A Parameterized View on Matroid Optimization Problems*

Dániel Marx
Department of Computer Science and Information Theory,
Budapest University of Technology and Economics
Budapest H-1521, Hungary
dmarx@cs.bme.hu

7th November 2007

Abstract

Matroid theory gives us powerful techniques for understanding combinatorial optimization problems and for designing polynomial-time algorithms. However, several natural matroid problems, such as 3-matroid intersection, are NP-hard. Here we investigate these problems from the parameterized complexity point of view: instead of the trivial $n^{O(k)}$ time brute force algorithm for finding a k-element solution, we try to give algorithms with uniformly polynomial (i.e., $f(k) \cdot n^{O(1)}$) running time. The main result is that if the ground set of a represented linear matroid is partitioned into blocks of size ℓ, then we can determine in randomized time $f(k, \ell) \cdot n^{O(1)}$ whether there is an independent set that is the union of k blocks. As consequence, algorithms with similar running time are obtained for other problems such as finding a k-element set in the intersection of ℓ matroids, or finding k terminals in a network such that each of them can be connected simultaneously to the source by ℓ disjoint paths.

1 Introduction

Many of the classical combinatorial optimization problems can be studied in the framework of matroid theory. The polynomial-time solvability of finding minimum weight spanning trees, finding perfect matchings in bipartite and general graphs, and certain connectivity problems all follow from the general algorithmic results on matroids.

Deciding whether there is an independent set of size k in the intersection of two matroids can be done in polynomial time, but the problem becomes NP-hard if we have to find a k-element set in the intersection of three matroids.

*Research partially supported by the Magyary Zoltán Felsőoktatási Közalapítvány and the Hungarian National Research Fund (Grant Number OTKA 67651).

Of course, the problem can be solved in $n^{O(k)}$ time by brute force, hence it is polynomial-time solvable for every fixed value of k. However, the running time is prohibitively large, even for small values of k (e.g., $k = 10$) and moderate values of n (e.g., $n = 1000$). In general, if k appears in the exponent of n in the running time, then the algorithm is usually too slow even for small values of k. The aim of parameterized complexity is to identify problems where the exponential increase of the running time can be restricted to some parameter k, thus the problem might be efficiently solvable for small values of k, even if n is large. A problem is called *fixed-parameter tractable* (FPT) if it has an algorithm with running time $f(k) \cdot n^{O(1)}$. Notice that here the exponent of n is independent of the parameter k, thus the running time depends polynomially on n and $f(k)$ can be considered as a constant factor for small values of k. There is a huge qualitative difference between running times such as $O(2^k \cdot n^2)$ and n^k: the former can be efficient even for, say, $k = 15$, while the latter has no chance of working. For more background and details on parameterized complexity, see Section 2 and [2, 3].

The question that we investigate in this paper is whether the NP-hard matroid optimization problems are fixed-parameter tractable if the parameter k is the size of the object that we are looking for. The most general result is the following:

Theorem 1.1 (Main). *Let $M(E, \mathcal{I})$ be a linear matroid where the ground set is partitioned into blocks of size ℓ. Given a linear representation A of M, it can be determined in $f(k, \ell) \cdot \|A\|^{O(1)}$ randomized time whether there is an independent set that is the union of k blocks. ($\|A\|$ denotes the length of A in the input.)*

Actually, our algorithm finds such an independent set, if it exists. Since it is easy to test whether a set is really independent in a linear matroid, the algorithm has only one-sided error: it cannot produce false positives.

For $\ell = 2$, this problem is exactly the so-called matroid parity problem: given a partition of the ground set into pairs, find an independent set of maximum size that contains 0 or 2 elements from each pair. A celebrated result of Lovász shows that matroid parity is polynomial-time solvable for linear matroids, if the linear representation is given in the input [6]. For $\ell \geq 3$, the problem is NP-hard: this can be shown by a reduction from the intersection problem of three matroids.

As applications of the main result, we show that the following problems are also solvable in randomized time $f(k, \ell) \cdot n^{O(1)}$. It is easy to see that these problems are polynomial-time solvable for every fixed value of k; the result states that there is such an algorithm where the exponent does not depend on k.

1. Given a family of subsets each of size at most ℓ, find k of them that are pairwise disjoint.
2. Given a graph G, find k (edge) disjoint triangles in G.
3. Given ℓ matroids over the same ground set, find a set of size k that is independent in each matroid.

4. Feedback Edge Set with Budget Vectors: given a graph with ℓ-dimensional cost vectors on the edges, find a feedback edge set of size at most k such that the total cost does not exceed a given vector C (see Section 5.3 for the precise definition).

5. Reliable Terminals: select k terminals and connect each of them to the source s with ℓ paths such that these $k \cdot \ell$ paths are pairwise disjoint.

The fixed-parameter tractability of the first two problems is well-known: they can be solved either with color coding or using representative systems [1, 9]. However, it is interesting to see that (randomized) fixed-parameter tractability can be obtained as a straightforward corollary of our results on matroids. We are not aware of any parameterized investigations of the last three problems. The algorithms presented in the paper are not practical, thus the results are of theoretical interest only. Therefore, determining exactly and optimizing the running time is not the focus of the paper. Nevertheless, as our techniques can be used to quickly show that certain problems are fixed-parameter tractable, we believe that it is a useful addition to the toolbox of parameterized complexity.

The algorithm behind the main result is inspired by the technique of representative systems introduced by Monien [9] (see also [11, 8] and [2, Section 8.2]). Iteratively for $i = 1, 2, \ldots, \ell$, we construct a collection $\mathcal{S}_i$ that contains independent sets arising as the union of i blocks (if there are such independent sets). The crucial observation is that it is sufficient to consider a subcollection of $\mathcal{S}_i$ whose size is at most a constant depending only on k and ℓ. In [8], this bound is obtained using Bollobás' Inequality. In our case, the bound can be obtained using a linear-algebraic generalization of Bollobás' Inequality due to Lovász [5, Theorem 4.8] (see also [4, Chapter 31, Lemma 3.2]). However, we need an algorithmic way of bounding the size of the $\mathcal{S}_i$'s, hence we do not state and use these inequalities here, but rather reproduce the proof of Lovász in a way that can be used in the algorithm (Lemma 4.2). The proof of this lemma is a simple application of multilinear algebra.

