathcal{F}$ to (6) in time $N^{o(\log N)}$, where $N = m(nk)^{\log \max\{t_1, \ldots, t_m\}}$. Since $t_j \leq |U_j|, \; j = 1, \ldots, m$, we thus conclude that all minimal solutions to (5) can be enumerated in *incremental quasi-polynomial* time:

Theorem 4 ([1]) *Given m matroids $M_1, \ldots, M_m$ defined by independence oracles on ground sets $U_1, \ldots, U_m$, and a collection of n sets $A_{j1}, \ldots, , A_{jn} \subseteq U_j$ along with an integer threshold $t_j \in \{1, \ldots, r(M_j)\}$ for each of the matroids, the set $\mathcal{F}$ of minimal solutions $X \subseteq \{1, \ldots, n\}$ to the system of generalized rank inequalities (5) can be computed in incremental quasi-polynomial time, i.e. $k \leq |\mathcal{F}|$ elements of $\mathcal{F}$ can be produced in $2^{polylog(K)}$ time, where $K = \max\{k, n, m, |U_1|, \ldots, |U_m|\}$.*

Theorem 4 clearly indicates that for matroids defined by polynomial-time independence oracles the enumeration of all generalized bases or, more generally, the enumeration of all minimal solutions for (5) cannot be NP-hard unless NP $\subseteq$ QUASI-POLYTIME.

A function $f : 2^S \to \Re$ is called *α-smooth* if $|f(X \cup \{i\}) - f(X)| \leq \alpha$ for all $X \subseteq S$ and $i \in S \setminus X$. The rank function r of any matroid is 1-smooth, while the parallel extension of r with respect to given sets $A_1, \ldots, A_n$ is $\max\{|A_1|, \ldots, |A_n|\}$-smooth. When the number of polymatroid inequalities in (6) is fixed and each of these inequalities is α-smooth for some fixed α, Theorem 4 can be strengthened as follows:

Theorem 5 *When* $\max\{m, |A_{11}|, ..., |A_{nm}|\} = O(1)$ *all minimal solutions to (6) can be enumerated with polynomial delay.*

Proof. Let $\mathcal{F}$ be the family of minimal feasible sets for (6). Then the elements of $\mathcal{F}$ can be enumerated with polynomial delay by traversing the *strongly connected* directed metagraph $\mathcal{G} = (\mathcal{F}, \mathcal{E})$, in which a pair of vertices (X, X') forms an edge in $\mathcal{E}$ if and only if X' can be obtained from X by adding an element from $X' \setminus X$ and deleting at most $m(2\alpha - 1)$ elements from $X \setminus X'$, i.e. if $X' = X \cup \{e\} \setminus Y$, for some $e \in X' \setminus X$, and $Y \subseteq X \setminus X'$ with $|Y| \leq m(2\alpha - 1)$. Let $\alpha \stackrel{\text{def}}{=} \max\{|A_{11}|, ..., |A_{nm}|\}$ and note that the functions $f_1, \ldots, f_m$ are α-smooth. Note also that for constant α and m, the out-degree of each vertex of G is polynomially bounded. Furthermore, the strong connectivity of $\mathcal{G}$ can be proved as follows. Given two vertices $X, X' \in \mathcal{F}$ of G, there exists a set $\{X_0, X_1, \ldots, X_{k-1}, X_k\}$ of elements of F, where $X_0 = X$, $X_k = X'$, and for all $i = 1, \ldots, k$, X_i is obtained from X_{i-1} by adding an element from $X_k \setminus X_{i-1}$ and deleting some elements from $X_{i-1} \setminus X_k$. Thus it is enough to show that the number of deleted elements in each step does not exceed $m(2\alpha - 1)$. To prove this, consider a set $X \in \mathcal{F}$. By the minimality of X, for each $x \in X$, there is a $j \in [m]$ such that $f_j(X \setminus \{x\}) \leq t_j - 1$. Let $I \stackrel{\text{def}}{=} \{j \in [m] \ : \ f_j(X \setminus \{x\}) \leq t_j - 1, \text{ for some } x \in X\}$, then for each $i \in I$,

