# On Matroid Representability and Minor Problems

**Petr Hliněný**

Faculty of Informatics,
Masaryk University in Brno,
Botanická 68a, 602 00 Brno, Czech Republic
and
Department of Computer Science,
VŠB – Technical University Ostrava,
17. listopadu 15, 708 33 Ostrava, Czech Republic
hlineny@fi.muni.cz

**Abstract.** In this paper we look at complexity aspects of the following problem (matroid representability) which seems to play an important role in structural matroid theory: Given a rational matrix representing the matroid $M$, the question is whether $M$ can be represented also over another specific finite field. We prove this problem is hard, and so is the related problem of minor testing in rational matroids. The results hold even if we restrict to matroids of branch-width three.

**Keywords:** matroid representability, minor, finite field, spike, swirl.
2000 Math subject classification: 05B35, 68Q17, 68R05.

## 1 Introduction

We postpone necessary formal definitions until later sections. Matroids present a wide combinatorial generalization of graphs. A useful geometric essence of a matroid is shown in its vector representation over a field $\mathbb{F}$; the elements–vectors of the representation can be viewed as points in the projective geometry over $\mathbb{F}$. Not all matroids, however, have vector representations. That is why the question of $\mathbb{F}$-representability of a matroid is important to solve.

Another motivation for our research lies in a current hot trend in structural matroid theory; work of Geelen, Gerards and Whittle, e.g. [4, 5] extending significant portion of the Robertson–Seymour's Graph Minors project [15] to matroids. It turns out that matroids represented over finite fields $\mathbb{F}$ play a crucial role in that research, analogous to the role played by graphs embedded on surfaces in Graph Minors. Such a role is further justified by related works concerning logic and complexity aspects of matroids, e.g. our [8, 10], and by a somehow surprising connection of binary matroids with graph rank-width [1] of Courcelle and Oum.

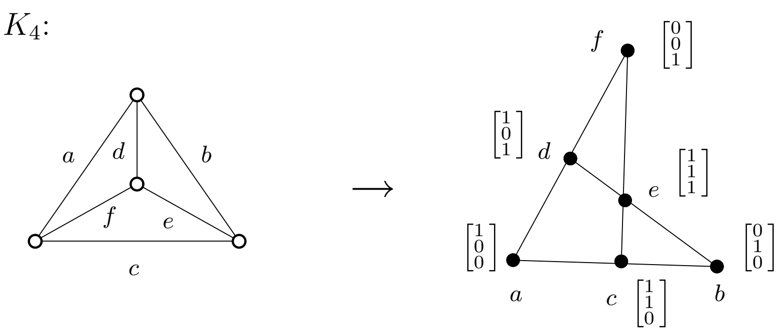
In this paper we prove that it is hard to decide whether a matroid given by a vector representation over the rational numbers, has a vector representation over a specific finite field $\mathbb{F}$ (Theorems 3.1 and 4.1). In particular this result implies that also the problem of minor testing in rational matroids is generally hard. We moreover prove that the minor testing problem is hard even for a certain small planar minor (Theorem 5.6).

## 2 Matroids and Vector Representations

We refer to Oxley's book [12]. Since matroid theory seems not widely known among computer scientists, we should briefly review some basic terms here:

A *matroid* is a pair $M = (E, \mathcal{B})$ where $E = E(M)$ is the finite ground set of $M$ (*elements* of $M$), and $\mathcal{B} \subseteq 2^E$ is a nonempty collection of *bases* of $M$, no two of which are in an inclusion. Moreover, matroid bases satisfy the "exchange axiom": if $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then there is $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$. Subsets of bases are called *independent sets*, and the remaining sets are *dependent*. Minimal dependent sets are called *circuits*. All bases have the same cardinality called the *rank* $\mathrm{r}(M)$ of the matroid. The *rank function* $r_M(X)$ in $M$ assigns the maximal cardinality of an independent subset of a set $X \subseteq E(M)$. A set $X$ is *spanning* if $r_M(X) = \mathrm{r}(M)$, and maximal non-spanning sets are called *hyperplanes*.

The reader may notice that a matroid, according to the presented definition, carries some information about all subsets of $E$ which is exponential in the number of elements $|E|$. (See also [11].) Studying computational complexity on matroids one has to find a workaround for that: A common way to handle a matroid input is to consider a particular polynomially sized representation, instead.




$$M(K_4):\quad \mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

**Fig. 1.** An example of a vector representation (on the right) $\boldsymbol{A}$ of the cycle matroid $M(K_4)$ of the complete graph $K_4$ (on the left). The matroid elements are depicted by dots, and their (linear) dependency is shown using lines.

