Computing representations of matroids of bounded branch-width

Daniel Král'*

Abstract

For every $k \geq 1$ and two finite fields $\mathbb{F}$ and $\mathbb{F}'$, we design a polynomial-time algorithm that given a matroid $\mathcal{M}$ of branch-width at most k represented over $\mathbb{F}$ decides whether $\mathcal{M}$ is representable over $\mathbb{F}'$ and if so, it computes a representation of $\mathcal{M}$ over $\mathbb{F}'$. The algorithm also counts the number of non-isomorphic representations of $\mathcal{M}$ over $\mathbb{F}'$. Moreover, it can be modified to list all such non-isomorphic representations.

1 Introduction

Algorithmic matroid theory has attracted recently a lot of attention of researchers in particular in the area of algorithm for matroids with small width. Matroids are combinatorial structures that generalize the notions of graphs and linear independence of vectors. Similarly, as in the case of graphs, some hard problems (that cannot be solved in polynomial time for general matroids) can be efficiently solved for (representable) matroids of small width. Though the notion of tree-width generalizes to matroids [14], a more natural width parameter for matroids is the notion of *branch-width*. Let us postpone a formal definition of this width parameter to Section 2 and just mention at this point that the branch-width of matroids is linearly related with their tree-width, in particular, the branch-width of a graphic matroid is bounded by twice the tree-width of the corresponding graph.

*Institute for Theoretical Computer Science (ITI), Faculty of Mathematics and Physics, Charles University, Malostranské náměstí 25, 118 00 Prague, Czech Republic. E-mail: kral@kam.mff.cuni.cz. Institute for Theoretical Computer Science is supported by the Ministry of Education of the Czech Republic as project 1M0545.

The results obtained so far suggest that the algorithmic results generalize from graphs to matroids representable over finite fields but not to matroids that can be represented only over an infinite field or which are not representable at all. This is consistent with the structural results on matroids [5–9] that also suggest that matroids representable over finite fields are close to graphic matroids (and thus graphs) but general matroids can be quite different.

In the global perspective, one would like to be able for a matroid (with or without its representation) to decide whether it has a bounded branch-width, whether it is representable over a particular finite field and to compute one of its (possibly more) representations. In particular, the following problems naturally arise in this area:

1. Is it possible for $k \geq 1$ to decide in polynomial time whether a branch-width of a given matroid $\mathcal{M}$ is bounded by k and, if so, to find a branch-decomposition of $\mathcal{M}$ of small branch-width?

2. Is it possible for a field $\mathbb{F}$ and $k \geq 1$ to decide in polynomial time whether a matroid of branch-width at most k is representable over $\mathbb{F}$?

3. What problems (otherwise intractable) are polynomial-time solvable for matroids representable over finite fields that have bounded branch-width?

Another issue is how the matroid $\mathcal{M}$ is presented to an algorithm: it can be given as represented by an *oracle*, which is simply a function that for a given subset of elements of $\mathcal{M}$ determines whether it is independent, or by a representation over a field $\mathbb{F}$ which can be either finite or infinite (see Section 2 for more details on matroid representations). The complexity of algorithms for matroids is measured in terms of the number n of elements of an input matroid.

Let us now survey the status of the problems mentioned in the previous paragraph. The first problem is solved in a very satisfactory way: Oum and Seymour [15, 16] constructed for fixed $k \geq 1$ an $O(n^4)$-algorithm which computes a branch decomposition of an oracle-given matroid with width at most $3k-1$ or certifies that the branch-width of the input matroid is greater than k. Moreover, for fixed $k \geq 1$ and a fixed finite field $\mathbb{F}$, it can be tested in polynomial-time whether a branch-width of a matroid represented over $\mathbb{F}$ is at most k [11] and an optimal branch decomposition can be constructed. Since it is possible to compute a good branch decomposition (if it exists) of any matroid in polynomial time, we can always assume that the matroid is presented with its decomposition.

Let us now focus on the status of the second problem. Seymour [20] showed that there is no sub-exponential algorithm to test whether an oracle-given matroid is binary, i.e., representable over GF(2). His result straightforwardly generalize to any finite field and holds even if the input matroid has a bounded branch-width. On the other hand, if the matroid is represented over rationals $\mathbb{Q}$, it can be tested in polynomial-time whether it is binary [19]. Since it is well-known that if a matroid is binary, it has a unique representation over GF(2) and it is easy to find such a representation, we conclude that the answer to the second question is positive for $\mathbb{F} = \mathrm{GF}(2)$ even if the branch-width of $\mathcal{M}$ is not restricted. On the other, for every finite field $\mathbb{F} \neq \mathrm{GF}(2), \mathrm{GF}(3)$ and every $k \geq 3$, the problem is NP-hard [13] for matroids with branch-width at most k.

A general answer to the third problem for matroids represented over finite fields was given in [10, 12]: all MSOL-definable[1] properties can be tested in polynomial time for matroids represented over a fixed finite field with bounded branch-width. These result match analogous results [1–4] for graphs.