$$f_i(X) \leq t_i + \alpha - 1 \tag{7}$$

follows by the minimality of X and the α-smoothness of f_i. Let $X' \stackrel{\text{def}}{=} X \cup \{e\} \setminus Y$, for some $e \in S \setminus X$ and some $Y \subseteq X$, and assume that $X' \in \mathcal{F}$. For $i \in I$, define $Y_i \stackrel{\text{def}}{=} \{x \in Y \mid f_i(X \setminus \{x\}) \leq t_i - 1\}$. Then if follows by the α-smoothness and the monotonicity of the functions $f_1, \ldots, f_m$ that

$$f_i(X') \leq f_i(X \setminus Y_i) + \alpha, \qquad \text{for all } i \in I. \tag{8}$$

It follows, furthermore, by the submodularity and minimality of X that

$$f_i(X) - f_i(X \setminus Y_i) \geq |Y_i|, \qquad \text{for all } i \in I. \tag{9}$$

But $f_i(X') \geq t_i$ for all $i \in I$, which together with (7), (8), and (9), gives

$$|Y| \leq \sum_{i \in I} |Y_i| \leq \sum_{i \in I} (f_i(X) - f_i(X \setminus Y_i)) \leq |I|(2\alpha - 1).$$

The theorem follows. $\square$

In the remainder of the paper we briefly discuss some application examples for Theorems 4 and 5.

Example 3 (Minimal t-spanning sets and connectivity ensuring collections of graphs) Theorems 4 and 5 imply that given a matroid M on ground set U and an integer threshold t, the family

$$\mathcal{F}(\mathcal{A}, t) = \{X \;:\; X \text{ minimal subset of } \{1, \ldots, n\} \text{ such that } r(\cup_{i \in X} A_i) \geq t\}$$

of all minimal t-spanning sets can be enumerated in incremental quasi-polynomial time for any given collection $\mathcal{A}$ of sets $A_1, \ldots, A_n \subseteq U$, and with polynomial delay when the sizes of $A_1, \ldots, A_n$ are bounded. In particular, this result applies to generalized bases, i.e. minimal subfamilies of $A_1, \ldots, A_n$ that span the entire matroid:

$$Span\langle \bigcup_{i \in X} A_i \rangle = U.$$

As an application, let $A_1, \ldots, A_n \subseteq V \times V$ be a family of undirected graphs on common vertex set V, and let $\mathcal{F}$ be all those minimal subfamilies X of $\{1, \ldots, n\}$ for which the graph $G(X) = (V, \bigcup_{i \in X} A_i)$ is connected (or has at most t connected components, where t is a given threshold). Then all elements of $\mathcal{F}$ can be enumerated in incremental polynomial time or with polynomial delay for $\max\{|A_1|, \ldots, |A_n|\} = O(1)$. This result generalizes the well-known fact that all spanning trees for a graph can be enumerated efficiently. Interestingly, enumerating all minimal collections of $A_1, \ldots, A_n$ *connecting two given vertices* $a, a' \in V$ turns out to be NP-hard already when the input sets of edges $A_1, \ldots, A_n$ are pairwise disjoint and contain at most 2 edges each, see [5]. In other words, given n disjoint sets $A_1, \ldots, A_n \subseteq U$ of size 2 in a (graphic) matroid M it may be NP-hard to enumerate all minimal subfamilies $X \subseteq \{1, \ldots, n\}$ which span a *given flat* A of the matroid

$$A \subseteq Span\langle \bigcup_{i \in X} A_i \rangle,$$

even when A is a line, i.e. $r(A) = 1$. In addition, Proposition 2 shows that generating the family of all generalized hyperplanes

$$\mathcal{H}(\mathcal{A}) = \{X \;:\; X \text{ maximal subset of } \{1, \ldots, n\} \text{ such that } r(\cup_{i \in X} A_i) \leq r(M) - 1\}$$

is also NP-hard already for graphic matroids and $|A_1| = \ldots = |A_n| = 2$. In fact, given a connected graph $G = (V, A_1 \cup A_2 \ldots \cup A_n)$, where $A_1, \ldots, A_n \subseteq V \times V$ are n disjoint pairs of edges, it is NP-hard to enumerate all *generalized cuts* $X \subseteq \{1, \ldots, n\}$, i.e. all minimal subfamilies of $A_1, \ldots, A_n$ whose removal disconnect some vertices of V, see [5].