If $G$ is a (multi)graph, then its *cycle matroid* on the ground set $E(G)$ is denoted by $M(G)$: The independent sets of $M(G)$ are the acyclic subsets (forests) in $G$, and the circuits of $M(G)$ are the cycles in $G$. Another example of a matroid is a finite set of vectors with usual linear independence: If $\boldsymbol{A}$ is a matrix, then the matroid formed by the column vectors of $\boldsymbol{A}$ is called the *vector matroid* of $\boldsymbol{A}$, and denoted by $M(\boldsymbol{A})$. (Fig. 1.) The matrix $\boldsymbol{A}$ is a *vector representation* of a matroid $M \simeq M(\boldsymbol{A})$, and such $M(\boldsymbol{A})$ is $\mathbb{F}$-represented when $\boldsymbol{A}$ is over a field $\mathbb{F}$. We say that a matroid $M$ is $\mathbb{F}$*-representable* if $M$ has a vector representation over $\mathbb{F}$.

Questions of representability over finite fields $\mathbb{F}$ seem to play very important role in structural matroid theory. (We refer also to Section 5 for a closer discussion.) We now look at the problem from a complexity point of view.

**Definition.** The $\mathbb{F}$*-representability problem* for $\mathbb{F}'$-represented matroids is:

*Input.* A matrix $\boldsymbol{A}$ over a field $\mathbb{F}'$.
*Question.* Is the vector matroid $M(\boldsymbol{A})$ representable over $\mathbb{F}$?

**Summary.** If the input (matrix $\boldsymbol{A}$) is represented over $\mathbb{F}' = \mathbb{Q}$ (the rational numbers), the known answers to the $\mathbb{F}$-representability problem follow.

**(2.1)** For $\mathbb{F} = GF(2)$, the $\mathbb{F}$-representability problem for the matroid $M(\boldsymbol{A})$ is solvable in **polynomial** time by a deep result of Seymour [16].
**(2.2)** For $\mathbb{F} = GF(3)$, the answer is still open.
**(2.3)** For $\mathbb{F} = GF(q)$ a finite field on $q \geq 4$ elements, the $\mathbb{F}$-representability problem is ***co-NP*-complete** by our Theorems 3.1 and 4.1 and by [6].

Discussing (2.1), we explain that if a $GF(2)$-representable (*binary*) matroid $M$ had also a vector representation over any field of characteristic not 2, then $M$ could be represented by a totally-unimodular matrix. Hence $M$ would be a so called regular matroid (representable over all fields), and then one can use Seymour's decomposition theorem [16] for regular matroids to recognize such $\mathbb{Q}$-represented $M$ in polynomial time.

About (2.3) in the summary, one should understand why an apparently straightforward argument "guess an $\mathbb{F}$-representation and verify it" does not readily prove membership of the $\mathbb{F}$-representability problem in $NP$: The problem is that verifying whether two matrices represent isomorphic matroids may require evaluating too many subdeterminants. Indeed, Seymour [16] has proved that verifying a matrix over $GF(2)$ represents a matroid $M$ (given by an oracle) requires testing independence on an exponential number of subsets. On the other hand, the following interesting result, showing membership of the $\mathbb{F}$-representability problem in *co-NP*, is proved in [6, Theorem 1.3]:

**Theorem 2.4** (Geelen, Gerards and Whittle).
*Let $\mathbb{F} = GF(q)$ be a finite field. Proving non-$\mathbb{F}$-representability of a matroid $M$ needs only $O\big(|E(M)|^2\big)$ rank evaluations in $M$.*

Lastly we add two remarks concerning possible extensions of our results in (2.3). First, the proofs of Theorems 3.1 and 4.1 show that the hardness result holds even for matroids of branch-width 3. On contrary to that, the $\mathbb{F}$-representability problem, as well as all other minor-closed properties, can be tested in polynomial time [7] if the input matroid is represented over a finite field $GF(q)$ and has bounded branch-width. Second, Theorems 3.1 and 4.1 could be extended to other infinite fields using the method of [9, Section 5]. We skip such extensions here to avoid the boring technical details.

## 3 Spikes: The Case of Non-prime Fields

The purpose of this section is to prove one case of the hardness result:

**Theorem 3.1.** *Let $\mathbb{F} = GF(q)$, where $q = p^a, a > 1$, be a finite non-prime field. Suppose $\boldsymbol{A}$ is a matrix given over $\mathbb{Q}$, and let $M = M(\boldsymbol{A})$ be its vector matroid. Then it is $NP$-hard to recognize that $M$ has no vector representation over $\mathbb{F}$. The same conclusion remains true even if $M$ is restricted to have branch-width* 3.

For the proof we need a definition of an interesting class of matroids, called "spikes". Let $n \geq 3$ and $S_0$ be a matroid circuit on the ground set $e_0, e_1, \ldots, e_n$. Denote by $S_1$ an arbitrary simple matroid obtained from $S_0$ by adding $n$ new elements $f_i$ for $i \in [1, n]$ such that $\{e_0, e_i, f_i\}$ is a triangle. Then the matroid $S = S_1 \setminus e_0$ obtained by deleting the central element $e_0$ is called a *rank-$n$ spike.* The pairs $\{e_i, f_i\}$, $i \in [1, n]$ are called the *legs* of the spike. (Fig. 2.) Let *main circuits / bases* be those circuits / bases of $S$ which intersect each leg of $S$ in exactly one element. For instance, $\{e_1, \ldots, e_n\}$ is a main basis of $S$. We say that a spike $S$ is a *free spike* if $S$ has no main circuit. There is just one free spike of each rank up to isomorphism, see also Proposition 3.2(b),(e).