A property that can be defined in MSOL is whether a given matroid is representable over a fixed finite field. Hence, the answer to the first half of the second question is positive if the matroid is given by its representation over a *finite* field (note that the answer is negative if the matroid is given by an oracle or by its representation over $\mathbb{Q}$ as we explained earlier). Another way how to see that a representatibility over a fixed finite field $\mathbb{F}$ can be solved in polynomial time for matroids represented over another fixed finite field $\mathbb{F}'$ is to realize that the class of matroids representable over $\mathbb{F}$ is minor-closed and the matroids representable over $\mathbb{F}'$ with bounded branch-width are well-quasi-ordered [9]. Note that it is still open whether for every finite field $\mathbb{F}$, there exists a finite set of forbidden minors for $\mathbb{F}$-representatibility (a famous conjecture of Rota [18] asserts this to be the case).

The aim of this note is to provide the answer for the other half of the second question in case that the input matroid is represented over a finite field $\mathbb{F}$. In particular, we show that there is a polynomial-time algorithm that for fixed finite fields $\mathbb{F}$ and $\mathbb{F}'$ and a fixed integer $k \geq 1$ decides whether a given matroid $\mathcal{M}$ represented over $\mathbb{F}$ with branch-width at most k can be represented over $\mathbb{F}'$ and if so, it finds its representation over $\mathbb{F}'$. Our algorithm

[1] MSOL stands for monadic second-order logic.

can be modified to compute the number of non-isomorphic representations of $\mathcal{M}$ over $\mathbb{F}'$ and to list all such non-isomorphic representations.

The algorithm is divided into two steps—in the first step, we compute certain auxiliary bipartite graphs that fully determine the structure of a given matroid. This is the only place where a representation of $\mathcal{M}$ over $\mathbb{F}$ is used. In the second step, we use the auxiliary graphs capturing the structure of $\mathcal{M}$ to verify the existence and in the positive case to construct a representation of $\mathcal{M}$ over $\mathbb{F}'$. Our algorithm similarly as algorithms of [10–12] implicitly involves rooted configurations as introduced in [9], and "structural finiteness" on cuts represented in the branch decomposition.

2 Definitions

In this section, we formally introduce all the notions used throughout the paper. We also refer the reader to the monographs [17, 21] for further exposition on matroids. A *matroid* $\mathcal{M}$ is a pair $(X, \mathcal{I})$ where $\mathcal{I} \subseteq 2^X$. The elements of X are called *elements* of $\mathcal{M}$ and the sets contained in $\mathcal{I}$ are called *independent* sets. The set $\mathcal{I}$ is required to contain the empty set, to be hereditary, i.e., for every $X' \in \mathcal{I}$, $\mathcal{I}$ must contain all subsets of X', and to satisfy the exchange axiom: if X' and X'' are two sets of $\mathcal{I}$ such that $|X'| < |X''|$, then there exists $x \in X''$ such that $X' \cup \{x\} \in \mathcal{I}$. The *rank* of a set X', denoted by $\operatorname{rank} X'$, is the size of the largest independent subset of X' (it can be inferred from the exchange axiom that all inclusion-wise maximal independent subsets of $\mathcal{M}$ have the same size). In the rest, we often understand matroids as sets of elements equipped with a property of "being independent". Consistently with this view, $|\mathcal{M}|$ denotes the number of elements of $\mathcal{M}$ and $\operatorname{rank} \mathcal{M}$ denotes the size of the largest independent set of $\mathcal{M}$.

Let us now introduce further notation related to matroids. If X' is a set of elements of $\mathcal{M}$, then $\mathcal{M} \setminus X'$ is the matroid obtained from $\mathcal{M}$ by *deleting* the elements of X', i.e., the elements of $\mathcal{M} \setminus X'$ are those not contained in X' and a subset X'' of such elements is independent in the matroid $\mathcal{M} \setminus X'$ if and only if X'' is independent in $\mathcal{M}$. The matroid $\mathcal{M}/X'$ which is obtained by *contraction* of X' is the following matroid: the elements of $\mathcal{M}/X'$ are those not contained in X' and a subset X'' of such elements is independent in $\mathcal{M}/X'$ if and only if $X' \cup X''$ is independent in $\mathcal{M}$. Finally, a *loop* of $\mathcal{M}$ is an element e of $\mathcal{M}$ such that $\operatorname{rank} \{e\} = 0$ and a *bridge* is an element such that $\operatorname{rank} \mathcal{M} \setminus \{e\} = \operatorname{rank} \mathcal{M} - 1$. A *separation* (A, B) is a partition of the elements of $\mathcal{M}$ into two disjoint sets and a separation is called a *k-separation* if $\operatorname{rank} A + \operatorname{rank} B = \operatorname{rank} \mathcal{M} + k$.

