Cycle bases for lattices of binary matroids with no Fano dual minor and their one-element extensions

Tamás Fleiner
CWI, Amsterdam

Winfried Hochstättler
Center for Parallel Computing
University of Cologne

Monique Laurent
CWI, Amsterdam

Martin Loebl
Department of Applied Mathematics
Charles University, Prague

November 11, 1998

Abstract

In this paper we study the question of existence of a cycle basis (that is, a basis consisting only of cycles) for the lattice $\mathbb{Z}(\mathcal{M})$ generated by the cycles of a binary matroid $\mathcal{M}$. We show that, if $\mathcal{M}$ has no Fano dual minor, then the set of fundamental circuits of any maximal independent set of $\mathcal{M}$ can be completed to a cycle basis of $\mathbb{Z}(\mathcal{M})$; moreover, for any one-element extension $\mathcal{M}'$ of such matroid $\mathcal{M}$, any cycle basis for $\mathbb{Z}(\mathcal{M})$ can be completed to a cycle basis for $\mathbb{Z}(\mathcal{M}')$.

1 Introduction

Let $\mathcal{M} = (E, \mathcal{C})$ be a binary matroid on a (finite) set E with cycle space $\mathcal{C}$; that is, $\mathcal{C}$ is a family of subsets of E which is closed under taking symmetric differences, whose members are called the *cycles* of $\mathcal{M}$. The minimal nonempty cycles are called *circuits*; then every nonempty cycle is a disjoint union of circuits. In this paper we consider the set

$$\mathbb{Z}(\mathcal{M}) := \{\sum_{C\in\mathcal{C}} \lambda_C \chi^C \mid \lambda_C \in \mathbb{Z} \ \forall C \in \mathcal{C}\}.$$

The set $\mathbb{Z}(\mathcal{M})$ is clearly a *lattice* (that is, a discrete subgroup of $\mathbb{R}^E$), called the *cycle lattice* of $\mathcal{M}$; a basis of $\mathbb{Z}(\mathcal{M})$ consisting only of cycles of $\mathcal{M}$ is called a *cycle basis*. Recall that a *basis* of a lattice L is a set B of linearly independent vectors of L that *generates* L, i.e., such that every vector $x \in L$ can be expressed as $x = \sum_{b\in B} \lambda_b b$ for some integers λ_b. As is well known, a lattice generated by integral vectors admits a basis consisting only of integral vectors (cf. chap. 4.1 in [15]). However a generating set of a lattice does not necessarily contain a basis of the lattice in general.

Hochstättler and Loebl [7] conjectured that every cycle lattice admits a cycle basis. This conjecture is, in fact, a special case of a more general problem posed by Deza, Grishukhin and Laurent ([2],[3]) in the setting of Delaunay polytopes (see below for details). Galluccio and Loebl showed the validity of this conjecture for graphic matroids ([4]) and, more generally, for binary matroids with no F_7^* minor ([5]). The proof given in [5] relies on Seymour's decomposition results for matroids with no F_7^* minor ([16]).

In this paper we give a short and elementary proof for the fact that the cycle lattice of a binary matroid with no F_7^* minor has a cycle basis and we show that the cycle lattice of a one-element extension of such matroid also has a cycle basis. More precisely, we show that, if $\mathcal{M}$ is a binary matroid with no F_7^* minor, then a cycle basis of $\mathbb{Z}(\mathcal{M})$ can be obtained from any set of fundamental circuits (thus a basis over $GF(2)$) by adding some circuits that are the symmetric difference of two fundamental ones; the main ingredient for this result is the fact that there exist two fundamental circuits of $\mathcal{M}$ intersecting in exactly one element (cf. Theorem 2.2). If $\mathcal{M}'$ is a one-element extension of $\mathcal{M}$, then one can extend any cycle basis of $\mathbb{Z}(\mathcal{M})$ by an appropriate set of circuits of $\mathcal{M}'$ in order to obtain a cycle basis of the cycle lattice of $\mathcal{M}'$. Moreover, in both cases we can construct efficiently the above mentioned cycle bases.

Although cycle bases can be constructed for some other specific instances of matroids, e.g., for projective spaces and their duals, the question of existence of a cycle basis remains open for general binary matroids, even for the binary matroids having the so-called lattice of circuits property (see below for the definition). We will make some further observations concerning these matroids in Remark 2.6.

The question of existence of a basis of a special kind has been considered for other lattices generated by combinatorial objects, for instance, for the lattice generated by the incidence vectors of the perfect matchings of a graph. This lattice has been studied extensively by Lovász [8]; Carvalho, Lucchesi and Murty [13] have shown that this lattice has a basis consisting only of perfect matchings, answering a question posed by Murty [12].

In what follows, we introduce some definitions and preliminaries that are needed in the paper. Our notation and terminology are fairly standard and can be found, e.g., in the textbooks by Oxley [14] and Welsh [18]. We will use the following notation: For a set $A \subseteq E$, we let $\chi^A \in \{0,1\}^E$ denote its *incidence vector*, i.e., $\chi^A_e := 1$ if and only if $e \in A$. Moreover, for a finite subset $X \subseteq \mathbb{R}^E$, we set:

$$\mathbb{Z}(X) := \{\sum_{x \in X} \lambda_x x \mid \lambda_x \in \mathbb{Z}\ \forall x \in X\}.$$

Definitions and facts about matroids. Let $\mathcal{M} = (E, \mathcal{C})$ be a binary matroid. Setting

$$\mathcal{C}^* := \{D \subseteq E : |D \cap C| \in 2\mathbb{Z}\ \forall C \in \mathcal{C}\},$$

$\mathcal{M}^* := (E, \mathcal{C}^*)$ is also a binary matroid, called the *dual* of $\mathcal{M}$; the members of $\mathcal{C}^*$ are called the *cocycles* of $\mathcal{M}$. The minimal nonempty cocycles are called the *cocircuits* of $\mathcal{M}$.