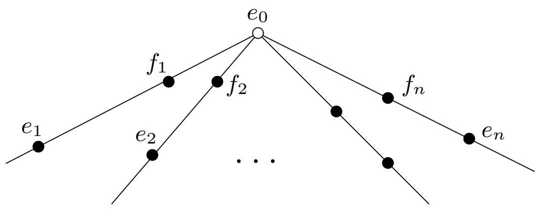



**Fig. 2.** An illustration of the definition of a rank-$n$ spike.

Spikes are known for giving "difficult counterexamples" in structural matroid theory. Some well known simple properties of spikes are summarized next; these implicitly originate perhaps in [13], and we refer to e.g. [9] for explicit proofs. Let $\boldsymbol{D}^1(x_1, \ldots, x_n) = [d_{i,j}]_{i=1}^n$ denote an $n \times n$ matrix such that $d_{i,j} = 1$ if $i \neq j \in [1, n]$, and $d_{i,i} = x_i$.

**Proposition 3.2.** *Let $S$ be a rank-$n$ spike where $n \geq 3$. Then*

*a) the union of any two legs forms a* 4*-element circuit in $S$,*
*b) every other circuit intersects all legs of $S$,*

*c) $S$ is 3-connected and the branch-width of $S$ is 3,*

*d) $S$ has a vector representation, if and only if it has a representation of the form $[\,\boldsymbol{I}_n \mid \boldsymbol{D}^1(x_1,\dots,x_n)\,]$ where $x_1,\dots,x_n \neq 1$ and $\boldsymbol{I}_n$ displays a chosen main basis of $S$, see e.g.*

$$\begin{array}{c} \\ e_1 \\ e_2 \\ \vdots \\ e_{n-1} \\ e_n \end{array} \begin{array}{c} \begin{array}{cccccccccc} e_1 & e_2 & \dots & e_{n-1} & e_n & f_1 & f_2 & \dots & f_{n-1} & f_n \end{array} \\ \left[\begin{array}{ccccc|ccccc} 1 & 0 & \cdots & 0 & 0 & x_1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & x_2 & 1 & 1 & 1 \\ \vdots & 0 & \ddots & 0 & \vdots & \vdots & 1 & \ddots & 1 & \vdots \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & x_{n-1} & 1 \\ 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & x_n \end{array}\right] \end{array},$$

*e) if $S$ has a representation, as in (d), and $X \subseteq E(S)$ is such that $X$ intersects each leg of $S$ in exactly one element, then $X$ is a circuit of $S$ if and only if*

$$\sum\nolimits_{j\in[1,n];\; f_j\in X} \frac{1}{x_j-1} = -1\,,$$

*f) the free spike is $\mathbb{F}$-representable if $\mathbb{F}$ is a non-prime finite field.*

*Remark.* Notice that a vector representation of a matroid in the "standard" form $\boldsymbol{A} = [\boldsymbol{I} \mid \boldsymbol{A}']$ has a property that the matroid bases are in a one-to-one correspondence with the nonzero subdeterminants in $\boldsymbol{A}'$ (via matrix pivoting).

Following [9], we have chosen to prove Theorem 3.1 via a polynomial reduction from the $NP$-complete PARTITION problem [2] over the integers. (Briefly saying, the PARTITION problem asks whether a given multiset of integers can be partitioned into two parts such that their sums equal.)

Let $\mathbb{F} = GF(q)$, where $q = p^a$, be a finite non-prime field.

**Lemma 3.3.** *If $S$ is an $\mathbb{F}$-representable spike that is not the free spike, and $B \subset E(S)$ is any main basis of $S$, then there is a main circuit $C \subset E(S)$ such that $|C \setminus B| < q$ (independently of $S$).*

***Proof.*** We refer to Proposition 3.2. According to (d), we select an $\mathbb{F}$-representation $[\,\boldsymbol{I}_n \mid \boldsymbol{D}^1(x_1,\dots,x_n)\,]$ of $S$ where $\boldsymbol{I}_n$ shows the basis $B = \{e_1, e_2, \dots, e_n\}$. We choose the circuit $C$ such that $|C \setminus B|$ is the smallest possible. Let $J = \{j \in [1,n];\ f_j \in C\}$. For a contradiction, we assume $|J| = |C \setminus B| \geq q$. Then among the partial sums $S(J') = \sum_{j\in J'} \frac{1}{x_j-1} \in \mathbb{F}$ for $J' \subseteq J$, there exist two such equal, $S(J_1) = S(J_2)$ where $J_1 \subset J_2 \subseteq J$, by the pigeon-hole principle. We set $J_0 = J_2 \setminus J_1$, and by (e) we may write

$$-1 \;=\; \sum\nolimits_{j\in J} \frac{1}{x_j-1} \;=\; S(J) = S(J) - S(J_2) + S(J_1) \;=\; \sum\nolimits_{j\in J\setminus J_0} \frac{1}{x_j-1}\,.$$