As mentioned in Introduction, matroids generalize the notion of linear independence of vectors. If $\mathbb{F}$ is a (finite or infinite) field, a mapping $\varphi : \mathcal{M} \to \mathbb{F}^d$ from the element set of $\mathcal{M}$ to a d-dimensional vector space over $\mathbb{F}$ is a *representation* of $\mathcal{M}$ if a set $\{e_1, \dots, e_k\}$ of elements of $\mathcal{M}$ is independent in $\mathcal{M}$ if and only if $\varphi(e_1), \dots, \varphi(e_k)$ are linearly independent vectors in $\mathbb{F}^d$. For a subset X of the elements of $\mathcal{M}$, $\varphi(X)$ denotes the linear subspace of $\mathbb{F}^d$ generated by the images of the elements of X. In particular, $\dim \varphi(X) = \operatorname{rank} X$. Two representations φ_1 and φ_2 of $\mathcal{M}$ are isomorphic if there exists an isomorphism ψ of vector spaces $\varphi_1(\mathcal{M})$ and $\varphi_2(\mathcal{M})$ such that $\psi(\varphi_1(e))$ is a non-zero multiple of $\varphi_2(e)$ for every element e of $\mathcal{M}$. Next, we introduce additional notation for vector spaces over a field $\mathbb{F}$. If U_1 and U_2 are two linear subspaces of a vector space over $\mathbb{F}$, $U_1 \cap U_2$ is the linear space formed by all the vectors lying in both U_1 and U_2, and $\overline{U_1 \cup U_2}$ is the linear space formed by all the linear combinations of the vectors of U_1 and U_2, i.e., the linear hull of $U_1 \cup U_2$.

A *branch decomposition* of a matroid $\mathcal{M}$ is a tree with all inner vertices of degree three and the leaves corresponding to the elements of $\mathcal{M}$. Each edge e of the tree naturally splits the elements of $\mathcal{M}$ into two disjoint subsets X_1^e and X_2^e (the elements of each subset correspond to the leaves of the two subtrees obtained by removing e). The *width* of the branch decomposition is the maximum over all e of $\operatorname{rank} X_1^e + \operatorname{rank} X_2^e - \operatorname{rank} \mathcal{M}$. If φ is a representation of $\mathcal{M}$ over a field $\mathbb{F}$, the width of the branch decomposition is also equal to the maximum of $\dim \varphi(X_1^e) \cap \varphi(X_2^e)$ taken over all the edges e of the tree. The *branch-width* of a matroid $\mathcal{M}$ is the smallest width of a branch decomposition of $\mathcal{M}$.

In our considerations, it turns out to be useful to consider rooted branch decompositions of $\mathcal{M}$. A *rooted branch decomposition* of $\mathcal{M}$ is obtained from a branch decomposition of $\mathcal{M}$ by subdividing one of the edges of the tree and introducing a new vertex of degree one adjacent to the obtained vertex of degree two. We now root the tree at the new vertex of degree one and add a new element e_0 to $\mathcal{M}$. The element e_0 is a loop and is associated with the root of the tree. Throughout the paper, the vertices of the tree forming the rooted branch decomposition are referred as *nodes*, nodes of degree one different from the root are *leaves* and those of degree three are *inner nodes.* Note that each inner node has two children and a unique parent. Let us remark that adding a loop to $\mathcal{M}$ does not change any properties of $\mathcal{M}$ that we are interested in, in particular, the branch-width of $\mathcal{M}$ is preserved as well as its representatibility over any particular field $\mathbb{F}$.

3 Structural observations

In this section, we establish some properties of matroids of bounded branch-width that can be represented over a finite field. We start with a lemma that has been implicitly used in most of algorithms for matroids of bounded branch-width, e.g., in those computing the Tutte polynomial. Since the proof of this lemma is a simple application of basic linear algebra facts, we decided to leave it to the reader.

Lemma 1. *Let (A, B) be a separation of a matroid $\mathcal{M}$ and let $\varphi : \mathcal{M} \to \mathbb{F}^d$, $d = \operatorname{rank} \mathcal{M}$, be a representation of $\mathcal{M}$ over a field $\mathbb{F}$. Let further C be the linear subspace $\varphi(A) \cap \varphi(B)$. For every subsets $A' \subseteq A$ and $B' \subseteq B$, the following holds:*

$$\begin{aligned}\operatorname{rank} A' \cup B' \quad = \quad & (\dim \varphi(A') - \dim \varphi(A') \cap C) + \\ & (\dim \varphi(B') - \dim \varphi(B') \cap C) + \\ & \dim \overline{(\varphi(A') \cap C) \cup (\varphi(B') \cap C)}\ .\end{aligned}$$

If (A, B) is a separation of a matroid $\mathcal{M}$, we say that subsets $A_1, A_2 \subseteq A$ are *B-indistinguishable* if for every $B' \subseteq B$,

$$\operatorname{rank} B' \cup A_1 - \operatorname{rank} A_1 = \operatorname{rank} B' \cup A_2 - \operatorname{rank} A_2\ .$$

Note that subsets A_1 and A_2 are B-indistinguishable if and only if the identity on the elements of B is an isomorphism between the matroids $(\mathcal{M}/A_1) \setminus (A \setminus A_1)$ and $(\mathcal{M}/A_2) \setminus (A \setminus A_2)$. Also note that the relation of being B-indistinguishable is an equivalence relation and thus we can talk about *classes* of B-indistinguishable subsets of A.