The algorithms that we obtain are randomized in the sense that they use random numbers and there is a small probability of not finding a solution even if it exists. The randomized nature of the algorithm comes from the fact that we rely on the Zippel-Schwartz Lemma in some of the operations involving matroid representations. Additionally, when working with representations over finite fields, then some of the algebraic operations are most conveniently done randomized. As the main result makes essential use of the Zippel-Schwartz Lemma (and hence is inherently randomized), we do not discuss whether these miscellaneous algebraic operations can be derandomized.

The paper is organized as follows. Section 2 summarizes the most important notions of parameterized complexity and matroid theory. (Some further definitions appear in Section 3.) Section 3 discusses how certain operations can be performed on the representations of matroids. Most of these constructions are either easy or folklore. The reason why we discuss them in detail is that we need these results in algorithmic form. The main result is presented in Section 4. In

Section 5, the randomized fixed-parameter tractability of certain problems are deduced as corollaries of the main result.

2 Preliminaries

This section briefly states the most important definitions of parameterized complexity, matroid theory, and randomized algorithms.

2.1 Parameterized Complexity

We follow [3] for the standard definitions of parameterized complexity. Let Σ be a finite alphabet. A decision problem is represented by a set $Q \subseteq \Sigma^*$ of strings over Σ. A *parameterization* of a problem is a polynomial-time computable function $\kappa : \Sigma^* \to \mathbb{N}$. A *parameterized decision problem* is a pair (Q, κ), where $Q \subseteq \Sigma^*$ is an arbitrary decision problem and κ is a parameterization. Intuitively, we can imagine a parameterized problem as a decision problem where each input instance $x \in \Sigma^*$ has a positive integer $\kappa(x)$ associated with it. A parameterized problem (Q, κ) is *fixed-parameter tractable (FPT)* if there is an algorithm that decides whether $x \in Q$ in time $f(\kappa(x)) \cdot |x|^c$ for some constant c and computable function f. An algorithm with such running time is called an *fpt-time algorithm* or simply *fpt-algorithm.* In a straightforward way, the theory can be extended to parameterization with more than one parameters. For example, we say that a problem is *FPT with combined parameters* κ_1, κ_2 if it has an algorithm with running time $f(\kappa_1(x), \kappa_2(x)) \cdot |x|^c$.

Many NP-hard problems were investigated in the parameterized complexity literature, with the goal of identifying fixed-parameter tractable problems. There is a powerful toolbox of techniques for designing fpt-algorithms: kernelization, bounded search trees, color coding, well-quasi ordering—just to name some of the more important ones. On the other hand, certain problems resisted every attempt at obtaining fpt-algorithms. Analogously to NP-completeness in classical complexity, the theory of W[1]-hardness can be used to give strong evidence that certain problems are unlikely to be fixed-parameter tractable. As the current paper does not contain any hardness result, we omit the details of W[1]-hardness theory; see [2, 3].

2.2 Matroids

A *matroid* $M(E, \mathcal{I})$ is defined by a *ground set* E and a collection $\mathcal{I} \subseteq 2^E$ of *independent sets* satisfying the following three properties:

(I1) $\emptyset \in \mathcal{I}$

(I2) If $X \subseteq Y$ and $Y \in \mathcal{I}$, then $X \in \mathcal{I}$.

(I3) If $X, Y \in \mathcal{I}$ and $|X| < |Y|$, then $\exists e \in Y \setminus X$ such that $X \cup \{e\} \in \mathcal{I}$.

An inclusionwise maximal set of $\mathcal{I}$ is called a *basis* of the matroid. It can be shown that the bases of a matroid all have the same size. This size is called the *rank* of the matroid M, and is denoted by $r(M)$. The rank $r(S)$ of a subset $S \subseteq E$ is the size of the largest independent set in S.

The definition of matroids was motivated by two classical examples. Let $G(V, E)$ be a graph, and let a subset $X \subseteq E$ of edges be independent if X does not contain any cycles. This results in a matroid, which is called the *cycle matroid* of G. The second example comes from linear algebra. Let A be a matrix over an arbitrary field F. Let E be the set of columns of A, and let $X \subseteq E$ be independent if these columns are linearly independent. The matroids that can be defined by such a construction are called *linear matroids,* and if a matroid can be defined by a matrix A over a field F, then we say that the matroid is *representable over* F. In this paper we consider only representable matroids, hence we assume that the matroids are given by a matrix A in the input. To avoid complications involving the representations of the elements in the matrix, we assume that F is either a finite field or the rationals. If F is a finite field with p^n elements, then we assume that elements of F are given as degree $n-1$ polynomials over $Z[p]$, and a degree n irreducible polynomial is also given in the input. We denote by $\|A\|$ the size of the representation A: the total number of bits required to describe all elements of the matrix.

2.3 Randomized Algorithms

Some of the algorithms presented in this paper are randomized, which means that they can produce incorrect answer, but the probability of doing so is small. More precisely, we assume that the algorithm has an integer parameter P given in unary, and the probability of incorrect answer is 2^{-P}. We say that an algorithm is randomized polynomial time if the running time can be bounded by a polynomial of the input size (which includes the unary description of P). It is easy to see that if an algorithm performs a polynomial number of operations, and each operation can be done in randomized polynomial time, then the whole algorithm is randomized polynomial time as well. Most of the randomized algorithms in this paper are based on the following lemma:

Lemma 2.1 (Zippel-Schwartz [13, 15]). *Let $p(x_1, \ldots, x_n)$ be a nonzero polynomial of degree d over some field F, and let S be an N element subset of F. If each x_i is independently assigned a value from S with uniform probability, then $p(x_1, \ldots, x_n) = 0$ with probability at most d/N.*

3 Representation Issues

The algorithm in Section 4 is based on algebraic manipulations, hence it requires that the matroid is given by a linear representation in the input. Therefore, in the proof of the main result and in its applications, we need algorithmic results on how to find representations for certain matroids, and if some operation is performed on a matroid, then how to obtain a representation of the result.