A set $I \subseteq E$ is *independent* in $\mathcal{M}$ if it contains no circuit; the maximum cardinality of an independent set is the *rank* of $\mathcal{M}$. Let T be a maximal independent set in $\mathcal{M}$. For $e \in E \setminus T$, let $C_e \in \mathcal{C}$ denote the *fundamental circuit* of e with respect to T; that is, C_e is the unique circuit such that $e \in C_e \subseteq T \cup \{e\}$.

An element $e \in E$ is a *coloop* of $\mathcal{M}$ if $\{e\}$ is a cocircuit and two distinct elements $e, f \in E$ are said to be *coparallel* if $\{e, f\}$ is a cocircuit. A *coparallel class* P is a maximal subset of E whose elements are pairwise coparallel and are not coloops. The matroid $\mathcal{M}$ is said to be *cosimple* if every cocircuit has cardinality ≥ 3.

The cycle space of a binary matroid $\mathcal{M}$ on E can be realized as the set of solutions $x \in \{0,1\}^E$ of a linear equation of the form: $Mx \equiv 0$ (modulo 2), for some binary matrix M whose columns are indexed by E; such matrix M is called a *representation matrix* of $\mathcal{M}$.

The *Fano matroid* F_7 is the matroid on $E := \{1, \ldots, 7\}$ represented by the matrix:

$$\begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

and the *Fano dual matroid* is the dual F_7^* of F_7. For $r \geq 2$, the *projective space* $\mathcal{P}_r$ is the binary matroid represented by the $r \times (2^r - 1)$ matrix whose columns are all nonzero 0,1-vectors of length r; hence, $\mathcal{P}_r$ has rank r and $\mathcal{P}_3 = F_7$.

Let $\mathcal{M} = (E, \mathcal{C})$ be a binary matroid and let $e \in E$. Setting

$$\mathcal{C}\backslash e := \{C \in \mathcal{C} \mid e \notin C\}, \ \mathcal{C}/e := \{C \setminus \{e\} \mid C \in \mathcal{C}\},$$

then $\mathcal{M}\backslash e := (E \setminus \{e\}, \mathcal{C}\backslash e)$ and $\mathcal{M}/e := (E \setminus \{e\}, \mathcal{C}/e)$ are binary matroids obtained from $\mathcal{M}$ by, respectively, *deleting* and *contracting* e. A *minor* of $\mathcal{M}$ is any binary matroid $\mathcal{N}$ that can be obtained from $\mathcal{M}$ by a sequence of deletions and/or contractions.

The lattice of circuits property. Let $\mathcal{M} = (E, \mathcal{C})$ be a binary matroid. Then, the following holds obviously for all $x \in \mathbb{Z}(\mathcal{M})$:

(1.1) $\quad \sum_{e \in D} x_e$ is even for all cocircuits $D \in \mathcal{C}^*$,

(1.2) $\quad x_f = x_g$ if f and g are coparallel in $\mathcal{M}$,

(1.3) $\quad x_e = 0$ if e is a coloop of $\mathcal{M}$.

Following Goddyn [6], we say that $\mathcal{M}$ has the *lattice of circuits property*[1] if the above conditions (1.1)-(1.3) characterize $\mathbb{Z}(\mathcal{M})$; that is, if any $x \in \mathbb{Z}^E$ satisfying

[1]This terminology reflects the analogy with the *sums of circuits property* considered by Seymour [17], a binary matroid having the latter property if the cone generated by its cycles is completely described by some 'obvious necessary' linear conditions. Lovász and Seress [10] call a binary matroid $\mathcal{M}$ *Eulerian* if its dual $\mathcal{M}^*$ has the lattice of circuits property.

(i)-(iii) belongs to $\mathbb{Z}(\mathcal{M})$. As can easily be verified, $\mathcal{M}$ has the lattice of circuits property if and only if $2\chi^P \in \mathbb{Z}(\mathcal{M})$ for every coparallel class P of $\mathcal{M}$. Recall that the dual lattice of $\mathbb{Z}(\mathcal{M})$ is given by

$$(\mathbb{Z}(\mathcal{M}))^* := \{x \in \mathbb{R}^E \mid \sum_{e \in C} x_e \in \mathbb{Z} \ \forall C \in \mathcal{C}\}.$$

Then, assuming $\mathcal{M}$ cosimple, $\mathcal{M}$ has the lattice of circuits property if and only if $(\mathbb{Z}(\mathcal{M}))^*$ is contained in $\frac{1}{2}\mathbb{Z}^E$. Note that F_7^* does not have the lattice of circuits property since $\frac{1}{4}\chi^E \in (\mathbb{Z}(F_7^*))^*$.

Cunningham [1] has proved that, if $\mathcal{M}$ has no F_7^* minor then, for every element e, there exist two circuits C, C' such that $C \cap C' = \{e\}$ if and only if every cocircuit containing e has cardinality ≥ 3; this implies that every binary matroid with no F_7^* minor has the lattice of circuits property. Note that Theorem 2.2 and Corollary 2.3 below can be seen as a variation of Cunningham's result. Lovász and Seress ([10],[11]) studied the lattice of circuits property in detail. In particular, they have given several equivalent characterizations for the binary matroids having the lattice of circuits property and they have shown that, if $\mathcal{M}$ is cosimple with no $\mathcal{P}_{r+1}^*$ minor, then $2^{r-1}\mathbb{Z}^E \subseteq \mathbb{Z}(\mathcal{M})$.

The *dimension* of the cycle lattice $\mathbb{Z}(\mathcal{M})$, denoted as dim $\mathcal{M}$, is equal to the number of coparallel classes of $\mathcal{M}$. In view of relations (1.2) and (1.3), we may assume without loss of generality that $\mathcal{M}$ is cosimple, in which case $\mathbb{Z}(\mathcal{M})$ is full-dimensional. We will often use the observation that if $\mathcal{B}$ is a set of cycles of $\mathcal{M}$ which generates the lattice $\mathbb{Z}(\mathcal{M})$ and has cardinality $|\mathcal{B}| = \dim\ \mathcal{M}$, then $\mathcal{B}$ is a basis of $\mathbb{Z}(\mathcal{M})$.