If the matroid M has a representation $\varphi : \mathcal{M} \to \mathbb{F}^d$ over a field $\mathbb{F}$, Lemma 1 says that two subsets A_1 and A_2 are B-indistinguishable if for every subset $B' \subset B$,

$$\dim \overline{(\varphi(B') \cap C) \cup (\varphi(A_1) \cap C)} = \dim \overline{(\varphi(B') \cap C) \cup (\varphi(A_2) \cap C)}$$

where $C = \varphi(A) \cap \varphi(B)$. In particular, if $\varphi(A_1) \cap C = \varphi(A_2) \cap C$, the subsets A_1 and A_2 are B-indistinguishable, but the converse need not to be true. If $|\mathbb{F}|$ is a finite field and C has dimension k, i.e., (A, B) is a k-separation, there are at most $|\mathbb{F}|^{k^2}$ possible linear subspaces $\varphi(A_i) \cap C$ and thus the following holds:

Lemma 2. *Let (A, B) be a k-separation of a matroid $\mathcal{M}$ that is representable over a finite field $\mathbb{F}$. There are at most $|\mathbb{F}|^{k^2}$ B-indistinguishable subsets of A.*

4 Algorithm

In this section, we describe our algorithm for computing representations matroids with bounded branch-width over finite fields. The input of the algorithm consists of a rooted branch decomposition with width k of a matroid $\mathcal{M}$ together with its representation $\varphi : \mathcal{M} \to \mathbb{F}^d$, $d = \operatorname{rank} \mathcal{M}$, over a finite field $\mathbb{F}$. We assume throughout this section that $\mathcal{M}$ contains no loops except for the one corresponding to the root of the decomposition. This clearly does not decrease the generality of our results since the loops are always represented by the zero vectors.

As the first step, we compute for each inner node u_0 of the decomposition an auxiliary complete bipartite graph G_{u_0} that determines the mutual relation between two parts of the matroid corresponding to the subtrees of the left and right child of u_0. We explain the structure of the graphs G_{u_0} in more detail in Subsection 4.1 where we also discuss how the graphs are constructed. In Subsection 4.2, we show how to obtain a representation of $\mathcal{M}$ over any finite field $\mathbb{F}'$ (if it exists) with the aid of the constructed auxiliary graphs. Throughout this section, we write A_{u_0} for the set of the elements of $\mathcal{M}$ corresponding to the leaves of the subtree of u_0 in the decomposition and B_{u_0} for the elements of $\mathcal{M}$ not contained in this subtree.

4.1 Computing auxiliary graphs

Fix an inner node u_0 of the decomposition and let u_1 and u_2 be its two children. One part of the auxiliary bipartite graph G_{u_0} is formed by vertices corresponding to the classes of B_{u_1}-indistinguishable subsets of A_{u_1} and the other by vertices corresponding to the classes of B_{u_2}-indistinguishable subsets of A_{u_2}. If $A'_1 \subseteq A_{u_1}$ and $A'_2 \subseteq A_{u_2}$, the edge joining the vertices of G_{u_0} that correspond to the classes containing A'_1 and A'_2 is labeled with

$$\operatorname{rank} A'_1 + \operatorname{rank} A'_2 - \operatorname{rank} A'_1 \cup A'_2 \tag{1}$$

By the definitions of B_{u_1}-indistinguishability and B_{u_2}-indistinguishability, the value of (1) does not depend on the choice of subsets A'_1 and A'_2 in the two classes. The edge between the classes containing A'_1 and A'_2 is further associated with the vertex of the graph $G_{u'}$, where u' is the parent of u, that corresponds to the class of B_{u_0}-indistinguishable sets that contains $A_1' \cup A_2'$. Note that a single vertex of $G_{u'}$ can be (and usually is) associated with several different edges of G_{u_0}.

We now turn our attention to the actual computation of the auxiliary graphs G_{u_0}. We first find for every node u_0 the list $\mathcal{L}^A_{u_0}$ of all linear subspaces of $\varphi(A_{u_0}) \cap \varphi(B_{u_0})$ that are equal to $\varphi(A') \cap \varphi(B_{u_0})$ for some $A' \subseteq A_{u_0}$. Let us describe this process in more detail. If u_0 is a leaf of the decomposition and the element e associated with it is a bridge of $\mathcal{M}$, the list $\mathcal{L}^A_{u_0}$ consists only of the zero subspace. If e is not a bridge, then the list $\mathcal{L}^A_{u_0}$ consists of the zero subspace and the linear subspace $\varphi(\{e\})$. If u_0 is an inner node with two children u_1 and u_2, then the list $\mathcal{L}^A_{u_0}$ is formed by all the linear subspaces equal to $\overline{U_1 \cup U_2} \cap \varphi(B_{u_0})$ for some $U_1 \in \mathcal{L}^A_{u_1}$ and $U_2 \in \mathcal{L}^A_{u_2}$. Since the lists $\mathcal{L}^A_{u_0}$ are formed by linear subspaces of a k-dimensional linear space over $\mathbb{F}$, $|\mathcal{L}^A_{u_0}| \leq |\mathbb{F}|^{k^2}$. Hence, the sizes of the lists $\mathcal{L}^A_{u_0}$ are bounded by a function of $\mathbb{F}$ and k only and we only perform a constant number of operations with linear subspaces over $\mathbb{F}$ for each node u_0 (if the field $\mathbb{F}$ and the branch-width k are fixed). Analogously, we can find the lists $\mathcal{L}^B_{u_0}$ of all linear subspaces equal to $\varphi(B') \cap \varphi(A_{u_0})$ for some $B' \subseteq B_{u_0}$.