3.1 Dimension

The rank of a matroid represented by an $m \times n$ matrix is a most m: if the columns are m-dimensional vectors, then more than m of them cannot be independent. Conversely, every linear matroid of rank r has a representation with r rows:

Proposition 3.1. *Given a matroid M of rank r with a representation A over F, we can find in polynomial time a representation A' over F having r rows.*

Proof. Let r be the rank of the matroid M. By applying Gaussian elimination and possibly reordering the columns, it can be assumed that A is of the form

$$\begin{pmatrix} I_{r\times r} & B \\ 0 & 0 \end{pmatrix},$$

where $I_{r\times r}$ is the unit matrix of size $r \times r$, and B is a matrix of size $r \times (n-r)$. Clearly, only the first r rows of the representation have to be retained. Gaussian elimination requires a polynomial number of arithmetic operations. If F is a finite field, then it is clear that each arithmetic operation can be done in polynomial time. In the case when F is the rationals, the arithmetic operations are polynomial if the length of the elements remain polynomially bounded during every step of Gaussian elimination. We briefly sketch a possible argument to show that the length of the elements are of polynomial size. The row operations of Gaussian elimination can be interpreted as multiplying the matrix with a square matrix from the left. Gaussian elimination transforms the first r columns into a unit matrix, hence this square matrix is the inverse of the submatrix formed by the first r columns. The entries of this inverse matrix can be obtained as the ratio of a cofactor and the determinant, hence they are of polynomial length. Therefore, after Gaussian elimination terminates, the length of each entry is polynomially bounded. The argument can be tweaked to bound the length of the elements in the intermediate steps. □

3.2 Increasing the Size of the Field

The applications of Lemma 2.1 requires N to be large, so the probability of accidentally finding a root is small. However, N can be large only if the field F contains a sufficient number of elements. Therefore, if a matroid is given by a representation over some small field F, then we need a method of transforming this representation into a representation over a field F' having at least N elements.

Let $|F| = q$ and let $n = \lceil \log_q N \rceil$. We construct a field F' having $q^n \geq N$ elements. In order to do this, an irreducible polynomial $p(x)$ of degree n over F is required. Such a polynomial $p(x)$ can be found for example by the randomized algorithm of Shoup [14] in time polynomial in n and $\log q$. Now the ring of degree n polynomials over F modulo $p(x)$ is a field F' of size q^n. If a representation over F is given, then each element can be replaced by the corresponding degree 0 polynomial from F', which yields a representation over F'.

Proposition 3.2. *Let A be the representation of a matroid M over some field F. For every N, it is possible to construct a representation A' of M over some field F' with $|F'| \geq N$ in randomized time $(\|A\| \cdot \log N)^{O(1)}$.* □

3.3 Making the Field Finite

If a matroid is represented over the rationals, and we perform repeated operations on the representation, then the size of the rational elements can become very large, and it is not at all clear whether the size of the resulting representation is polynomially bounded in the original size. On the other hand, if the representation is over a finite field, then the size of the representation cannot increase above a certain size. Therefore, sometimes it is convenient to assume that the representation is over a finite field:

Proposition 3.3. *Given a matroid M with a representation A over the rationals, we can construct in randomized polynomial time a representation A' that is over some finite field F.*

Proof. Using Prop. 3.1, it can be assumed that A is of size $r \times n$, where r is the rank of the matroid. Multiplying by the product of the denominators, it can be assumed that the elements are integers (note that the length of the elements increase only polynomially). Let M be the maximum absolute value in the matrix, and let $N = 4r!M^r$. The determinant of an $r \times r$ submatrix is clearly between $-r!M^r$ and $r!M^r$, hence if we calculate the determinant of a submatrix with modulo p arithmetic where $p \geq N$, then we get the same value. It is not difficult to find a prime number p with $N \leq p \leq 2N$ in randomized polynomial time. Replacing each element with the corresponding element from the p-element field does not change which submatrices have nonzero determinants and hence does not change which set of columns are independent. □

3.4 Direct Sum

Let $M_1(E_1, \mathcal{I}_1)$ and $M_2(E_2, \mathcal{I}_2)$ be two matroids with $E_1 \cap E_2 = \emptyset$. The *direct sum* $M_1 \oplus M_2$ is a matroid over $E := E_1 \cup E_2$ such that $X \subseteq E$ is independent if and only if $X \cap E_1 \in \mathcal{I}_1$ and $X \cap E_2 \in \mathcal{I}_2$. If A_1 and A_2 are representations of the two matroids over the same field F, then it is easy to see that

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

is a representation of $M_1 \oplus M_2$. The construction can be generalized for the sum of more than two matroids, hence we have

Proposition 3.4. *Given representations of matroids $M_1, \ldots, M_k$ over the same field F, a representation of their direct sum can be found in polynomial time.* □

3.5 Uniform and Partition Matroids

The *uniform matroid* $U_{n,k}$ has an n-element ground set E, and a set $X \subseteq E$ is independent if and only if $|X| \leq k$. Every uniform matroid is linear and can be represented over the rationals by a $k \times n$ matrix where the element in the i-th column of j-th row is $i^{(j-1)}$. Clearly, no set of size larger than k can be independent in this representation, and every set of k columns is independent, as they form a Vandermonde matrix.

A *partition matroid* is given by a ground set E partitioned into k blocks E_1, $\ldots$, E_k, and by k integers a_1, $\ldots$, a_k. A set $X \subseteq E$ is independent if and only if $|X \cap E_i| \leq a_i$ holds for every $i = 1, \ldots, k$. As this partition matroid is the direct sum of uniform matroids $U_{|E_1|,a_1}$, $\ldots$, $U_{|E_k|,a_k}$, we have

Proposition 3.5. *A representation over the rationals of a partition matroid can be constructed in polynomial time.* □

3.6 Dual

The *dual* of a matroid $M(E, \mathcal{I})$ is a matroid $M^*(E, \mathcal{I}^*)$ over the same ground set where a set $B \subseteq E$ is a basis of M^* if and only if $E \setminus B$ is a basis of M.