Hence there is another main circuit $C' = B\Delta\{e_j, f_j : j \in J \setminus J_0\}$ in $S$ such that $|C' \setminus B| = |J \setminus J_0| < |J| = |C \setminus B|$, a contradiction to our choice of $C$. ∎

***Proof of Theorem 3.1.*** Let $T = \{t_1, t_2, \dots, t_n\}$ be a multiset of positive integers – an input to the PARTITION problem, and $t = t_1 + t_2 + \ldots + t_n$. We denote by $z_i = \frac{-2t_i}{t}$ and set $x_i = \frac{1}{z_i} + 1$, for $i \in [1, n]$. We consider the matrix $\boldsymbol{A} = [\, \boldsymbol{I}_n \,|\boldsymbol{D}^1(x_1, \ldots, x_n)\,]$ over $\mathbb{Q}$ as the input in the theorem. The vector matroid $S = M(\boldsymbol{A})$ is actually a spike by Proposition 3.2(d). Let $B = \{e_1, \ldots, e_n\}$ be the main basis of $S$ displayed by $\boldsymbol{I}_n$ in $\boldsymbol{A}$.

Assume $J \subset [1, n]$ is such that the multiset partition $\big(\{t_i : i \in J\}, \{t_i : i \in [1, n] \setminus J\}\big)$ is a solution to *Partition*. That is equivalent to $\sum_{i \in J} z_i = -1$, i.e. $\sum_{i \in J} \frac{1}{x_i - 1} = -1$. Hence by Proposition 3.2(e) the set $X = B \Delta \{e_i, f_i : i \in J\}$ is a main circuit. We conclude:

*Claim 3.4.* Solutions to the *Partition* problem on $T$ are in a one-to-one correspondence with main circuits in the associated spike $S$.

Our polynomial reduction from *Partition* to $\mathbb{F}$-representability follows:

1. In the first stage we check by brute force all parts of $T$ smaller than $q$. If we succeed, we answer YES to *Partition*.
2. In the second stage we ask about $\mathbb{F}$-representability of the matroid $S = M(\boldsymbol{A})$ defined above. If the outcome is negative, we again answer YES to *Partition*. Otherwise, our answer is NO.

It remains to prove that our reduction is correct. Assume the *Partition* problem on $T$ has no solution ($S$ is the free spike). Then in the first stage we find nothing, and in the second stage we answer NO by Proposition 3.2(f). Conversely, assume the *Partition* problem on $T$ has a solution $(T_1, T_2)$. If $\min(|T_1|, |T_2|) < q$, then we answer YES in stage 1. Otherwise, there is a main circuit $C$ in $S$, but no such $C$ with $|C \setminus B| < q$ by Claim 3.4. Hence $S$ is not $\mathbb{F}$-representable by Lemma 3.3, and we answer YES in stage 2. ∎

## 4 Swirls: The Case of Prime Fields

Analogously to Theorem 3.1 we now finish the remaining, slightly more involved case of (2.3).

**Theorem 4.1.** *Let $\mathbb{F} = GF(p)$ be a finite prime field, $p \geq 5$. Suppose $\boldsymbol{A}$ is a matrix given over $\mathbb{Q}$, and let $M = M(\boldsymbol{A})$ be its vector matroid. Then it is $NP$-hard to recognize that $M$ has no vector representation over $\mathbb{F}$. The same conclusion remains true even if $M$ is restricted to have branch-width 3.*

For proving the statement we define another very interesting class of matroids called "swirls", which have been implicitly introduced in [13]. Let rank-$r$ *whirl* $\mathcal{W}^r$ be the unique matroid obtained from the cycle matroid of the wheel graph $W_r$ with spokes $e_1, \ldots, e_r$ and rim edges $f_1, \ldots, f_r$, by relaxing (i.e. declaring independent) the rim circuit $\{f_1, \ldots, f_r\}$. A simple $3n$-element matroid $R$ is a rank-$n$ *swirl* if $R$ is obtained from the whirl $\mathcal{W}^n$ by adding a new element (denoted by $g_i$) on each dependent line (triangle $\{e_i, f_i, e_{i+1}\}$) of $\mathcal{W}^r$. (Fig. 3.)

The pairs $\{f_i, g_i\}$, $i \in [1, n]$ are called here *feet* of the swirl $R$. Let *main circuits / bases* be those circuits / bases of $R$ which intersect each foot of $R$ in

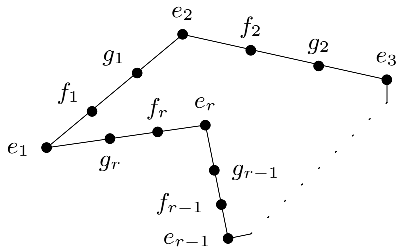



**Fig. 3.** An illustration of the definition of a rank-$n$ swirl.

exactly one element. For instance, $\{f_1, \dots, f_n\}$ is a main basis of $S$. The basis $\{e_1, \dots, e_n\}$ of $R$, formed by the spokes, is called the *central basis*. Notice that the central basis of a swirl is uniquely determined (unlike main bases). Swirls seem to be less known that spikes, and their structure is more complex. Fortunately, all the swirl properties we need in our proof have been implicitly proved in [13, Section 5], and we summarize them in the next proposition.