Our next goal is to recognize B_{u_0}-indistinguishable sets. By the definition of B_{u_0}-indistinguishability, if two different subsets $A_1, A_2 \subseteq A_{u_0}$ correspond to the same set of $\mathcal{L}^A_{u_0}$, i.e.,

$$\varphi(A_1) \cap \varphi(B_{u_0}) = \varphi(A_2) \cap \varphi(B_{u_0}) = U \in \mathcal{L}^A_{u_0} ,$$

then the sets A_1 and A_2 are B_{u_0}-indistinguishable. The converse need not to be true. Still, we can now efficiently test whether two sets A_1 and A_2 are B_{u_0}-indistinguishable as follows: let $U_1 = \varphi(A_1) \cap \varphi(B_{u_0}) \in \mathcal{L}^A_{u_0}$ and $U_2 = \varphi(A_2) \cap \varphi(B_{u_0}) \in \mathcal{L}^A_{u_0}$. The sets A_1 and A_2 are B_{u_0}-indistinguishable if and only if

$$\dim \overline{U_1 \cup U} = \dim \overline{U_2 \cup U} \tag{2}$$

for every $U \in \mathcal{L}^B_{u_0}$. This condition can be efficiently tested since the size of $\mathcal{L}^B_{u_0}$ is bounded by a function of $\mathbb{F}$ and k. Hence, we can partition the list $\mathcal{L}^A_{u_0}$ into classes of linear subspaces that correspond to B_{u_0}-indistinguishable sets. Formally, two linear subspaces U_1 and U_2 of $\mathcal{L}^A_{u_0}$ are B_{u_0}-*equivalent* if (2) holds for every $B \in \mathcal{L}^B_{u_0}$. Note that two subsets A_1 and A_2 of A_{u_0} are B_{u_0}-indistinguishable if and only if the linear subspaces $\varphi(A_1) \cap \varphi(B_{u_0})$ and $\varphi(A_2) \cap \varphi(B_{u_0})$ are B_{u_0}-equivalent. Clearly, partitioning the lists $\mathcal{L}^A_{u_0}$ into classes of B_{u_0}-equivalent linear subspaces requires only a constant number of operations with linear subspaces over $\mathbb{F}$ at each node of the tree (under the assumption that $\mathbb{F}$ and k are fixed).

We are now ready to construct our auxiliary bipartite graphs G_{u_0}. Let u_1 and u_2 be the two children of u_0 and u' the parent of u_0. The vertices of G_{u_0} are classes of B_{u_1}-equivalent linear subspaces of $\mathcal{L}^A_{u_1}$ and B_{u_2}-equivalent linear subspaces of $\mathcal{L}^A_{u_2}$. The edge joining two vertices of G_{u_0}, one corresponding to the class containing $U_1 \in \mathcal{L}^A_{u_1}$ and the other to the class containing $U_2 \in \mathcal{L}^A_{u_2}$, is labelled with $\dim U_1 + \dim U_2 - \dim \overline{U_1 \cup U_2}$ and is associated with the vertex of $G_{u'}$ that corresponds to the class containing the linear subspaces of $\mathcal{L}^A_{u_0}$ that are B_{u_0}-equivalent $\overline{U_1 \cup U_2} \cap B_{u_0}$. Clearly, computing each of the auxiliary graphs G_{u_0} requires a constant number of operations with linear subspaces over $\mathbb{F}$ at each node of the decomposition. Hence, we conclude that the entire process described in this subsection requires time at most $O(n^4)$ where n is the number of elements of $\mathcal{M}$ if we assume that we can decide the equality of m-dimensional linear spaces over $\mathbb{F}$ and compute their unions and intersections in time $O(m^3)$ (note that the rank of $\mathcal{M}$ cannot exceed n).

4.2 Computing representations

Throughout this subsection, we assume that the auxiliary bipartite graphs G_{u_0} as described in Subsection 4.1 have been constructed. We would like to point out that we do not use the original representation of $\mathcal{M}$ over $\mathbb{F}$ at all throughout this subsection and use only the auxiliary bipartite graphs to construct a representation of $\mathcal{M}$ over a given finite field $\mathbb{F}'$.

Let us consider a node u_0 of the branch decomposition and let ℓ_{u_0} be the number of the classes of B_{u_0}-indistinguishable subsets of A_{u_0}. Note that ℓ_{u_0} is also the number of vertices of $G_{u'}$ where u' is the parent of u_0 that form the part of $G_{u'}$ corresponding to A_{u_0}. Let further $k_{u_0} = \text{rank } A_{u_0} + \text{rank } B_{u_0} - \text{rank } \mathcal{M}$.

If φ is a representation of $\mathcal{M} \setminus B_{u_0}$ in a vector space over $\mathbb{F}'$ and U is its k_{u_0}-dimensional linear subspace, the *type* of a representation φ with respect to U is an ℓ_{u_0}-tuple $[\mathcal{L}_1, \dots, \mathcal{L}_{\ell_{u_0}}]$ where $\mathcal{L}_i$ is the set of all linear subspaces of U equal to $\varphi(A') \cap U$ for some $A' \subseteq A_{u_0}$ contained in the i-th class of B_{u_0}-indistinguishable subsets of A_{u_0}, $i = 1, \dots, \ell_{u_0}$. The representation φ is *proper* with respect to U if the sets $\mathcal{L}_i$ are mutually disjoint and the dimensions of linear subspaces contained in the same $\mathcal{L}_i$ are equal. Observe that a restriction of any representation φ of $\mathcal{M}$ to A_{u_0} with $U = \varphi(A_{u_0}) \cap \varphi(B_{u_0})$ is proper with respect to U.