Proposition 3.6. *Given a representation A of a matroid M, a representation of the dual matroid M^* can be found in polynomial time.*

Proof. Let r be the rank of the matroid M. By Prop. 3.1, it can be assumed that A is of the form $(I_{r\times r} \;\; B)$, where $I_{r\times r}$ is the unit matrix of size $r \times r$, and B is a matrix of size $r \times (n-r)$. Now the matrix $A^* = (B^\top \;\; I_{(n-r)\times(n-r)})$ represents the dual matroid M^*; see any text on matroid theory (e.g., [12]). □

3.7 Truncation

The *k-truncation* of a matroid $M(E, \mathcal{I})$ is a matroid $M'(E, \mathcal{I}')$ such that $S \subseteq E$ is independent in M' if and only if $|S| \leq k$ and S is independent in M.

Proposition 3.7. *Given a matroid M with a representation A over a finite field F and an integer k, a representation of the k-truncation M' can be found in randomized polynomial time.*

Proof. By Prop. 3.1 and 3.2, it can be assumed that A is of size $r \times n$ and the size of F is at least $N := 2^P \cdot kn^k$ (where P is the parameter describing the amount of error we tolerate, see Section 2.3). Let R be a random matrix of size $k \times r$, where each element is taken from F with uniform distribution. We claim that with high probability, the matroid M' represented by RA is the k-truncation of M. Since the $k \times m$ matrix RA cannot have more than k independent columns, all we have to show is that a k-element set is independent in M' if and only if it is independent in M. Let S be a set of size k, let A_0 be the $r \times k$ submatrix of A formed by the corresponding k columns, and let $B_0 = RA_0$ be the corresponding k columns in RA. If S is not independent in

M, (i.e., the columns of A_0 are not independent), then the columns of B_0 are not independent either. This means that S is not independent in the matroid M' represented by RA. Assume now that S is independent in M. The columns of A_0 are independent, thus $\det RA_0 \neq 0$ with positive probability (e.g., there is a matrix R such that RA_0 is the unit matrix). We use Lemma 2.1 to show that this probability is at least $1 - 2^{-P}/n^k$. The value $\det RA_0$ can be considered as a polynomial, with the kr elements of the matrix R being the variables. Since $\det RA_0$ is not always zero, the polynomial is not identically zero. As the degree of this polynomial is k, Lemma 2.1 ensures that $\det RA_0 = 0$ with probability at most $k/N = 2^{-P}/n^k$. Thus the probability that a particular k-element independent set of M is not independent in M' is at most $2^{-P}/n^k$. Matroid M has not more than n^k independent set of size k, hence the probability that M' is not the k-truncation of M is at most 2^{-P}. □

Given a matroid represented over the rationals, we can find a representation over a finite field in randomized polynomial time (Prop. 3.3) and then apply Prop. 3.8 to obtain the truncation. Thus we have:

Proposition 3.8. *Given a matroid M with a representation A over the rationals and an integer k, a representation of the k-truncation M' can be found in randomized polynomial time.* □

3.8 Deletion and Contraction

Let $M(E, \mathcal{I})$ be a matroid, and let X be a subset of E. *Deleting* X from M gives a matroid $M \setminus X = (E \setminus X, \mathcal{I}')$ such that $S \subseteq E \setminus X$ is independent in $M \setminus X$ if and only if S is independent in M. Given a representation of M, a representation of $M \setminus X$ can be obtained by deleting the columns corresponding to X.

Contracting the set X gives a matroid $M/X(E \setminus X, \mathcal{I}'')$ where $S \subseteq E \setminus X$ is independent if and only if $r(S \cup X) = |S| + r(X)$. Deletion and contraction are dual operations: if M^* is the dual of M, then $M^* \setminus X$ is the dual of M/X. Therefore, a representation of M/X can be obtained by finding a representation of the dual matroid M^* (using Prop. 3.6), deleting X, and taking the dual of the resulting matroid.

Proposition 3.9. *Given a matroid M over E with a representation A and a subset $X \subseteq E$, representations of the matroids $M \setminus X$ and M/X can be found in polynomial time.* □

3.9 Cycle Matroids

The cycle matroid of $G(V, E)$ can be represented over the 2-element field as follows. Consider the $|V| \times |E|$ incidence matrix of G, where the i-th element of the j-th row is 1 if and only if the i-th vertex is an endpoint of the j-th edge. If a set of edges form a cycle, then the sum of the corresponding columns is zero (mod 2), hence these columns are not independent. On the other hand, if some

columns are not independent, then these columns have a subset whose sum is zero. These columns form at least one cycle, which means that a set of columns is linearly independent if and only if the corresponding edges are acyclic.

Proposition 3.10. *Given a graph, a representation of the cycle matroid over the two element field can be constructed in polynomial time.* □

3.10 Transversal Matroids

Let $G(A, B; E)$ be a bipartite graph. The *transversal matroid* M of G has A as its ground set, and a subset $X \subseteq A$ is independent in M if and only if there is a matching that covers X. That is, X is independent if and only if there is an injective mapping $\phi : X \to B$ such that $\phi(v)$ is a neighbor of v for every $v \in X$.

Proposition 3.11. *Given a bipartite graph $G(A, B; E)$, a representation of its transversal matroid can be constructed in randomized polynomial time.*

Proof. Let R be a $|B| \times |A|$ matrix, where the i-th element in the j-th row is

- a random integer between 1 and $N := 2^P \cdot |A| \cdot 2^{|A|}$ if the i-th element of A and the j-th element of B are adjacent, and
- 0 otherwise.

We claim that with high probability, R represents the transversal matroid of M. Assume that a subset X of columns is independent. These columns have a $|X| \times |X|$ submatrix with nonzero determinant, hence there is at least one nonzero term in the expansion of this determinant. The nonzero term is a product of $|X|$ nonzero cells, and these cells define a matching covering X: they map each column in X to a distinct row.