Let $\boldsymbol{D}^2(x_1, \dots, x_n) = [d_{i,j}]_{i=1}^n$ denote an $n \times n$ matrix such that $d_{i,j} = 0$, $i, j \in [1, n]$ if $i \neq j, j+1$, $d_{i,i} = x_i$, and $d_{i+1,i} = 1$ (indices are take modulo $n$). Let the *free swirl* be a swirl having no main circuits. There is just one free swirl of each rank up to isomorphism, see also Proposition 4.2(a).

**Proposition 4.2.** *Let $R$ be a rank-n swirl where $n \geq 4$. Then*

*a) the only non-spanning circuits that possibly depend on a choice of elements $g_i$ in the definition of a swirl are main circuits of $R$,*
*b) $R$ is 3-connected and the branch-width of $R$ is 3,*
*c) $R$ has a vector representation, if and only if it has a representation of the form $[\,\boldsymbol{I}_n \,|\, \boldsymbol{D}^2(x_1, \dots, x_n) \,|\, \boldsymbol{D}^2(y_1, \dots, y_n)\,]$ where $x_1, \dots, x_n, y_1, \dots, y_n \neq 0$, $x_i \neq y_i$ and $x_1 x_2 \cdots x_n \neq (-1)^n$, $\boldsymbol{I}_n$ displays the central basis and $\{f_1, \dots, f_n\}$ displays any main basis of $R$, see e.g.*

$$\begin{array}{ccccccccccccccc}
e_1 & e_2 & \dots & e_{n-1} & e_n & f_1 & g_1 & f_2 & g_2 & & \dots & & g_{n-1} & f_n & g_n \\
\end{array}$$
$$\left[\begin{array}{ccccccccccccccc}
1 & 0 & \cdots & 0 & 0 & x_1 & y_1 & 0 & 0 & & \cdots & & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & x_2 & y_2 & & & 0 & 0 & 0 & 0 \\
\vdots & & \ddots & 0 & 0 & 0 & 0 & 1 & 1 & & \ddots & & 0 & 0 & 0 \\
 & 0 & & & \vdots & \vdots & 0 & \vdots & 0 & & & & 0 & \vdots & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & & & y_{n-1} & 0 & 0 \\
0 & 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & & \cdots & & 1 & x_n & y_n
\end{array}\right],$$

*d) if $R$ has a representation, as in (c), and $X \subseteq E(R)$ is such that $X$ intersects each foot of $R$ in exactly one element, then $X$ is a circuit of $R$ if and only if*

$$\prod_{j \in [1,n];\; g_j \notin X} x_j \cdot \prod_{j \in [1,n];\; g_j \in X} y_j = (-1)^n ,$$

*e) the free swirl is $\mathbb{F}$-representable if $\{1, -1\}$ is a proper 2-element subgroup of the multiplicative group $\mathbb{F}^*$ (in particular if $\mathbb{F} = GF(p)$ where $p \geq 5$).*

*Remark.* Notice that, if two matroids agree on all non-spanning circuits, then they are isomorphic.

Looking at Proposition 4.2(d), one might get an easy idea: How about solving this case in direct analogy with Section 3, relating the main circuits of a swirl with solutions to a kind of a "product-partition" problem? This idea is generally good, but an immediate approach—to "lift" the *Partition* problem to exponents, fails since such a reduction produces exponentially large instances. We use the following intermediate step (reduced from the 3-dim matching problem):

**Definition.** The *ProdSelect* problem over the integers is:
*Input.* A multiset of $k$ positive integers $T$, and an integer $c$.
*Question.* Is there a subset $P \subseteq T$ such that $\prod_{t \in P} t = c$?

**Lemma 4.3.** *ProdSelect is an $NP$-complete problem.*

Due to space restrictions, we skip some supplementary proofs. Let $\mathbb{F} = GF(p)$ be a prime field. Analogously to Lemma 3.3 one may prove:

**Lemma 4.4.** *If $R$ is an $\mathbb{F}$-representable swirl that is not the free swirl, and $B \subset E(R)$ is any main basis of $R$, then there is a main circuit $C \subset E(R)$ such that $|C \setminus B| < p$ (independently of $R$).*

***Proof of Theorem 4.1.*** Let $T = \{t_1, t_2, \ldots, t_{n-1}\}$ and $c$, positive integers, form an input to *ProdSelect* ($NP$-complete by Lemma 4.3). We may clearly assume $\min(T) > 1$, $c > 1$ and $c \notin T$. Let a matrix $\boldsymbol{A} = \left[\, \boldsymbol{I}_n \mid \boldsymbol{D}^2\big(1, \ldots, 1, (-1)^n c^{-1}\big) \mid \boldsymbol{D}^2\big(t_1, \ldots, t_{n-1}, (-1)^{n-1}\big) \,\right]$ over $\mathbb{Q}$ be the input in the theorem. The vector matroid $R = M(\boldsymbol{A})$ is actually a swirl by Proposition 4.2(c). Denote by $B = \{f_1, \ldots, f_n\}$ the main basis of $R$ formed by the columns of $\boldsymbol{D}^2(1, \ldots, 1, (-1)^n c^{-1})$, cf. 4.2(d).