Example 4 (Bar-and-joint structure) The following example is taken from [11]. "Let B be a bar-and-joint structure, i.e. a graph $G = (V, E)$ whose nodes are points of the Euclidean 3-space, and whose edges are rigid bars attached to the nodes by flexible joints. Let, for each $X \subseteq V$, $f(X)$ denote the *degree of freedom* of the subset X, i.e. the dimension of the infinitesimal motions of all nodes in X which extend to an infinitesimal motion of all nodes compatible with the given bars. Then $f(\emptyset) = 0$, $f(\{x\}) = 3$ for every $x \in V(G)$ and $f(\{x, y\}) = 5$ or 6 depending on whether or not the whole structure forces x and y to stay at the same distance, etc. It follows from the elements of the theory of rigid bar-and-joint structures that f is a submodular set-function on the subsets of $V(G)$. See [2]."

Moreover, it is easy to see that function f is polymatroid. Hence, it follows from Theorem 4 that, given a (positive integer) threshold t, we can generate all minimal familes of nodes whose degree of freedom is at least t in incremental quasi-polynomial time. Standardly, this result can be generalized to parallel extensions of f and to families of bar-and-joint structures with different thresholds.

Example 5 (Maximal independent sets in m matroids) An important special case of Theorem 4 is when all matroids are defined on the same ground set $U = U_1 = \ldots = U_n = \{1, \ldots, n\}$, and $A_{ji} = \{i\}$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, r\}$. For this case, defining $t_j = |U| - r_j(U)$ and writing the system (5) for the dual matroids $M_1^*, \ldots, M_m^*$:

$$r_j^*(X) = r_j(U \setminus X) + |X| - r_j(U) \geq |U| - r_j(U), \quad j = 1, \ldots, m, \tag{10}$$

we notice that the complement $Y = U \setminus X$ to each minimal feasible solution X to (10) is a maximal set Y independent in all m matroids

$$r_j(Y) \geq |Y|, \quad j = 1, \ldots, m,$$

and vice versa. Thus, the set of all minimal feasible solutions to (10) can be identified with the family

$$\mathcal{I}(M_1, \ldots, M_m) = \{Y \ : \ Y \text{ maximal set independent in } M_1, \ldots, M_m\}.$$

The complexity of enumerating $\mathcal{I}(M_1, \ldots, M_m)$ was asked in 1980 by Lawler, Lenstra, and Rinnooy Kan [8] who gave an algorithm running in exponential time $O(n^{m+2})$ per each generated element. Theorem 4 indicates that in fact this enumeration problem (called *Matroid Intersections* in [8]) can be solved in incremental quasi-polynomial time.

Theorem 6 ([1]) *Given m matroids $M_1, \ldots, M_m$ on common ground set U, we can enumerate $k \leq |\mathcal{I}(M_1, \ldots, M_m)|$ maximal independent sets in $N^{o(\log N)}$ time and poly(N) calls to the independence oracles, where $N = \max\{m, k, |U|\}$.*

Example 6 (Packing flats in a matroid) In our final example, given a matroid M be on ground set U, subsets $A_1, \ldots, A_n \subseteq U$, and an integer threshold t, we consider the inequality