Assume now that $X \subseteq A$ is independent in the transversal matroid: it can be matched with elements $Y \subseteq B$. This means that the determinant of the $|Y| \times |X|$ submatrix R_0 of R corresponding to X and Y has a term that is the product of nonzero elements. The determinant of R_0 can be considered as a polynomial of degree at most $|A|$, where the variables are the random elements of R_0. The polynomial has at most $|X||Y| \leq |A||B|$ variables and degree at most $|A|$. The existence of the matching and the corresponding nonzero term in the determinant shows that this polynomial is not identically zero. By Lemma 2.1, the probability that the determinant of R_0 is zero is at most $|A|/N = 2^{-P}/2^{|A|}$, implying that the columns X are independent with high probability. There are at most $2^{|A|}$ independent sets in M, thus the probability that not all of them are independent in the matroid represented by R is at most 2^{-P}. □

4 The Main Result

In this section we give a randomized fpt-algorithm for determining whether there are k blocks whose union is independent, if a matroid is given with a partition of the ground set into blocks of size ℓ. The idea is to construct for $i = 1, \ldots, k$

the collection $\mathcal{S}_i$ of all independent sets that arise as the union of i blocks. A solution exists if and only if $\mathcal{S}_k$ is not empty. It is not difficult to see that the set $\mathcal{S}_i$ can be constructed if $\mathcal{S}_{i-1}$ is already known. The problem is that the size of $\mathcal{S}_i$ can be as large as $n^{\Omega(i)}$, hence we cannot handle sets of this size in fpt-time. The crucial idea is that we retain only a constant size subcollection of each $\mathcal{S}_i$ in such a way that we do not throw away any sets essential for the solution. The property that this reduced collection has to satisfy is the following:

Definition 4.1. *Given a matroid $M(E,\mathcal{I})$ and a collection $\mathcal{S}$ of subsets of E, we say that a subcollection $\mathcal{S}^* \subseteq \mathcal{S}$ is* r-representative for $\mathcal{S}$ *if the following holds: for every set $Y \subseteq E$ of size at most r, if there is a set $X \in \mathcal{S}$ disjoint from Y with $X \cup Y \in \mathcal{I}$, then there is a set $X^* \in \mathcal{S}^*$ disjoint from Y with $X^* \cup Y \in \mathcal{I}$.*

That is, if some independent set in $\mathcal{S}$ can be extended to a larger independent set by r new elements, then there is a set in $\mathcal{S}^*$ that can be extended by the *same* r elements. 0-representative means that $\mathcal{S}^*$ is not empty if $\mathcal{S}$ is not empty. We use the following lemma to obtain a representative subcollection of constant size. The lemma is essentially the same as [5, Theorem 4.8] and [4, Chapter 31, Lemma 3.2] due to Lovász, but here it is presented in an algorithmic way.

Lemma 4.2. *Let M be a linear matroid of rank $r+s$, and let $\mathcal{S} = \{S_1, \ldots, S_m\}$ be a collection of independent sets, each of size s. If $|\mathcal{S}| > \binom{r+s}{s}$, then there is a set $S \in \mathcal{S}$ such that $\mathcal{S} \setminus \{S\}$ is r-representative for $\mathcal{S}$. Furthermore, given a representation A of M, we can find such a set S in $f(r,s) \cdot (\|A\|m)^{O(1)}$ time.*

Proof. Assume that M is represented by an $(r+s) \times n$ matrix A over some field F. Let E be the ground set of the matroid M, and for each element $e \in E$, let x_e be the corresponding $(r+s)$-dimensional column vector of A. Let $w_i = \bigwedge_{e \in S_i} x_e$, a vector in the exterior algebra of the linear space F^{r+s} (cf. [7, Sections 6-10]). As every w_i is the wedge product of s vectors, the w_i's span a space of dimension at most $\binom{r+s}{s}$. Therefore, if $|\mathcal{S}| > \binom{r+s}{s}$, then the w_i's are not independent. Thus it can be assumed that some vector w_k can be expressed as the linear combination of the other vectors.

We claim that if S_k is removed from $\mathcal{S}$, then the resulting subsystem is r-representative for $\mathcal{S}$. Assume that, on the contrary, there is a set Y of size at most r such that $S_k \cap Y = \emptyset$ and $S_k \cup Y$ is independent, but this does not hold for any other S_i with $i \neq k$. Let $y = \bigwedge_{e \in Y} x_e$. A crucial property of the wedge product is that the product of some vectors in F^{r+s} is zero if and only if they are not independent. Therefore, $w_k \wedge y \neq 0$, but $w_i \wedge y = 0$ for every $i \neq k$. However, w_k is the linear combination of the other w_i's, thus, by the multilinearity of the wedge product, $w_k \wedge y \neq 0$ is a linear combination of the values $w_i \wedge y = 0$ for $i \neq k$, which is a contradiction.

It is straightforward to make this proof algorithmic. First we determine the vectors w_i, then a vector w_k that is spanned by the other vectors can be found by standard techniques of linear algebra. Let us fix a basis of F^{r+s}, and express the vectors x_e as the linear combination of the basis vectors. The

vector w_i is the wedge product of s vectors, hence, using the multilinearity of the wedge product, each w_i can be expressed as the sum of $(r+s)^s$ terms. Each term is the wedge product of basis vectors of F^{r+s}; therefore, the antisymmetry property can be used to reduce each term to 0 or a basis vector of the exterior algebra. Thus we obtain each w_i as a linear combination of at most $\binom{r+s}{s}$ basis vectors. Now Gaussian elimination can be used to determine the rank of the subspace spanned by the w_i's, and to check whether the rank remains the same if one of the vectors is removed. If so, then the set corresponding to this vector can be removed from $\mathcal{S}$, and the resulting subsystem $\mathcal{S}^*$ is representative for $\mathcal{S}$. The running time of the algorithm can be bounded by a polynomial of the number m of vectors, the number of terms in the expression of a w_i (i.e., $(r+s)^s$), the dimension of the subspace spanned by the w_i's (i.e., $\binom{r+s}{s}$), and the size of the representation of M. Therefore, the running time is of the form $f(r,s) \cdot (\|A\|m)^{O(1)}$ for some function $f(r,s)$. □

Now we are ready to prove the main result:

of Theorem 1.1. First we obtain a representation A' for the $k\ell$-truncation of the matroid. By Prop 3.8, this can be done in time polynomial in $\|A\|$. Using A' instead of A does not change the answer to the problem, as we consider the independence of the union of at most k blocks. However, when invoking Lemma 4.2, it will be important that the elements are represented as $k\ell$-dimensional vectors.