Finally, let us refine the notion of isomorphic representations. Two representations φ_1 and φ_2 of $\mathcal{M} \setminus B_{u_0}$ are *strongly isomorphic* with respect to U if they have the same type $[\mathcal{L}_1, \ldots, \mathcal{L}_{\ell_{u_0}}]$ and there exists an isomorphism ψ of the linear spaces $\varphi_1(A_{u_0})$ and $\varphi_2(A_{u_0})$ such that $\psi(\varphi_1(e))$ is a non-zero multiple of $\varphi_2(e)$ for each element e of A_{u_0}. Note that if φ_1 and φ_2 are strongly isomorphic, then they are also isomorphic representations of $\mathcal{M} \setminus B_{u_0}$, but the converse need not to be true since the strong isomorphism requires that they agree on the linear subspaces of U corresponding to B_{u_0}-indistinguishable subsets of A_{u_0}.

Let us fix a linear space U_{u_0} over $\mathbb{F}'$ of dimension k_{u_0} for each inner node u_0. Our next step is to compute the number of strongly non-isomorphic representations of $\mathcal{M} \setminus B_0$ with respect to U_{u_0} for each type $[\mathcal{L}_1, \ldots, \mathcal{L}_{\ell_{u_0}}]$ of a possible proper representation. The linear subspaces U_{u_0} are fixed in order to allow us to be able to define the type of a representation and are not the actual subspaces $\varphi(A_{u_0}) \cap \varphi(B_{u_0})$ in the representation of $\mathcal{M}$ that we aim to construct. The numbers of representations of $\mathcal{M} \setminus B_{u_0}$ are computed in the bottom to top fashion in the branch decomposition as we explain further in more detail.

Assume first that u_0 is a leaf of the branch decomposition and let e be the element of $\mathcal{M}$ corresponding to u_0. If e is a bridge of $\mathcal{M}$, then the empty set and $\{e\}$ are B_{u_0}-indistinguishable, $k_{u_0} = 0$ and $\ell_{u_0} = 1$. Hence, there is a single possible type $[\mathcal{L}_1]$ of a proper representation of $\mathcal{M} \setminus B_{u_0}$ in which $\mathcal{L}_1$ is the set containing only the zero subspace of U_{u_0} and there is a single (up to a strong isomorphism) representation of $\mathcal{M} \setminus B_{u_0}$ of this type—any representation of e with a non-zero vector over $\mathbb{F}'$.

If e is not a bridge of $\mathcal{M}$, then $k_{u_0} = 1$ and the empty set and $\{e\}$ are B_{u_0}-indistinguishable. Hence, $\ell_{u_0} = 2$ and there is again a single possible type $[\mathcal{L}_1, \mathcal{L}_2]$ of a proper representation of $\mathcal{M} \setminus B_{u_0}$ in which $\mathcal{L}_1$ is the set containing only the zero subspace of U_{u_0} and $\mathcal{L}_2$ the set containing the linear space U_{u_0}. Clearly, there is a single (up to a strong isomorphism) representation of $\mathcal{M} \setminus B_{u_0}$ of this type.

Assume now that u_0 is an inner node of the branch decomposition and let u_1 and u_2 be its two children. We now have to merge the representations of $\mathcal{M} \setminus B_{u_1}$ and $\mathcal{M} \setminus B_{u_2}$ (this is closely related to rooted configurations as described in [9]). Let U be a superspace of U_{u_0} of dimension $k_{u_1} + k_{u_2}$ (note that $k_{u_0} \leq k_{u_1} + k_{u_2}$ by submodularity of the rank function). For all possible identifications of U_{u_1} and U_{u_2} with k_{u_1}-dimensional and k_{u_2}-dimensional linear subspaces of U, we proceed as described in what follows.

We say that two types $[\mathcal{L}'_1, \ldots, \mathcal{L}'_{\ell_{u_1}}]$ and $[\mathcal{L}''_1, \ldots, \mathcal{L}''_{\ell_{u_2}}]$ are *weakly com-*

patible if for every $U' \in \mathcal{L}'_{i'}$, $1 \le i' \le \ell_{u_1}$ and $U'' \in \mathcal{L}''_{i''}$, $1 \le i'' \le \ell_{u_2}$,

$$\dim U' + \dim U'' - \dim \overline{U' \cup U''}$$

is equal to the label of the edge joining the i'-th vertex and i''-th vertex of the two parts of G_{u_0}. Finally, let $\mathcal{L}_i$ for $i = 1, \ldots, \ell_{u_0}$ be the set of all linear subspaces equal to

$$\overline{U' \cup U''} \cap U_{u_0} \text{ for some } U' \in \mathcal{L}'_{i'}, 1 \le i' \le \ell_{u_1} \text{ and } U'' \in \mathcal{L}''_{i''}, 1 \le i'' \le \ell_{u_2}$$

such that the edge between the i'-th and i''-th vertices of the two parts of G_{u_0} is associated with the i-th vertex of the auxiliary graph of the parent of u_0. If all the sets $\mathcal{L}_i$, $1 \le i \le \ell_{u_0}$, are disjoint and the subspaces contained in each $\mathcal{L}_i$ have the same dimension, we say that the types $[\mathcal{L}'_1, \ldots, \mathcal{L}'_{\ell_{u_1}}]$ and $[\mathcal{L}''_1, \ldots, \mathcal{L}''_{\ell_{u_2}}]$ are *strongly compatible*.