The basis question for Delaunay polytopes. Let $P \subseteq \mathbb{R}^k$ be a full-dimensional polytope with set of vertices V_P admitting the origin as a vertex. Then, P is said to be a *Delaunay polytope* if it satisfies the following conditions: (i) the set $L := \mathbb{Z}(V_P)$ is a lattice; (ii) P is inscribed on a sphere; that is, $\|x - c\| = r$ for all $x \in V_P$, for some $r > 0$ and $c \in \mathbb{R}^k$ with $\|c\| = r$; (iii) $\|x - c\| \geq r$ for all $x \in L$, with equality if and only if $x \in V_P$. (Here, $\|x\|$ denotes the Euclidean norm of $x \in \mathbb{R}^k$.) Deza, Grishukhin and Laurent ([2],[3]) posed the following question:

> Given a Delaunay polytope P, is it always possible to find a basis of the lattice $L = \mathbb{Z}(V_P)$ consisting only of vertices of P ?

No example of a Delaunay polytope is known for which this question has a negative answer. On the other hand, a basis consisting only of vertices has been constructed for several concrete instances of Delaunay polytopes in [2]. In fact, the question of existence of a cycle basis for a cycle lattice arises as a special instance of the above problem. Indeed, for a binary matroid $\mathcal{M} = (E, \mathcal{C})$, let conv$(\mathcal{C})$ denote the polytope in $\mathbb{R}^E$ defined as the convex hull of the incidence vectors of the cycles of $\mathcal{M}$. Then, as we see below, conv$(\mathcal{C})$ is a Delaunay polytope in the lattice $\mathbb{Z}(\mathcal{M})$.

Lemma 1.4. *Let X be a finite full-dimensional subset of $\{0,1\}^k$ and set $Y :=$*

$\mathbb{Z}(X) \cap \{0,1\}^k$. *Then, the polytope* $\mathrm{conv}(Y)$ *is a Delaunay polytope.*

PROOF. The polytope $P := \mathrm{conv}(Y)$ is full-dimensional in $\mathbb{R}^k$ since X is full-dimensional. Assertion (i) holds obviously since Y consists of integer vectors. Let S denote the sphere in $\mathbb{R}^k$ with center $c := (\frac{1}{2}, \ldots, \frac{1}{2})$ and radius $r := \frac{1}{2}\sqrt{|E|}$. Then all points of Y lie on the sphere S, i.e., (ii) holds. We have that $\|x - c\|^2 - r^2 = \sum_{e \in E} x_e(x_e - 1) \geq 0$ for all $x \in \mathbb{Z}(X)$. Moreover, equality holds if and only if $x \in \{0,1\}^k$, i.e., if $x \in Y$; thus, (iii) holds. This shows that P is a Delaunay polytope. ∎

Note that, with the notation of Lemma 1.4, it may happen that X is a proper subset of Y. For such an example, let X consist of the unit vectors in $\mathbb{R}^k$ in which case $Y = \{0,1\}^k$. On the other hand, if X consists of the incidence vectors of the cycles of a binary matroid $\mathcal{M}$, then equality $X = Y$ holds. Indeed, the only $(0,1)$-vectors in the cycle lattice $\mathbb{Z}(\mathcal{M})$ are the incidence vectors of cycles (which follows essentially from the fact that $(\mathcal{M}^*)^* = \mathcal{M}$). (Note that the equality: $\mathbb{Z}(X) \cap \{0,1\}^k = X$ for a finite subset $X \subseteq \{0,1\}^k$, does not imply that X is closed under taking symmetric differences, i.e., X is not necessarily the cycle space of a binary matroid. For a counterexample, consider the set $X \subseteq \{0,1\}^4$ consisting of the vectors $(0,0,0,0)$, $(1,1,1,0)$, $(1,1,0,1)$, $(1,0,1,1)$ and $(0,1,1,1)$.

Corollary 1.5. *Let* $\mathcal{M} = (E, \mathcal{C})$ *be a cosimple binary matroid. Then, the polytope* $\mathrm{conv}(\mathcal{C})$ *which is defined as the convex hull of the incidence vectors of the cycles of* $\mathcal{M}$*, is a Delaunay polytope.* ∎

2 Cycle basis for matroids with no F_7^* minor

We indicate here a very simple method for constructing a cycle basis of the cycle lattice of any binary matroid with no F_7^* minor. It consists of extending a set of fundamental circuits (thus a basis over $GF(2)$) to a basis of the cycle lattice by adding some circuits obtained as symmetric difference of two fundamental circuits. This method can also be applied to some other binary matroids, for instance, to projective spaces.

Let $\mathcal{M} = (E, \mathcal{C})$ be a binary matroid, let T be a maximal independent set in $\mathcal{M}$, set $\overline{T} := E \setminus T$ and, for $e \in \overline{T}$, let C_e denote its fundamental circuit. So, $|T| = r$ if $\mathcal{M}$ has rank r and $r \leq |E| - 2$ if $\mathcal{M}$ is cosimple. We start with an easy observation.

Lemma 2.1. *Let* $\mathcal{A}$ *be a set of vectors in* $\mathbb{Z}^E$*. If* $\mathcal{A}$ *generates (over* $\mathbb{Z}$*) the fundamental circuits of a given maximal independent set* T *of* $\mathcal{M}$ *and the vectors* $2\chi^e$ *(for* $e \in T$*), then* $\mathcal{A}$ *generates all elements in* $\mathbb{Z}(\mathcal{M})$ *and in* $2\mathbb{Z}^E$.