For $i = 1, \ldots, k$, let $\mathcal{S}_i$ be the set system containing those independent sets that arise as the union of i blocks. Clearly, the task is to determine whether $\mathcal{S}_k$ is empty or not. For each i, we construct a subsystem $\mathcal{S}_i^* \subseteq \mathcal{S}_i$ that is $(k-i)\ell$-representative for $\mathcal{S}_i$. As $\mathcal{S}_k^*$ is 0-representative for $\mathcal{S}_k$, the emptiness of $\mathcal{S}_k$ can be checked by checking whether $\mathcal{S}_k^*$ is empty.

The set system $\mathcal{S}_1$ is easy to construct, hence we can take $\mathcal{S}_1^* = \mathcal{S}_1$. Assume now that we have a set system $\mathcal{S}_i^*$ as above. The set system $\mathcal{S}_{i+1}^*$ can be constructed as follows. First, if $|\mathcal{S}_i^*| > \binom{i\ell+(k-i)\ell}{i\ell} = \binom{k\ell}{i\ell}$, then by Lemma 4.2, we can throw away an element of $\mathcal{S}_i^*$ in such a way that $\mathcal{S}_i^*$ remains $(k-i)\ell$-representative for $\mathcal{S}_i$. Therefore, it can be assumed that $|\mathcal{S}_i^*| \leq \binom{k\ell}{i\ell}$. To obtain $\mathcal{S}_{i+1}^*$, we enumerate every set S in $\mathcal{S}_i^*$ and every block B, and if S and B are disjoint and $S \cup B$ is independent, then $S \cup B$ is put into $\mathcal{S}_{i+1}^*$. We claim that the resulting system is $(k-i-1)\ell$-representative for $\mathcal{S}_{i+1}$ provided that $\mathcal{S}_i^*$ is $(k-i)\ell$-representative for $\mathcal{S}_i$. Assume that there is a set $X \in \mathcal{S}_{i+1}$ and a set Y of size $(k-i-1)\ell$ such that $X \cap Y = \emptyset$ and $X \cup Y$ is independent. By definition, X is the union of $i+1$ blocks; let B be an arbitrary block of X. Let $X_0 = X \setminus B$ and $Y_0 = Y \cup B$. Now X_0 is in $\mathcal{S}_i$, and we have $X_0 \cap Y_0 = \emptyset$ and $X_0 \cup Y_0 = X \cup Y$ is independent. Therefore, there is a set $X_0^* \in \mathcal{S}_i^*$ with $X_0^* \cap Y_0 = \emptyset$ and $X_0^* \cup Y_0$ independent. This means that the independent set $X^* := X_0^* \cup B$ is put into $\mathcal{S}_{i+1}^*$, and it satisfies $X^* \cap Y = \emptyset$ and $X^* \cup Y$ independent.

When constructing the set system $\mathcal{S}_{i+1}^*$, the amount of work to be done is polynomial in $\|A'\|$ for each member S of $\mathcal{S}_i^*$. As discussed above, the size of each $\mathcal{S}_i^*$ can be bounded by $\binom{k\ell}{i\ell}$, thus the running time is $f(k,\ell) \cdot \|A'\|^{O(1)}$. □

We remark that the above algorithm actually finds a required independent set, if it exists: any member of $\mathcal{S}_k^*$ is a solution.

5 Applications

In this section we derive some consequences of the main result: we list problems that can be solved using the algorithm of Theorem 1.1.

5.1 Matroid Intersection

Given matroids $M_1(E, \mathcal{I}_1)$, ..., $M_\ell(E, \mathcal{I}_\ell)$ over a common ground set, their *intersection* is the set system $\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_\ell$. In general, the resulting set system is not a matroid, even for $\ell = 2$. Deciding whether there is a k-element set in the intersection of two matroids is polynomial-time solvable (cf. [12]), but NP-hard for more than two matroids. Here we show that the problem is randomized fixed-parameter tractable for a fixed number of represented matroids:

Theorem 5.1. *Let M_1, ..., M_ℓ be matroids with the same ground set E, given by their linear representations A_1, ..., A_ℓ over the same field F. We can decide in $f(k,\ell) \cdot (\sum_{i=1}^{\ell} \|A_i\|)^{O(1)}$ randomized time if there is a k-element set that is independent in every M_i.*

Proof. Let $E = \{e_1, \ldots, e_n\}$. We rename the elements of the matroids to make the ground sets pairwise disjoint: let $e_j^{(i)}$ be the copy of e_j in M_i. By Prop. 3.4, a representation of $M := M_1 \oplus \cdots \oplus M_\ell$ can be obtained in polynomial time. Partition the ground set of M into blocks of size ℓ: for $1 \leq j \leq n$, block B_j is $\{e_j^{(1)}, \ldots, e_j^{(\ell)}\}$. If M has an independent set that is the union of k blocks, then the corresponding k elements of E is independent in each of M_1, ..., M_ℓ. Conversely, if $X \subseteq E$ is independent in every matroid, then the union of the corresponding blocks is independent in M. Therefore, the algorithm of Theorem 1.1 answers the question. □

5.2 Disjoint Sets

Packing problems form a well-studied class of combinatorial optimization problems. Here we study the case when the objects to be packed are small:

Theorem 5.2. *Let $\mathcal{S} = \{S_1, \ldots, S_n\}$ be a collection of subsets of E, each of size at most ℓ. There is an $f(k,\ell) \cdot n^{O(1)}$ time randomized algorithm for deciding whether it is possible to select k pairwise disjoint subsets from $\mathcal{S}$.*