Observe now that representations of $\mathcal{M} \setminus B_{u_1}$ and $\mathcal{M} \setminus B_{u_2}$ form a representation of $\mathcal{M} \setminus B_{u_0}$ if and only if their types are weakly compatible. The condition of being strongly compatible is then equivalent to having a proper type with respect to B_{u_0}. The sum of the products of the numbers of strongly compatible representations of $\mathcal{M} \setminus B_{u_1}$ and $\mathcal{M} \setminus B_{u_2}$ with the same resulting (proper) type $[\mathcal{L}_1, \ldots, \mathcal{L}_{u_0}]$ yields after normalization (we have to divide by the number of isomorphic identifications of U_{u_1} and U_{u_2} with linear subspaces of U that fix U_{u_0}) the number of strongly non-isomorphic representations of $\mathcal{M} \setminus B_{u_0}$ with the type $[\mathcal{L}_1, \ldots, \mathcal{L}_{u_0}]$.

Since the root u_r of the branch decomposition corresponds to a loop, U_{u_r} is the zero space and there is a single type of representations of $\mathcal{M} \setminus B_{u_r}$ associated with u_r. This type is $[\mathcal{L}_1]$ where $\mathcal{L}_1$ is a set consisting of the zero subspace only. The number of strongly non-isomorphic representations of $\mathcal{M} \setminus B_{u_r}$ of this type is the number of non-isomorphic representations of $\mathcal{M}$. Hence, we have just presented an algorithm for counting the number of non-isomorphic representations of $\mathcal{M}$ over $\mathbb{F}'$. Note that the number of all mappings from $\mathcal{M}$ to an n-dimensional vector space over $\mathbb{F}'$, where n is the number of elements of $\mathcal{M}$, is at most $|\mathbb{F}'|^{n^2}$ and thus all the numbers involved in the computation are $O(n^2)$-bit numbers. In particular, our algorithm has running time polynomial in n. If we just want to decide the existence of the representation over $\mathbb{F}'$, we can replace the numbers of strongly non-isomorphic representations in our computation with flags indicating their existence. In this way, we obtain an $O(n)$-algorithm for computing the existence of a representation of $\mathcal{M}$ over $\mathbb{F}'$ (note that $\mathbb{F}'$ and the maximal branch-width of $\mathcal{M}$ are fixed) from the auxiliary graphs G_{u_0}.

Finally, it is easy to modify the presented algorithm to either output one possible representation of $\mathcal{M}$ over $\mathbb{F}'$ (keeping the running time polynomial in $n = |\mathcal{M}|$) or to output all such non-isomorphic representations (in this case, each representation can be output in time polynomial in $|\mathcal{M}|$, but the running time of the algorithm need not to be polynomial in $|\mathcal{M}|$ since the number of such representations could be exponential in $|\mathcal{M}|$).

4.3 Finale

The results of Subsections 4.1 and 4.2 can be combined to the following:

Theorem 3. *For every $k \geq 1$ and two finite fields $\mathbb{F}$ and $\mathbb{F}'$, there is a polynomial-time algorithm that for a given matroid $\mathcal{M}$ of branch-width at most k that is represented over the field $\mathbb{F}$ decides whether $\mathcal{M}$ can be represented over $\mathbb{F}'$ and if so, it computes one of its representation over $\mathbb{F}'$. The algorithm also counts the number of non-isomorphic representations of $\mathcal{M}$ over $\mathbb{F}'$. Moreover, it can be modified to list all such non-isomorphic representations (in time linearly dependant on the number of such representations).*

5 Concluding remarks

We would like to address a possibility of extending our algorithm to matroids that are not represented over a finite field. As discussed in Introduction, it is NP-hard to decide whether a matroid $\mathcal{M}$ represented over $\mathbb{Q}$ with branch-width three can be represented over a finite field $\mathbb{F}$, $\mathbb{F} \neq \mathrm{GF}(2), \mathrm{GF}(3)$. A possible extension would thus be to assume that $\mathcal{M}$ is guaranteed to be representable over $\mathbb{F}$:

Problem 1. *For every $k \geq 1$ and every finite field $\mathbb{F}$, design a polynomial-time algorithm that for a matroid $\mathcal{M}$ represented over $\mathbb{Q}$ of branch-width at most k that is representable over $\mathbb{F}$ finds a representation of $\mathcal{M}$ over $\mathbb{F}$.*

In Problem 1, one can also consider matroids that are given by an oracle, however, in this setting, we do not believe that such an algorithm could be designed.

Let us now have a closer look at Problem 1. The algorithm that we presented in Section 4 has two separate parts. In the first part, we compute auxiliary bipartite graphs G_{u_0} and in the second part, we just decide the existence and eventually compute the representations just using these auxiliary graphs. Hence, we need the representation of $\mathcal{M}$ over a finite field only in the first part of our algorithm.