PROOF. Let C be a cycle in M. Then, C is the symmetric difference of the fundamental circuits C_e for $e \in C \cap \overline{T}$. Hence, $x := \chi^C - \sum_{e \in C \cap \overline{T}} \chi^{C_e}$ is an even vector (i.e., $x \in 2\mathbb{Z}^E$) which is zero on $\overline{T}$. Hence, $x \in \mathbb{Z}(\mathcal{A})$ by the assumption, which implies that $\chi^C \in \mathbb{Z}(\mathcal{A})$ too. Finally, for $e \in \overline{T}$, $\mathcal{A}$ generates $2\chi^e$ since $2\chi^e = 2\chi^{C_e} - 2\chi^{C_e \cap T}$. ∎

The following result will be the main tool for constructing a cycle basis.

Theorem 2.2. *Let $\mathcal{M}$ be a cosimple binary matroid with no F_7^* minor. Let T be a maximal independent set in $\mathcal{M}$ and assume that $|T| \geq 1$. Then there exist two fundamental circuits C and C' such that $|C \cap C'| = 1$.*

PROOF. We begin with observing that, as $\mathcal{M}$ is cosimple and the fundamental circuits generate over $GF(2)$ all cycles, then for any distinct elements $e, f \in E$ there exists a fundamental circuit C such that $|C \cap \{e, f\}| = 1$. From this follows that there exist two distinct nondisjoint fundamental circuits. Let C_x and C_y (where $x, y \in \overline{T}$) be two fundamental circuits for which $C_x \cap C_y \neq \emptyset$ and $|C_x \cap C_y|$ is minimum. If $|C_x \cap C_y| = 1$ we are done. Else, let $e, f \in C_x \cap C_y$, $e \neq f$, and let C_z be a fundamental circuit such that $|C_z \cap \{e, f\}| = 1$; say, $e \in C_z$, $f \notin C_z$. Then, there exists an element $g \in C_z \cap (C_x \setminus C_y)$ since, by our minimality assumption, $C_z \cap C_x \not\subseteq C_x \cap C_y \setminus \{f\}$. Similarly, there exists an element $h \in C_z \cap (C_y \setminus C_x)$. Set $X := \overline{T} \setminus \{x, y, z\}$ and $Y := T \setminus \{e, f, g, h\}$ and consider the matroid $\mathcal{M}' := \mathcal{M} \backslash X / Y$. Then, the circuits C_x, C_y, C_z have the following form:

$$\begin{array}{c} \\ C_x \\ C_y \\ C_z \end{array} \begin{array}{c} \begin{array}{cccccccccc} e & f & g & h & Y & x & y & z & X \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & * & 1 & 0 & 0 & 0\ldots0 \\ 1 & 1 & 0 & 1 & * & 0 & 1 & 0 & 0\ldots0 \\ 1 & 0 & 1 & 1 & * & 0 & 0 & 1 & 0\ldots0 \end{pmatrix} \end{array}.$$

Thus, $\{e, f, g, h\}$ is a maximal independent set of $\mathcal{M}'$ with fundamental circuits the sets $\{e, f, g, x\}$, $\{e, f, h, y\}$, and $\{e, g, h, z\}$. Therefore, $\mathcal{M}'$ coincides with the Fano dual matroid F_7^*, which contradicts our assumption that $\mathcal{M}$ has no F_7^* minor. ∎

Corollary 2.3. *Let $\mathcal{M}$ be a cosimple binary matroid with no F_7^* minor. Let T be a maximal independent set in $\mathcal{M}$ and assume that $r := |T| \geq 1$. Then, the elements of T can be ordered as $e_1, \ldots, e_r$ in such a way that, for every $i = 1, \ldots, r$, there exist two fundamental circuits C_i, C_i' such that $e_i \in C_i \cap C_i' \subseteq \{e_1, \ldots, e_i\}$.*

PROOF. We show the result by induction on the size of the groundset. By Theorem 2.2, there exists an element $e_1 \in T$ and two fundamental circuits C_1, C_1' (with respect to $\mathcal{M}$, T) such that $C_1 \cap C_1' = \{e_1\}$. We are done if $|T| = 1$. Otherwise, we consider $\mathcal{M}' := \mathcal{M}/e_1$. Then, $T \setminus \{e_1\}$ is a maximal independent set in $\mathcal{M}'$. Applying the induction assumption to $\mathcal{M}'$ which is cosimple with no F_7^* minor, we obtain that the elements of $T \setminus \{e_1\}$ can be ordered as $e_2, \ldots, e_r$ in such a way that, for every $i = 2, \ldots, r$, there exist two fundamental circuits D_i, D_i' (with respect to $\mathcal{M}'$, $T \setminus \{e_1\}$) such that $e_i \in D_i \cap D_i' \subseteq \{e_2, \ldots, e_i\}$.

Then, $D_i = C_i \setminus \{e_1\}$, $D'_i = C'_i \setminus \{e_1\}$ where C_i, C'_i are circuits of $\mathcal{M}$. In fact, C_i, C'_i are also fundamental circuits with respect to T in $\mathcal{M}$ as each of them contains a unique element of $\overline{T}$. Moreover, $e_i \in C_i \cap C'_i \subseteq \{e_1, e_2, \ldots, e_i\}$. ∎

An immediate application of Corollary 2.3 is that $2\mathbb{Z}^E \subseteq \mathbb{Z}(\mathcal{M})$ for any cosimple binary matroid $\mathcal{M}$ with no F_7^* minor; in other words, matroids with no F_7^* minor have the lattice of circuits property. We formulate below further consequences.

Corollary 2.4. *Let $\mathcal{M}$ be a binary matroid with no F_7^* minor, let P be a coparallel class of $\mathcal{M}$, and let r denote the rank of $\mathcal{M}$.*

(i) The lattice $\mathbb{Z}(\mathcal{M})$ has a basis consisting only of circuits of $\mathcal{M}$; such a basis can be obtained by extending the set of fundamental circuits of an arbitrary maximal independent set by r circuits, each of them being the symmetric difference of two fundamental circuits.

(ii) There exist a circuit C_P and a set $\mathcal{A}$ of circuits of $\mathcal{M}$ such that the set $\mathcal{A} \cup \{C_P\}$ is a basis of the lattice $\mathbb{Z}(\mathcal{M})$ and the set $\{C \setminus P \mid C \in \mathcal{A}\}$ is a basis of the lattice $\mathbb{Z}(\mathcal{M}/P)$.