Assume $J \subseteq [1, n-1]$ is such that the multiset $P = \{t_i : i \in J\}$ is a solution to *ProdSelect*. That is equivalent to $(-1)^n c^{-1} \cdot \prod_{i \in J} t_i = (-1)^n$. So by Proposition 4.2(d) the set $X = B \Delta \{f_i, g_i : i \in J\}$ is a main circuit. Notice also that our assumption $\min(T), c > 1$ implies that all main circuits $X$ – solutions to the equation of 4.2(d), must involve term $c^{-1}$, in other words $g_n \notin X$. Hence:

*Claim 4.5.* Solutions to the *ProdSelect* problem on $T$, $c$ are in a one-to-one correspondence with main circuits in the associated swirl $R$.

Our polynomial reduction from *ProdSelect* to $\mathbb{F}$-representability follows:

1. In the first stage we check by brute force all subsets of $T$ smaller than $p$. If we succeed, we answer YES to *ProdSelect*.
2. In the second stage we ask about $\mathbb{F}$-representability of the matroid $R = M(\boldsymbol{A})$ defined above. If the outcome is negative, we again answer YES to *ProdSelect*. Otherwise, our answer is NO.

It remains to prove that our reduction is correct. Assume the *ProdSelect* problem on $T$ has no solution ($R$ is the free swirl). Then we answer NO by Proposition 4.2(e). Conversely, assume the *ProdSelect* problem on $T$ has a solution $P$. If $|P| < p$, then we answer YES in stage 1. Otherwise, there is a main circuit $C$ in $R$, but no such $C$ with $|C \setminus B| < p$ by Claim 4.5. Hence $R$ is not $\mathbb{F}$-representable by Lemma 4.4, and we answer YES in stage 2. ∎

The proof of (2.3) is now complete by Theorems 2.4, 3.1 and 4.1.

## 5 Matroid Minors

The Graph Minor project [14, 15] of Robertson and Seymour is commonly considered a milestone in structural graph theory. Moreover, the project has had a great impact into theoretical computer science: We mention in particular an $O(n^3)$-time algorithm for testing whether an input graph contains a minor isomorphic to a fixed graph, implying efficient algorithmic solutions to all minor-closed graph properties.

In the more general setting of structural matroid theory, direct extensions of the great Graph Minors results are often false, but a stream of new theoretical results of Geelen, Gerards and Whittle, e.g. [4, 5] in past several years extended significant portion of the Graph Minors theory to matroids representable over finite fields. Questions of matroid representability, and the notion of branch-width, turned out to be the key ingredients in that research. On the algorithmic side, that effort has been contributed by a sequence of results of the author dealing with FPT computation of matroid branch-width and recognition of MSO-definable matroid properties, e.g. [7, 8, 10].

Formally, a *minor* $N$ of a matroid $M$ is obtained by a sequence of deletions and contractions of elements, the order of which does not matter. The meaning of deletion is standard, and *contraction* is the dual operation to deletion, analogous to contraction of a graph edge. In geometric terms, a contraction $M/e$ means a linear projection from the point representing $e$. We write $N = M \setminus D/C$ where $D$ are the deleted and $C$ the contracted elements.

**Definition.** The *$N$-minor problem* for represented matroids is such:

*Input.* A matrix $\boldsymbol{A}$ over a field $\mathbb{F}'$.
*Question.* Does the vector matroid $M(\boldsymbol{A})$ contain a minor isomorphic to a fixed matroid $N$?

Note that $N$ may be arbitrary in the problem, but fixed; $N$ is not considered a part of the input to the problem. The problem easily belongs to $NP$:

**Lemma 5.1.** *Let a matroid $N$ be fixed. One needs only bounded number of rank evaluations to prove that a matroid $M$ has a minor isomorphic to $N$.*

***Proof.*** Let $M' = M \setminus D/C$ be a minor of $M$. The formula $\mathrm{r}_{M'}(X) = \mathrm{r}_M(X \cup C) - \mathrm{r}_M(C)$ determines the rank function of $M'$ relatively to $M$ (for example, [12, Chapter 3]). The minor $M'$ is isomorphic to $N$ if and only if $|E(M')| = |E(N)|$ and the rank functions equal for some bijection between $E(M')$ and $E(N)$. That can be verified, after guessing $C$ and $D$, using only bounded number of rank evaluations in $M$. ∎

Obviously, for some very simple $N$ such as the circuits $U_{k,k+1}$ the matroid $N$-minor problem is polynomial. We remark that $U_{r,n}$ denotes the matroid made of $n$ points (vectors) in general position in rank $r$. It is a kind of a miracle that for $\mathbb{Q}$-represented matroids the $U_{2,4}$-minor problem is also polynomial. See (2.1) and Seymour [16]; the claim follows from the fact that $U_{2,4}$ is the only forbidden minor for binary matroids. On the other hand, since we know the seven forbidden minors [3] for matroid representability over the field $GF(4)$, it follows from Theorem 3.1 that the matroid $N$-minor problem is hard for at least some $N$. Such an argument, however, does not apply to minors $N$ that are cycle matroids of graphs (*graphic* $N$), and hence representable over all fields.