$$\sum_{i \in X} r(A_i) - r(\bigcup_{i \in X} A_i) \leq t, \tag{11}$$

where $X \subseteq \{1, \ldots, n\}$ and r is the rank function of M. It is easy to see that the left-hand side of (11) monotonically increases with X. We call maximal solutions to (11) *t-packings* of $A_1, \ldots, A_n$ in M. When $t = 0$ and $r(X) = |X|$, this definition leads to the usual notion of set packings, i.e. maximal pairwise disjoint subfamilies of $A_1, \ldots, A_n$. When $t = 0$ and $A_1, \ldots, A_n$ are some flats, for instance, some subspaces of a linear space, each packing is a maximal mutually transversal subfamily of flats. This is because for $t = 0$ the packing inequality (11) is equivalent to $|X|$ transversality conditions: for each $i \in X$ the flat A_i must be transversal to the flat generated by all other flats: $r(A_i \cup L_i) = r(A_i) + r(L_i)$, where $L_i = Span\langle A_{j \in X \setminus i} A_j \rangle$. In particular, when M is the cycle matroid of a graph G and $A_1, \ldots, A_n$ are subgraphs of G then for $t = 0$ each maximal packing correspond to a maximal pairwise *edge-disjoint* subfamilies of graphs the union of which does not contain any new cycle (i.e. a cycle that does not belong to one of the subgraphs $A_1, \ldots, A_n$).

Rewriting inequality (11) as

$$\sum_{i \in X} r(A_i) - r(\bigcup_{i \notin X} A_i) \geq \sum_{i=1}^{n} r(A_i) - t,$$

we note that the maximal packings in (11) are in one to one correspondence with the minimal feasible sets of a polymatroid inequality. Thus we arrive at the following result:

Corollary 2 *Given a matroid M on ground set U, and subsets $A_1, \ldots, A_n \subseteq U$, all maximal t-packings of $A_1, \ldots, A_n$ can be enumerated in incremental quasi-polynomial time, for any given integer threshold t.*

In particular, given a family of acyclic graphs on the same vertex set V, all maximal *edge-disjoint* subfamilies, the union of which is still acyclic, can be enumerated incrementally in quasi-polynomial time. In contrast to this result, a seemingly very similar problem is NP-hard:

Proposition 3 *Given a family of acyclic graphs on the same vertex set V, it is NP-hard to enumerate all maximal (not necessarily edge-disjoint) subfamilies, the union of which is still acyclic.*

Proof. We use the following reduction from the CNF satisfiability problem. Given a conjunctive normal form $\phi(x_1, \ldots, x_N) = D_1 \wedge \ldots \wedge D_m$, where each D_j is a disjunction of some literals in $\{x_1, \bar{x}_1, \ldots, x_N, \bar{x}_N\}$, our construction is composed of the union G of $N + m$ vertex disjoint cycles $C_1, \ldots, C_N, C'_1, \ldots, C'_m$, where $|C_i| = N + 2$ for $i = 1, \ldots, N$ and $|C'_j| = |D_j| + N$ for $j = 1, \ldots, m$. Each edge of G is labeled by one of the sets $\{x_i\}$, $\{\bar{x}_i\}$, or $\{x_i, \bar{x}_i\}$ for some $i \in \{1, \ldots, N\}$. Each cycle C_i, for $i = 1, \ldots, N$, corresponds to a binary variable x_i and its $N + 2$ edges are labeled respectively by $\{x_1, \bar{x}_1\}$, $\ldots$, $\{x_N, \bar{x}_N\}$, $\{x_i\}$, $\{\bar{x}_i\}$. Similarly, each cycle C'_j, for $j = 1, \ldots, m$, corresponds to a clause D_j and its edges are labeled by $\{x_1, \bar{x}_1\}$, $\ldots$, $\{x_N, \bar{x}_N\}$, $\{l_1\}, \ldots, \{l_{k_j}\}$, where $l_1, \ldots, l_{k_j}$ are the literals appearing in D_j. Finally we define $2N$ acyclic subgraphs $X_1, \overline{X}_1, \ldots, X_n, \overline{X}_n$ of G, where

$X_i = \{e \in E(G) \ : \ x_i \in \text{label}(e)\}$ and $\overline{X}_i = \{e \in E(G) \ : \ \bar{x}_i \in \text{label}(e)\}$. Note that, for any $j \in \{1, \ldots, N\}$, the family $\{X_i \ : \ i \neq j\} \cup \{\overline{X}_i \ : \ i \neq j\}$ is maximal with the property that the union graph is acyclic. Thus any other maximal family whose union is acyclic must contain either X_i or $\bar{X}_i$, for all $i = 1, \ldots, N$. Furthermore, any such family cannot contain both X_i and $\overline{X}_i$ for some $i \in \{1, \ldots, N\}$ since otherwise we get the cycle C_i in the union. We conclude therefore that there exists a new maximal union-acyclic subfamily if and only if there is a subfamily containing exactly one of the sets $X_i, \overline{X}_i$, for all $i = 1, \ldots, N$, such all the cycles $C'_1, \ldots, C'_m$ are broken in the union graph. The latter condition is further equivalent with the condition that CNF ϕ is satisfiable. $\square$