Proof. We can assume without loss of generality that $\mathcal{M}$ is cosimple. We first verify (i). Let T be a maximal independent set in $\mathcal{M}$ ($|T| = r$) and let C_e ($e \in \overline{T}$) denote the associated fundamental circuits. If $r = 0$, then the result is obvious as the fundamental circuits $C_e = \{e\}$ ($e \in E$) constitute a cycle basis. We now assume that $r \geq 1$. Let $T = \{e_1, \ldots, e_r\}$ and let C_i, C'_i be the fundamental circuits provided by Corollary 2.3. Then we consider the set $\mathcal{B}$ consisting of the fundamental circuits C_e ($e \in \overline{T}$) together with the circuits $C_{e_i} := C_i \triangle C'_i$ (for $e_i \in T$). It follows from Corollary 2.3 that $\mathcal{B}$ generates $2\chi^e$ for $e \in T$. According to Lemma 2.1, this implies that $\mathcal{B}$ generates all elements in $\mathbb{Z}(\mathcal{M})$. Hence, $\mathcal{B}$ is a basis of $\mathbb{Z}(\mathcal{M})$ since $|\mathcal{B}| = |E|$ and, thus, (i) holds. We now verify (ii). As $\mathcal{M}$ is cosimple, we have that $P := \{p\}$. If $\{p\}$ is a circuit, then $\mathcal{M}/p = \mathcal{M} \backslash p$ and, thus, (ii) holds if we set $C_P := C_p$ and $\mathcal{A} := \mathcal{B} \setminus \{C_P\}$, where $\mathcal{B}$ is the cycle basis of $\mathbb{Z}(\mathcal{M})$ constructed above. Otherwise, we set again $C_P := C_p$ and $\mathcal{A} := \mathcal{B} \setminus \{C_P\}$, where $\mathcal{B}$ is the basis constructed above after chosing for T a maximal independent set of $\mathcal{M}$ containing p. Observe moreover that the above construction applied to matroid $\mathcal{M}/p$ and its maximal independent set $T \setminus \{p\}$ shows that the set $\{C \setminus P \mid C \in \mathcal{A}\}$ is a basis of $\mathbb{Z}(\mathcal{M}/p)$. Hence, (ii) holds. ∎

We close this section with some remarks on possible further applications of the above construction method, as well as its limits and open questions.

Remark 2.5. The projective space. Recall that the projective space $\mathcal{P}_r$ is the matroid defined on the set $E := GF(2)^r \setminus \{0\}$ whose cycles are the linearly dependent (over $GF(2)$) subsets of E. As we now see, the construction method presented earlier in this section applies very easily for finding a cycle basis of the lattice $\mathbb{Z}(\mathcal{P}_r)$. Indeed, let $T := \{e_1, \ldots, e_r\}$ be a maximal independent set in $\mathcal{P}_r$. We can suppose that $r \geq 3$ (else there is obviously a basis of cycles).

Then, every element $e_i \in T$ is the intersection of two fundamental circuits. For instance, the two fundamental circuits $\{e_1, e_2, e_1 \oplus e_2\}$ and $\{e_1, e_3, e_1 \oplus e_3\}$ meet in e_1. Therefore, the conclusion of Theorem 2.2 holds and, thus, the cycle lattice of $\mathcal{P}_r$ has a basis consisting of cycles.

Note that the above construction method does not apply to the Fano dual matroid $\mathcal{P}_3^* = F_7^*$. Indeed, the result from Theorem 2.2 does not hold for F_7^* since all pairwise intersections of its circuits have cardinality 2. However, the technique from the next section will apply to the matroid F_7^* since F_7^* is obviously a one-element extension of a matroid with no F_7^* minor. In fact, the cycle lattice of F_7^* and, more generally, of the dual $\mathcal{P}_r^*$ of the projective space has obviously a cycle basis, since the nonempty cycles of $\mathcal{P}_r^*$ are linearly independent over $\mathbb{R}$.

Remark 2.6. Matroids with the lattice of circuits property. Let us note again that the question of existence of a cycle basis for the cycle lattice remains open for general binary matroids with the lattice of circuits property. We mention here a possible way of attacking this question. Let $\mathcal{M} = (E, \mathcal{C})$ be a cosimple binary matroid, let T be a maximal independent subset of E, let C_e ($e \in \overline{T}$) be the corresponding fundamental circuits, and let W denote the matrix whose rows are the incidence vectors of the sets $C_e \cap C_f$ (for $e, f \in \overline{T}$). Lovász and Seress [10] have shown that $\mathcal{M}$ has the lattice of circuits property if and only if the matrix W has full column rank $|E|$ over $GF(2)$. If we could find a set I of pairs (e, f) ($e \neq f \in \overline{T}$) for which the submatrix W_I with rows C_e ($e \in \overline{T}$) and $C_e \cap C_f$ ($(e, f) \in I$) has its determinant equal to 1, then the set $\{C_e \ (e \in \overline{T}),\ C_e \triangle C_f \ ((e, f) \in I)\}$ would be a cycle basis of $\mathbb{Z}(\mathcal{M})$. What we have shown in Corollary 2.3 is that this goal of finding a submatrix W_I with determinant 1 can be achieved in the special case when $\mathcal{M}$ has no F_7^* minor. Note that for general matroids with the lattice of circuits property, by the above mentioned result of Lovász and Seress, there exists an index set I for which the submatrix W_I has its determinant equal to 1 modulo 2 !

3 One-element extensions of matroids with no Fano dual minor

Given a binary matroid $\mathcal{M}$ on a set E, a *one-element extension* of $\mathcal{M}$ is any binary matroid $\mathcal{N}$ on $E \cup \{t\}$ (where t is an additional element not belonging to E) such that $\mathcal{N} \backslash t = \mathcal{M}$. We show in this section that, if $\mathcal{M}$ is a matroid with no F_7^* minor, then the cycle lattice of any one-element extension of $\mathcal{M}$ also admits a cycle basis, obtained by extending any cycle basis of the cycle lattice of $\mathcal{M}$.