It is proved in [7, 8] that for every finite field $\mathbb{F}'$ one can solve the $N$-minor problem for $\mathbb{F}'$-represented matroids in polynomial time when restricted to inputs of bounded branch-width. Moreover using the matroid version of the "excluded grid" theorem [5], one can solve the $N$-minor problem for $\mathbb{F}'$-represented matroids in polynomial time, when $N$ is a planar graphic matroid, regardless of branch-width. Therefore it is particularly interesting how difficult is the $N$-minor problem for $\mathbb{Q}$-represented matroids when $N$ is a planar graphic matroid. We provide the answer in the rest of this section.

**Summary.** If the input (matrix $\boldsymbol{A}$) is represented over $\mathbb{F}'$, complexity cases of the $N$-minor problem follow:

**(5.2)** If $\mathbb{F}'$ is a finite field and the branch-width of $M(\boldsymbol{A})$ is bounded, then the problem is solvable in **cubic time** [7].
**(5.3)** If $\mathbb{F}'$ is a finite field and $N$ is the cycle matroid of a planar graph, then the problem is solvable in cubic time [5, 7], too.
**(5.4)** If $\mathbb{F}'$ is a finite field and $N$ is arbitrary, then complexity of the $N$-minor problem is a very interesting open question in structural matroid theory.
**(5.5)** For $\mathbb{F}' = \mathbb{Q}$, the $N$-minor problem is $NP$**-complete**, even when the branch-width of $M(\boldsymbol{A})$ is three and $N$ is the cycle matroid of a planar graph.

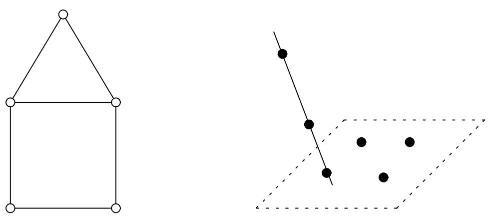


**Fig. 4.** The planar graph $G_6$, and its cycle matroid $M(G_6)$ on the right.

Let $G_6$ denote the planar graph on 6 vertices formed by a 3-cycle and a 4-cycle sharing an edge, see Fig. 4. Our main result reads:

**Theorem 5.6.** *Let the planar graph $G_6$ be as in Fig. 4. Suppose $\boldsymbol{A}$ is a given matrix over $\mathbb{Q}$, and let $M = M(\boldsymbol{A})$ be its vector matroid. Then it is $NP$-complete to decide whether $M$ has a minor isomorphic to the matroid $M(G_6)$. The same conclusion remains true even if $M$ is restricted to have branch-width* 3.

We build on the following result of [9], which follows also from Claim 3.4.

**Proposition 5.7.** *Let $S$ be the vector matroid of $[\,\boldsymbol{I}_n \mid \boldsymbol{D}^1(x_1, \ldots, x_n)\,]$ over $\mathbb{Q}$ where $n \geq 5$. It is $NP$-hard to recognize that $S$ is* not *the rank-$n$ free spike.*

In order to use this statement in making a reduction for the matroid minor problem, we have to find a forbidden minor characterization of the free spikes. This is, after all, not so difficult.

**Lemma 5.8.** *Let $S$ be the rank-$n$ free spike. Then $S$ has no $M(G_6)$-minor.*

***Proof.*** Let $G_6 = C_3 \cup C_4$, where the two cycles $C_3, C_4$ share one edge. We use the same notation $C_3, C_4$ for the corresponding two circuits in the cycle matroid $M_6 = M(G_6)$ of $G_6$. Assume that $M_6 = S \setminus D/C$ is a minor of the free spike $S$, where $C$ is the independent set of contracted elements of $S$. Let us call *leg circuits* in $S$ the 4-element circuits formed by pairs of legs. Recall that main circuits are those circuits of $S$ which intersect each leg in exactly one element. So $S$ is the free spike, i.e. having no main circuits, if and only if all non-leg circuits in $S$ are spanning (Proposition 3.2(b)). By the definition of a minor, a set $X$ is a circuit in $M_6$ if and only if there is a circuit $Y$ in $S$ such that $X \subseteq Y$ and $Y \setminus X \subseteq C$.

Firstly, we claim that not both of the circuits $C_3, C_4$ of the minor $M_6$ result by contracting leg circuits in $S$. If that was not true, then there would be two leg circuits $L_1 \supseteq C_3$ and $L_2 \supseteq C_4$ in $S$. Since, actually, $|L_2| = 4 = |C_4|$, no element of $L_2$ was contracted or deleted when making $M_6$, and so $C_3 \cap C_4 = L_1 \cap L_2$. However, $|L_1 \cap L_2| \in \{0, 2\}$ for any two distinct leg circuits, but $|C_3 \cap C_4| = 1$, a contradiction.