Proof. By adding dummy elements, it can be assumed that each S_i is of size exactly ℓ. Let $V = \{v_{i,j} : 1 \leq i \leq n, 1 \leq j \leq \ell\}$. We define a partition matroid over V as follows. For every element $e \in E$, let $V_e \subseteq V$ contain $v_{i,j}$ if and only if the j-th element of S_i is e. Clearly, the V_e's form a partition of V. Consider the partition matroid M where a set is independent if and only if it contains at most 1 element from each class of the partition. Let block B_i be

$\{v_{i,1}, \ldots, v_{i,\ell}\}$. If k pairwise disjoint sets can be selected from $\mathcal{S}$, then the union of the corresponding k blocks is independent in M as every element is contained in at most one of the selected sets. The converse is also true: if the union of k blocks is independent, then the corresponding k sets are disjoint, hence the result follows from Theorem 1.1. □

Theorem 5.2 immediately implies the existence of randomized fixed-parameter tractable algorithms for two well-know problems: Disjoint Triangles and Edge Disjoint Triangles. In these problems the task is to find, given a graph G and an integer k, a collection of k triangles that are pairwise (edge) disjoint. If E is the set of vertices (edges) of G, and the sets in $\mathcal{S}$ are the triangles of G, then it is clear that the algorithm of Theorem 5.2 solves the problem.

5.3 Feedback Edge Set with Budget Vectors

Given a graph $G(V, E)$, a *feedback edge set* is a subset X of edges such that $G(V, E \setminus X)$ is acyclic. If the edges of the graph are weighted, then finding a minimum weight feedback edge set is the same as finding a maximum weight spanning forest, which is well-known to be polynomial-time solvable. Here we study a generalization of the problem, where each edge has a vector of integer weights:

Feedback Edge Set with Budget Vectors	
Input:	A graph $G(V, E)$, a vector $\mathbf{x}_e \in [0, 1, \ldots, m]^\ell$ for each $e \in E$, a vector $C \in \mathbb{Z}_+^\ell$, and an integer k.
Parameter:	k, ℓ, m
Question:	Find a feedback edge set X of $\leq k$ edges such that $\sum_{e \in X} \mathbf{x}_e \leq C$.

That is, the cost of each edge has ℓ components, and we have to satisfy an upper bound on each component of the total cost. For $\ell = 1$, the we get the weighted version of Feedback Edge Set, which well-known to be solvable by a greedy algorithm. However, it can be shown that Feedback Edge Set with Budget Vectors is NP-hard. On the other hand, the problem is randomized fixed-parameter tractable with parameters k and ℓ:

Theorem 5.3. Feedback Edge Set with Budget Vectors *can be solved in* $f(k, \ell, m) \cdot n^{O(1)}$ *randomized time.*

Proof. It can be assumed that $k = |E| - |V| + c(G)$ (where $c(G)$ is the number of components of G): if k is smaller, then there is no solution; if k is larger, then it can be decreased without changing the problem. Let $M_0(E, \mathcal{I}_0)$ be the dual of the cycle matroid of G. The rank of M_0 is k, and a set X of k edges is a basis of M if and only if the complement of X is a spanning forest, i.e., X is a feedback edge set.

Let $C = [c_1, \ldots, c_\ell]$ and $n = |E|$. For $i = 1, \ldots, \ell$, let $M_i(E_i, \mathcal{I}_i)$ be the uniform matroid U_{nm,c_i}. By Props. 3.10, 3.2, 3.6, 3.5, and 3.4, a representation of the direct sum $M = M_0 \oplus M_1 \oplus \cdots \oplus M_k$ can be constructed in polynomial time. For each $e \in E$, let B_e be a block containing $e \in E$ and $x_e^{(i)}$ arbitrary elements of E_i for every $i = 1, \ldots, \ell$ (where $x_e^{(i)} \leq m$ denotes the i-th component of $\mathbf{x}_e$). Each set E_i contains nm elements, which is sufficiently large to make the blocks B_i disjoint. The size of each block is at most $\ell' := 1 + m\ell$. By adding dummy elements (elements that are independent from every subset of elements), we can ensure that the size of each block is exactly ℓ'. Hence the algorithm of Theorem 1.1 can be used to determine in randomized time $f(k, \ell') \cdot n^{O(1)}$ whether there is an independent set that is the union of k blocks. It is clear that every such independent set corresponds to a feedback edge set such that the total weight of the edges does not exceed C at any component. □

5.4 Reliable Terminals

In this section we give a randomized fixed-parameter tractable algorithm for a combinatorial problem motivated by network design applications.

Reliable Terminals	
Input:	A directed graph $D(V, A)$, a source vertex $s \in V$, a set $T \subseteq V \setminus \{s\}$ of possible terminals.
Parameter:	k, ℓ
Question:	Select k terminals $t_1, \ldots, t_k \in T$ and $k \cdot \ell$ internally vertex disjoint paths $P_{i,j}$ ($1 \leq i \leq k$, $1 \leq j \leq \ell$) such that path $P_{i,j}$ goes from s to t_i.

The problem models the situation when k terminals have to be selected that receive k different data streams (hence the paths going to different terminals should be disjoint due to capacity constraints) and each data stream is protected from $\ell - 1$ node failures (hence the ℓ paths of each data stream should be disjoint).

Let $D(V, A)$ be a directed graph, and let $S \subseteq V$ be a subset of vertices. We say that a subset $X \subseteq V$ is *linked to* S if there are $|X|$ vertex disjoint paths going from S to X. (Note that here we require that the paths are disjoint, not only internally disjoint. Furthermore, zero-length paths are also allowed if $X \cap S \neq \emptyset$.) A result due to Perfect shows that the set of linked vertices form a matroid:

Theorem 5.4 (Perfect [10]). *Let $D(V, A)$ be a directed graph, and let $S \subseteq V$ be a subset of vertices. The subsets that are linked to S form the independent sets of a matroid over V. Furthermore, a representation of this matroid can be obtained in randomized polynomial time.*

Proof. Let $V = \{v_1, \ldots, v_n\}$ and assume for convenience that no arc enters S. (Deleting these arcs does not change which sets are linked.) Let $G(U, W; E)$ be

a bipartite graph where a vertex $u_i \in U$ corresponds to each vertex $v_i \in V$, and a vertex $w_i \in W$ corresponds to each vertex $v_i \in V \setminus S$. For each $v_i \in V \setminus S$, there is an edge $w_i u_i \in E$, and for each $\overrightarrow{v_i v_j} \in A$, there is an edge $u_i w_j \in E$.