One-element extensions can be described in the following manner. Let $\mathcal{M}$ be a binary matroid on E and let Σ be a subset of E. Call a set $A \subseteq E$ Σ-*even* (resp. Σ-*odd*) if $|A \cap \Sigma|$ is even (resp. odd). Let $\mathcal{M}_\Sigma$ denote the binary matroid on $E \cup \{t\}$ (t is an additional element not belonging to E) whose cycles are the cycles of $\mathcal{M}$ and the sets $(C \triangle \Sigma) \cup \{t\}$, where C is a cycle of $\mathcal{M}$; hence, the cocycles of $\mathcal{M}_\Sigma$ are the Σ-even cocycles of $\mathcal{M}$ and the sets $D \cup \{t\}$ where D is a Σ-odd cocycle of $\mathcal{M}$. Obviously, $\mathcal{M}_\Sigma = \mathcal{M}_{C \triangle \Sigma}$ for any cycle C of $\mathcal{M}$. Clearly, $\mathcal{M}_\Sigma \backslash t = \mathcal{M}$ and any one-element extension of $\mathcal{M}$ is of the form $\mathcal{M}_\Sigma$ for an appropriate $\Sigma \subseteq E$.

It is useful to observe how the contraction operation applies to the one-element extension matroid $\mathcal{M}_\Sigma$; namely, $\mathcal{M}_\Sigma / f = (\mathcal{M}/f)_{\Sigma \setminus \{f\}}$ for any $f \in E$.

When $\mathcal{M}$ is a graphic matroid, the matroid $\mathcal{M}_\Sigma$ is also known under the name of *graft matroid* (cf. [9], [16]); Goddyn [6] has posed the question of describing the cycle lattice of graft matroids. Note that the Fano dual matroid F_7^* is, in fact, a graft matroid. Indeed, F_7^* can be seen as a one-element extension of the graphic matroid of the complete bipartite graph $K_{2,3}$, taking for Σ the set of edges adjacent to a given node of degree 3. Hence, the results of this section apply for constructing a cycle basis of $\mathbb{Z}(F_7^*)$. Moreover, this example shows that the one-element extension of a matroid with the lattice of circuits property does not need to have this property. We will give in Corollary 3.2 a characterization of the one-element extensions of matroids with no F_7^* minor having the lattice of circuits property.

Theorem 3.1. *Let $\mathcal{M}$ be a binary matroid on E with no F_7^* minor, let $\Sigma \subseteq E$, and let $\mathcal{M}_\Sigma$ be the corresponding one-element extension of $\mathcal{M}$. Then every cycle basis $\mathcal{B}_\mathcal{M}$ of $\mathbb{Z}(\mathcal{M})$ can be extended to a cycle basis $\mathcal{B}$ of $\mathbb{Z}(\mathcal{M}_\Sigma)$; moreover, if all members of $\mathcal{B}_\mathcal{M}$ are circuits then the same can be assumed about $\mathcal{B}$.*

Proof. We begin with noting that it suffices to show the result for one specific basis of $\mathbb{Z}(\mathcal{M})$; indeed, if $\mathcal{B}_\mathcal{M}$ and $\mathcal{B}'_\mathcal{M}$ are two bases of $\mathbb{Z}(\mathcal{M})$ and if $\mathcal{B}_\Sigma$ is a set of cycles of $\mathcal{M}_\Sigma$ for which $B_\mathcal{M} \cup \mathcal{B}_\Sigma$ is a basis of $\mathbb{Z}(\mathcal{M}_\Sigma)$, then $\mathcal{B}'_\mathcal{M} \cup \mathcal{B}_\Sigma$ too is a basis of $\mathbb{Z}(\mathcal{M}_\Sigma)$. Thus we fix a basis $\mathcal{B}_\mathcal{M}$ of $\mathbb{Z}(\mathcal{M})$ consisting only of circuits (it exists by Corollary 2.4). We show that we can find a set of circuits of $\mathcal{M}_\Sigma$ which together with $\mathcal{B}_\mathcal{M}$ forms a basis of $\mathbb{Z}(\mathcal{M}_\Sigma)$. The proof is by induction on $|E|$. As observed earlier, we may assume without loss of generality that the matroid $\mathcal{M}_\Sigma$ is cosimple. Hence, $\mathcal{M}$ has no coloop, but $\mathcal{M}$ may contain some cocircuits of size 2, all of them being Σ-odd. Therefore, every coparallel class P of $\mathcal{M}$ satisfies $|P \cap \Sigma| \leq 1$ and $|P \setminus \Sigma| \leq 1$. We distinguish the following two cases.

Case 1: All coparallel classes of $\mathcal{M}$ have cardinality 2. Then, the set

$$\mathcal{B} := \mathcal{B}_\mathcal{M} \cup \{(C \triangle \Sigma) \cup \{t\} \mid C \in \mathcal{B}_\mathcal{M}\} \cup \{\Sigma \cup \{t\}\}$$

is a cycle basis of $\mathbb{Z}(\mathcal{M}_\Sigma)$. Indeed, as $\mathcal{B}$ has the right cardinality, it suffices to verify that it generates all cycles of $\mathcal{M}_\Sigma$. For this, let C be a cycle of $\mathcal{M}$; then

$$\chi^C = \sum_{B \in \mathcal{B}_\mathcal{M}} \lambda_B \chi^B$$

where the λ_B's are integers. Therefore,

$$\chi^{(C \triangle \Sigma) \cup \{t\}} = \sum_{B \in \mathcal{B}_\mathcal{M}} \lambda_B \chi^{(B \triangle \Sigma) \cup \{t\}} + (1 - \sum_{B \in \mathcal{B}_\mathcal{M}} \lambda_B) \chi^{\Sigma \cup \{t\}}$$

belongs to $\mathbb{Z}(\mathcal{B})$.