As a final remark, we note that the family of sets described in Proposition 3 is the family of maximal feasible solutions of the inequality

$$F(X) \stackrel{\text{def}}{=} |\bigcup_{i \in X} A_i| - r(\bigcup_{i \in X} A_i) \leq 0,$$

over $X \subseteq \{1, \ldots, n\}$. In the special case, when $n = |U|$ and the sets A_i are the n disjoint singletons of U, the function $F(X)$ reduces to the *co-polymatroid* (that is monotone, supermodular) function $f(X) \stackrel{\text{def}}{=} |X| - r(X)$. It follows by Corollary 1 that, for any integer t, the maximal feasible solutions of the inequality $f(X) \leq t$ can be enumerated in incremental polynomial time. It follows furthermore by Theorem 5 that the minimal feasible solutions of the inequality $f(X) \geq t$ can be enumerated with polynomial delay. In contrast, Propositions 2 and 3 state that the analogous problems for the function $F(X)$ (which is a parallel extension of $f(X)$) may be NP-hard. Thus while the parallel extension of a polymatroid function is polymatroid, the parallel extension of a co-polymatroid function maybe *neither* polymatroid *nor* co-polymatroid, and the corresponding generation problems may be NP-hard.

References

[1] E. Boros, K. Elbassioni, V. Gurvich and L. Khachiyan, Matroid intersections, polymatroid inequalities, and related problems, in: *Proc. 27th International Symposium on Mathematical Foundations of Computer Science, MFCS Warsaw, 2002.*

[2] Structural Rigidity, *Structural Topology* 1, pp. 26–45.

[3] J. Edmonds, Submodular functions, matroids, and certain polyhedra, in: *Combinatorial structures and their applications* (eds. R. Guy, H. Hanani, N. Sauer, , J. Shönheim), Gordon and Breach, 69-87.

[4] T. Eiter and G. Gottlob, Identifying the minimal transversals of a hypergraph and related problems, *SIAM J. Comput.*, 24 (1995) 1278-1304.

[5] V. Gurvich and L. Khachiyan, On generating the irredundant conjunctive and disjunctive normal forms of monotone Boolean functions, *Discrete Applied Mathematics*, 96-97 (1999) 363-373.

[6] T. Helgason, Aspects of the theory of hypermatroids, in Hypergraph Seminar, eds C. Berge and D.K. Ray-Chaudhuri), Lecture Notes in Math. 411 (1975) Springer, 191-214.

[7] R. M. Karp, On the complexity of combinatorial problems, *Networks* 5 (1975) 45-68.

[8] E. Lawler, J. K. Lenstra and A. H. G. Rinnooy Kan, Generating all maximal independent sets: NP-hardness and polynomial-time algorithms, *SIAM J. Comput.*, 9 (1980) 558-565.

[9] T. Lazarson, Independence functions in algebra, (Thesis), University of London (1957).

[10] A. Lehman, A solution of the Shannon switching game, *J. Soc. Indust. Appl. Math.* 12 (1964) 687-725.

[11] L. Lovász, Submodular functions and convexity, in *Mathematical Programming: The State of the Art*, Bonn 1982, pp. 235-257, (Springer Verlag, 1983).

[12] J. S. Provan and D. R. Shier, A paradigm for listing (s,t)-cuts in graphs, *Algorithmica*, 15(4) (1996) 357–372.

[13] R. C. Read and R. E. Tarjan, Bounds on backtrack algorithms for listing cycles, paths, and spanning trees, *Networks*, 5 (1975) 237-252.

[14] N. Robertson and P. D. Seymour, Graph minors. XIII. The disjoint path problem. *J. Comb. Th.*, Ser. B 63 (1995) 65-110.

[15] D.J.A. Welsh, Matroid Theory, Academic Press, London, New York, San Francisco, 1976.