Secondly, we consider that $C_4 \subset K$, where $K$ is a spanning circuit in $S$, and $K \setminus C_4 \subseteq C$ ($C$ are the contracted elements of $S$). So it is $|C| \geq |K| - |C_4| = n + 1 - 4 = n - 3$, and the rank $\mathrm{r}(M) = \mathrm{r}(S) - |C| \leq n - (n - 3) = 3$. However, $\mathrm{r}(M(G_6)) = 4 > 3$. The same contradiction turns out when the remaining possibility $C_3 \subset K$ is considered. Hence $S$ cannot be the free spike, and the statement follows by means of contradiction. ∎

**Lemma 5.9.** *Let $S$ be a rank-$n$ spike for $n \geq 5$ that is not the free spike. Then $S$ has an $M(G_6)$-minor.*

***Proof.*** If $S$ is not the free spike, then there is a main circuit $D \subset E(S)$, cf. Proposition 3.2(b). Let us use the notation from the definition of a spike. We form a minor $N$ of $S$ by contracting the elements of $\{e_i, f_i : i = 5, 6, \dots, n\} \cap D$ and deleting the elements of $\{e_i, f_i : i = 2, 3, \dots, n-1\} \setminus D$. Without loss of generality we assume $e_1, e_n \in D$. Then $\{e_1, f_1, f_n\}$ is a triangle in $N$ and $\{e_i, f_i : i = 1, 2, 3, 4\} \cap D$ is a 4-element circuit in $N$, which intersect each other in $e_1$. Since there are no other non-spanning circuits in $N$, the minor $N$ is isomorphic to $M(G_6)$. ∎

***Proof of Theorem 5.6.*** If we could decide an $M(G_6)$-minor in the matroid $M = M(\boldsymbol{A})$ efficiently, then for a specific matrix $\boldsymbol{A} = [\boldsymbol{I}_n \mid \boldsymbol{D}^1(x_1, \dots, x_n)]$, we would be able to decide whether $M(\boldsymbol{A})$, a spike by Proposition 3.2, is the free spike by Lemmas 5.8 and 5.9. Hence the statement and (5.5) are concluded by Proposition 5.7. ∎

**Acknowledgments**

The research has been supported by Czech research grant GAČR 201/05/0050, and by the Institute of Theoretical Computer Science, project 1M0545. The author would in particular like to express his thanks to an anonymous referee of the paper [9], who suggested to extend our complexity results (on spikes and swirls) in the direction towards the $\mathbb{F}$-representability problem.

## References

1. B. Courcelle, S. Oum, *Vertex-Minors, Monadic Second-Order Logic, and a Conjecture by Seese*, J. Combin. Theory Ser. B, to appear (accepted 2006).
2. M.R. Garey, D.S. Johnson, Computers and Intractability, W.H. Freeman and Company, New York 1979.
3. J.F. Geelen, A.H.M. Gerards, A. Kapoor, *The excluded minors for $GF(4)$-representable matroids*, J. Combin. Theory Ser. B 79 (2000), 247–299.
4. J.F. Geelen, A.H.M. Gerards, G.P. Whittle, *Branch-Width and Well-Quasi-Ordering in Matroids and Graphs*, J. Combin. Theory Ser. B 84 (2002), 270–290.
5. J.F. Geelen, A.H.M. Gerards, G.P. Whittle, *Excluding a Planar Graph from a $GF(q)$-Representable Matroid*, manuscript, 2003.
6. J.F. Geelen, A.H.M. Gerards, G.P. Whittle, *Inequivalent Representations of Matroids I: An Overview*, in preparation, 2005.
7. P. Hliněný, *On Matroid Properties Definable in the MSO Logic*, In: Math Foundations of Computer Science MFCS 2003, Lecture Notes in Computer Science 2747, Springer Verlag Berlin (2003), 470–479.
8. P. Hliněný, *Branch-Width, Parse Trees, and Monadic Second-Order Logic for Matroids*, J. Combin. Theory Ser. B 96 (2006), 325–351.
9. P. Hliněný, *On Some Hard Problems on Matroid Spikes*, Theory of Computing Systems, to appear (accepted 2005).
10. P. Hliněný, D. Seese, *Trees, Grids, and MSO Decidability: from Graphs to Matroids*, Theoretical Computer Sci. 351 (2006), 372–393.
11. D. Mayhew, *Matroid Complexity and Large Inputs*, manuscript, 2005.
12. J.G. Oxley, Matroid Theory, Oxford University Press, 1992.
13. J.G. Oxley, D. Vertigan, G. Whittle, *On Inequivalent Representations of Matroids over Finite Fields*, J. Combin. Theory Ser. B 67 (1996), 325–343.
14. N. Robertson, P.D. Seymour, *Graph Minors – A Survey*, Surveys in Combinatorics, Cambridge Univ. Press 1985, 153–171.
15. N. Robertson, P.D. Seymour, *Graph Minors XX: Wagner's Conjecture*, J. Combin. Theory Ser. B 92 (2004), 325–357.
16. P.D. Seymour, *Decomposition of Regular Matroids*, J. Combin. Theory Ser. B 28 (1980), 305–359.