Case 2: $\mathcal{M}$ has a coparallel class $P := \{p\}$ of cardinality 1. By Corollary 2.4, there exist a circuit C_P and a set $\mathcal{A}$ of circuits of $\mathcal{M}$ such that $B_{\mathcal{M}} := \mathcal{A} \cup \{C_P\}$ is a basis of $\mathbb{Z}(\mathcal{M})$ and $\mathcal{A}' := \{A \setminus P \mid A \in \mathcal{A}\}$ is a basis of $\mathbb{Z}(\mathcal{M}/p)$. By the induction assumption applied to matroid $\mathcal{M}/p$, there exists a set $\mathcal{D}'$ of circuits of $(\mathcal{M}/p)_{\Sigma\setminus\{p\}} = \mathcal{M}_\Sigma/p$ such that $\mathcal{A}' \cup \mathcal{D}'$ is a basis of $\mathbb{Z}(\mathcal{M}_\Sigma/p)$. For each $D' \in \mathcal{D}'$, let D be a circuit of $\mathcal{M}_\Sigma$ such that $D \setminus \{p\} = D'$ and set $\mathcal{D} := \{D \mid D' \in \mathcal{D}'\}$. We claim that the set $\mathcal{B} := \mathcal{A} \cup \mathcal{D} \cup \{C_P\}$ is a basis of the lattice $\mathbb{Z}(\mathcal{M}_\Sigma)$. As $\mathcal{B}$ has the right cardinality, it suffices to verify that $\mathcal{B}$ generates all cycles of $\mathcal{M}_\Sigma$. Let C be a cycle of $\mathcal{M}_\Sigma$. Then, the set $C \setminus \{p\}$ is a cycle of $\mathcal{M}_\Sigma/p$ and thus is generated by $\mathcal{A}' \cup \mathcal{D}'$. ¿From this follows that $\chi^C + \lambda\chi^p$ is generated by $\mathcal{A} \cup \mathcal{D}$ for some integer λ. If λ is even, then $\lambda\chi^p$ is generated by $\mathcal{A} \cup \{C_P\}$ since $\mathcal{M}$ has the lattice of circuits property; otherwise, $\{p\}$ is a circuit and $C_P = \{p\}$. Hence, χ^C is generated by $\mathcal{B}$ in both cases. ∎

It follows from a result of Lovász and Seress [11] that $4\mathbb{Z}^{E\cup\{t\}} \subseteq \mathbb{Z}(\mathcal{M}_\Sigma)$ if $\mathcal{M}_\Sigma$ is a (cosimple) one-element extension of a matroid $\mathcal{M}$ with no F_7^* minor. The next result characterizes when $\mathcal{M}_\Sigma$ has the lattice of circuits property.

Corollary 3.2. *Let $\mathcal{M}$ be a matroid on E with no F_7^* minor and let $\mathcal{M}_\Sigma$ be a one-element extension of $\mathcal{M}$. Then, $\mathcal{M}_\Sigma$ does not have the lattice of circuits property if and only if there exist elements $e_1, \dots, e_k, f_1, \dots, f_k \in E$ ($k \geq 3$) such that the set $\{e_1, \dots, e_k\}$ is a cocircuit of $\mathcal{M}$ while the sets $\{e_i, f_i\}$ ($i = 1, \dots, k$) are Σ-odd cocircuits of $\mathcal{M}$.*

Proof. Suppose first that such cocircuits exist; we show that $\mathcal{M}_\Sigma$ does not have the lattice of circuits property by constructing a vector $x \in \frac{1}{4}\mathbb{Z}^{E\cup\{t\}} \setminus \frac{1}{2}\mathbb{Z}^{E\cup\{t\}}$ belonging to the dual lattice $(\mathbb{Z}(\mathcal{M}_\Sigma))^*$. For this, set $x(e_i) = x(f_i) := \frac{1}{4}$ ($i = 1, \dots, k$), $x(t) := 0, \frac{3}{4}, \frac{1}{2}, \frac{1}{4}$ if k is congruent to 0,1,2,3 modulo 4, respectively, and $x(e) := 0$ for all remaining elements $e \in E$. We show the converse implication by induction on the size of E. Assume that $\mathcal{M}_\Sigma$ does not have the lattice of circuits property. We can suppose without loss of generality that $\mathcal{M}_\Sigma$ is cosimple. We distinguish again the two cases considered in the proof of Theorem 3.1.

Consider first Case 1; that is, $E = \{e_1, f_1, \dots, e_m, f_m\}$, $\Sigma = \{e_1, \dots, e_m\}$ and $\{e_i, f_i\}$ is a Σ-odd cocircuit of $\mathcal{M}$ for every $i = 1, \dots, m$. Then, $m \geq 3$ for, if not, then $\mathcal{M}_\Sigma$ is a matroid on ≤ 5 elements and thus has the lattice of circuits property. We claim that the set Σ contains a cocircuit of $\mathcal{M}$. Indeed, if Σ contains no cocircuit of $\mathcal{M}$, then Σ is independent in the dual $\mathcal{M}^*$ of $\mathcal{M}$. Moreover, Σ is maximal independent in $\mathcal{M}^*$ since $\Sigma \cup \{f_i\}$ contains a cocircuit for all $i \leq m$. Therefore, $E \setminus \Sigma$ is is maximal independent in $\mathcal{M}$ with associated fundamental circuits the sets $\{e_i, f_i\}$ ($i = 1, \dots, m$). Then, one can easily verify that $2\mathbb{Z}^{E\cup\{t\}} \subseteq \mathbb{Z}(\mathcal{M}_\Sigma)$ and thus $\mathcal{M}$ has the lattice of circuits property. Therefore, Σ contains a cocircuit. Such cocircuit has cardinality ≥ 3 since $\mathcal{M}_\Sigma$ is cosimple and, thus, we are done.