The size of a maximum matching in G is at most $|W| = n - |S|$. Furthermore, a matching of size $n - |S|$ can be obtained by taking the edges $u_i w_i$ for every $v_i \in V \setminus S$. Let $V_0 \subseteq V$ be a subset of size $|S|$, and let U_0 be the corresponding subset of U. We claim that V_0 is linked to S if and only G has a matching covering $U \setminus U_0$. Assume first that there are $|S|$ disjoint paths going from S to V_0. Consider the matching where $w_i \in W$ is matched to u_j if one of the paths enters v_i from v_j, and w_i is matched to u_i otherwise. This means that u_i is matched if one of the paths reaches v_i and continues further on, or if none of the paths reaches v_i. Thus the unmatched u_i's corresponds to the end points of the paths, as required.

To see the other direction, consider a matching covering $U \setminus U_0$. As $|U \setminus U_0| = n - |S|$, this is only possible if the matching fully covers W. Let v_{i_1} be a vertex of $S \setminus U_0$. Let w_{i_2} be the pair of u_{i_1} in the matching, let w_{i_3} be the pair of u_{i_2}, etc. We can continue this until a vertex u_{i_k} is found that is not covered in the matching. Now $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ is a path going from S to $v_{i_k} \in V_0$. If this procedure is repeated for every vertex of S, then we obtain $|S|$ paths that are pairwise disjoint, and each of them ends in a vertex of V_0. This completes the proof of the claim that V_0 is linked if and only if G has a matching covering $U \setminus U_0$.

If X is linked to S, then X can be extended to a linked set of size exactly $|S|$ by adding vertices of S to it (as they are connected to S by zero-length paths). The observation above shows that linked sets of size $|S|$ are exactly the bases of the dual of the transversal matroid of G, which means that the linked sets are exactly the independent sets of this matroid. By Props. 3.11 and 3.6, a representation of this matroid can be constructed in randomized polynomial time. □

Theorem 5.5. Reliable Terminals *is solvable in* $f(k,\ell) \cdot n^{O(1)}$ *randomized time.*

Proof. Let us replace the vertex s with $k \cdot \ell$ independent vertices $S = \{s_1, \ldots, s_{k\ell}\}$ such that each new vertex has the same neighborhood as s. Similarly, each $t \in T$ is replaced with ℓ vertices $t^{(1)}, \ldots, t^{(\ell)}$, but now we remove every outgoing edge from $t^{(2)}, \ldots, t^{(\ell)}$. (Note that the outgoing edges of $t^{(1)}$ are preserved.) Denote by D' the new graph. It is easy to see that a set of terminals $t_1, \ldots, t_k$ form a solution for the Reliable Terminals problem if and only if the set $\{t_i^{(j)} : 1 \leq i \leq k, 1 \leq j \leq \ell\}$ is linked to S in D'. Using Theorem 5.4, we can construct a representation of the matroid whose independent sets are exactly the sets linked to S in D'. Delete the columns that do not correspond to vertices in T, hence the ground set of the matroid has $\ell|T|$ elements. Partition the ground set into blocks of size ℓ: for every $t \in T$, there is a block $B_t = \{t^{(1)}, \ldots, t^{(\ell)}\}$. Clearly, the Reliable Terminals problem has a solution if and only if the matroid has an independent set that is the union of k blocks.

Therefore, Theorem 1.1 can be used to solve the problem. □

Acknowledgments

I'm grateful to Lajos Rónyai for his useful comments on the paper.

References

[1] N. Alon, R. Yuster, and U. Zwick. Finding and counting given length cycles. *Algorithmica*, 17(3):209–223, 1997.

[2] R. G. Downey and M. R. Fellows. *Parameterized Complexity*. Monographs in Computer Science. Springer-Verlag, New York, 1999.

[3] J. Flum and M. Grohe. *Parameterized Complexity Theory*. Springer-Verlag, Berlin, 2006.

[4] R. L. Graham, M. Grötschel, and L. Lovász, editors. *Handbook of combinatorics. Vol. 1, 2*. Elsevier Science B.V., Amsterdam, 1995.

[5] L. Lovász. Flats in matroids and geometric graphs. In *Combinatorial surveys (Proc. Sixth British Combinatorial Conf., Royal Holloway Coll., Egham, 1977)*, pages 45–86. Academic Press, London, 1977.

[6] L. Lovász. Matroid matching and some applications. *J. Combin. Theory Ser. B*, 28(2):208–236, 1980.

[7] S. Mac Lane and G. Birkhoff. *Algebra*. Chelsea Publishing Co., New York, third edition, 1988.

[8] D. Marx. Parameterized coloring problems on chordal graphs. *Theoret. Comput. Sci.*, 351(3):407–424, 2006.

[9] B. Monien. How to find long paths efficiently. In *Analysis and design of algorithms for combinatorial problems (Udine, 1982)*, volume 109 of *North-Holland Math. Stud.*, pages 239–254. North-Holland, Amsterdam, 1985.

[10] H. Perfect. Applications of Menger's graph theorem. *J. Math. Anal. Appl.*, 22:96–111, 1968.

[11] J. Plehn and B. Voigt. Finding minimally weighted subgraphs. In *Graph-theoretic concepts in computer science (Berlin, 1990)*, volume 484 of *Lecture Notes in Comput. Sci.*, pages 18–29. Springer, Berlin, 1991.

[12] A. Recski. *Matroid theory and its applications in electric network theory and statics*, volume 6 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, New York and Akadémiai Kiadó, Budapest, 1989.

[13] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.*, 27(4):701–717, 1980.

[14] V. Shoup. Fast construction of irreducible polynomials over finite fields. *J. Symbolic Comput.*, 17(5):371–391, 1994.

[15] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 216–226. Springer, Berlin, 1979.