In order to compute the auxiliary graphs, we need to be able to recognize for a k-separation (A, B) of $\mathcal{M}$ which subsets $A_1, A_2 \subseteq A$ are B-indistinguishable. This test is equivalent to testing whether the matroids $(\mathcal{M}/A_1) \setminus (A \setminus A_1)$ and $(\mathcal{M}/A_2) \setminus (A \setminus A_2)$ are isomorphic and the identity on the elements of B is an isomorphism between them. We ask the reader to verify that the entire algorithm presented in Subsection 4.1 works even if each class of B_{u_0}-equivalent linear subspaces is represented by a single subset $A' \subseteq A$ which is B_{u_0}-indistinguishable from all subsets of A corresponding to B_{u_0}-equivalent linear subspaces.

Hence, the algorithm that we designed can be turned into a polynomial-time algorithm for computing representations of a matroid over a finite field from its representation over $\mathbb{Q}$ if the following algorithm exists:

Problem 2. *For every $k \geq 1$ and every finite field $\mathbb{F}$, design a polynomial-time algorithm that decides whether a bijection between the elements of two matroids $\mathcal{M}_1$ and $\mathcal{M}_2$ represented over $\mathbb{Q}$, such that the branch-widths of $\mathcal{M}_1$ and $\mathcal{M}_2$ are at most k and both $\mathcal{M}_1$ and $\mathcal{M}_2$ are representable over $\mathbb{F}$, is an isomorphism between $\mathcal{M}_1$ and $\mathcal{M}_2$.*

Note that if we dismiss the assumption that $\mathcal{M}_1$ and $\mathcal{M}_2$ are representable over $\mathbb{F}$, the algorithm described in Problem 2 does not exist. If it existed, this would imply that testing representatibility over a fixed finite field $\mathbb{F}$ can be solved in a polynomial time for matroids of bounded branch-width that are represented over $\mathbb{Q}$ which is an NP-hard problem.

Acknowledgement

The author would like to thank Jiří Fiala for fruitful discussions on algorithmic matroid theory, in particular on efficient computation of the Tutte polynomial, at various occasions in the spring of 2002, Ondřej Pangrác for sharing his insights into matroid theory, and Till Tantau for his computational complexity remarks.

References

[1] S. Arnborg, J. Lagergren, D. Seese: Easy problems for tree decomposable graphs, J. Algorithms 12 (1991), 308–340.

[2] H. Bodlaender: Dynamic programming algorithms on graphs with bounded tree-width, in: Proc. of ICALP 1988, LNCS. vol. 317, Springer, Berlin, 1988, 105–119.

[3] B. Courcelle: The monadic second-order logic of graph I. Recognizable sets of finite graphs, Information and Computation 85 (1990), 12–75.

[4] B. Courcelle: The expression of graph properties and graph transformations in monadic second-order logic, in: G. Rozenberg (ed.), Handbook of graph grammars and computing by graph transformations, Vol. 1: Foundations, World Scientific, 1997, 313–400.

[5] J. Geelen, B. Gerards, G. Whittle: Tangles, tree decomposition and grids in matroids, preprint.

[6] J. Geelen, B. Gerards, G. Whittle: On Rota's Conjecture and excluded minors containing large projective geometries, to appear in Journal of Combinatorial Theory Ser. B.

[7] J. Geelen, B. Gerards, G. Whittle: Excluding a planar graph from GF(q)-representable matroids, manuscript.

[8] J. Geelen, B. Gerards, G. Whittle: Inequivalent representations of matroids I: An overview, in preparation.

[9] J. Geelen, B. Gerards, G. Whittle: Branch-width and well-quasi-ordering in matroids and graphs, J. Combin. Theory Ser. B 84 (2002), 270–290.

[10] P. Hliněný: On matroid properties definable in the MSO logic, in: Proc. of MFCS 2003, LNCS vol. 2747, Springer, Berlin, 2003, 470–479.

[11] P. Hliněný: A parametrized algorithm for matroid branch-width, SIAM J. Computing 35(2) (2005), 259–277.

[12] P. Hliněný: Branch-width, parse trees and monadic second-order logic for matroids, J. Combin. Theory Ser. B 96 (2006), 325–351.

[13] P. Hliněný: On matroid representatibility and minor problems, in: Proc. of MFCS 2006, LNCS vol. 4192, Springer, Berlin, 2006, 505–516.

[14] P. Hliněný, G. Whittle: Matroid tree-width, to appear in European Journal on Combinatorics.

[15] S. Oum, P. Seymour: Certifying large branch-width, in: Proc. of SODA 2006, SIAM, 2006, 810–813.

[16] S. Oum, P. Seymour: Approximating clique-width and branch-width, to appear in Journal of Combinatorial Theory, Ser. B.

[17] J. G. Oxley: Matroid theory, Oxford University Press, 1992.

[18] G.-C. Rota: Combinatorial theory, old and new, Actes du Congrès International de Mathématiciens, vol. 3, Gauthier-Villars, Paris, 1970, 229–233.

[19] P. Seymour: Decomposition of regular matroids, J. Combin. Theory Ser. B 28 (1980), 305–359.

[20] P. Seymour: Recognizing graphic matroids, Combinatorica 1 (1981), 75–78.

[21] K. Truemper: Matroid decomposition, Academic Press, 1992.