Consider now Case 2; that is, $\mathcal{M}$ has a coparallel class $\{p\}$ of cardinality 1.

We claim that $\mathcal{M}_\Sigma/p$ does not have the lattice of circuits property. For, suppose that $\mathcal{M}_\Sigma/p$ has the lattice of circuits property; then we show that $\mathcal{M}_\Sigma$ too has the lattice of circuits property. Indeed, $2\chi^p \in \mathbb{Z}(\mathcal{M}) \subseteq \mathbb{Z}(\mathcal{M}_\Sigma)$; for $e \in E\setminus\{p\}$, $2\chi^e \in \mathbb{Z}(\mathcal{M}_\Sigma/p)$ which implies that $2\chi^e + \lambda\chi^p \in \mathbb{Z}(\mathcal{M}_\Sigma)$ for some integer λ and, thus, $2\chi^e \in \mathbb{Z}(\mathcal{M}_\Sigma)$; finally, $2\chi^t = 2\chi^{\Sigma\cup\{t\}} - 2\chi^\Sigma \in \mathbb{Z}(\mathcal{M}_\Sigma)$. Using the induction assumption applied to $\mathcal{M}/p$, there exist elements $e_1, f_1, \ldots, e_k, f_k \in E\setminus\{p\}$ ($k \geq 3$) such that $\{e_1, \ldots, e_k\}$ is a cocircuit of $\mathcal{M}/p$ and every $\{e_i, f_i\}$ i a Σ-odd cocircuit of $\mathcal{M}/p$. Hence, we have found the desired cocircuits of $\mathcal{M}$ and we are done. ∎

We conclude this section with an observation on the limits of local constructions. It has been observed in [7] that, given a cycle basis of the cycle lattice of a contraction minor $\mathcal{M}/e$ of a binary matroid $\mathcal{M}$, it is in general not possible to extend it to a cycle basis of the cycle lattice of $\mathcal{M}$. We now give an example showing that the same holds if we are given a cycle basis of a deletion minor $\mathcal{M}\backslash e$ of $\mathcal{M}$.

Lemma 3.3. *Let $\mathcal{M}$ be a cosimple binary matroid on E and let $e \in E$. Assume that $\mathcal{M}$ has the lattice of circuits property and that $\mathcal{M}\backslash e$ does not have the lattice of circuits property. Then any cycle basis for $\mathbb{Z}(\mathcal{M})$ must have at least two cycles containing e. Therefore, if $\mathcal{M}\backslash e$ is cosimple, then no cycle basis of $\mathbb{Z}(\mathcal{M})$ exists that contains a cycle basis of $\mathbb{Z}(\mathcal{M}\backslash e)$.*

Proof. By the assumption, there exists a coparallel class P in $\mathcal{M}\backslash e$ such that $2\chi^P \in \mathbb{Z}(\mathcal{M})\backslash\mathbb{Z}(\mathcal{M}\backslash e)$. This implies that any cycle basis of $\mathbb{Z}(\mathcal{M})$ must contain at least two cycles containing the element e. ∎

As an example of a matroid satisfying the conditions of Lemma 3.3, consider the matroid S_8 on the set $\{e_1, \ldots, e_8\}$ represented by the following matrix:

$$\begin{array}{c}
\begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\
\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1
\end{pmatrix}
\end{array}.$$

Then, $S_8\backslash e_1 \sim F_7^*$, both F_7^* and S_8 are cosimple, and S_8 has the lattice of circuits property while F_7^* does not have it. To see that S_8 has the lattice of circuits property, one can note that S_8 is, in fact, a graft matroid and use Corollary 3.2. Indeed, S_8 is the graft matroid of the graph from Figure 1 taking $T := \{1, 2, 3, 4\}$ (and labeling the edges $15, 25, 35, 45, 12, 13, 14$ as $e_1, \ldots, e_7$, respectively, and the additional element t as e_8). Therefore, S_8 admits a cycle basis by Theorem 3.1. (Alternatively, one can note that the set $T' := \{e_1, e_2, e_3, e_4\}$ is a maximal independent set in S_8 and that the pairwise intersections of fundamental circuits are the sets $\{e_1\}$ and $\{e_1, e_i\}$ for $i = 2, 3, 4$. This argument shows that S_8 has the lattice of circuits property and that a cycle basis for $\mathbb{Z}(S_8)$ can be constructed by applying the technique from Section 2.)

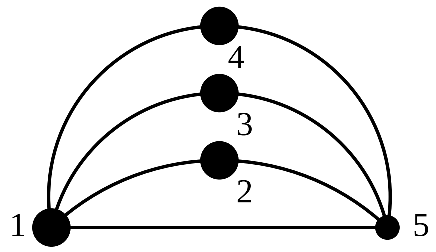

Figure 1: The matroid S_8 is a graft

Acknowledgements. The authors are grateful to Jim Geelen and Lex Schrijver for fruitful discussions.

References

[1] W.H. Cunningham. Chords and disjoint paths in matroids. *Discrete Mathematics*, 19 (1977), pp. 7–15.

[2] M. Deza, V.P. Grishukhin, and M. Laurent. Extreme hypermetrics and L-polytopes. In G. Halász et al., editor, *Sets, Graphs and Numbers, Budapest (Hungary), 1991*, volume 60 of *Colloquia Mathematica Societatis János Bolyai*, pp. 157–209, 1992.

[3] M. Deza, V.P. Grishukhin, and M. Laurent. Hypermetrics in geometry of numbers. In W. Cook, L. Lovász, and P.D. Seymour, editors, *Combinatorial Optimization*, volume 20 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pp. 1–109. American Mathematical Society, 1995.

[4] A. Galluccio and M. Loebl. (p, q)-odd digraphs. *Journal of Graph Theory* 23, 2 (1996), pp. 175–184.

[5] ——, Cycles of binary matroids without an F_7^*-minor. Preprint, 1996.

[6] L. A. Goddyn. Cones, lattices and Hilbert bases of circuits and perfect matchings, In N. Robertson and P.D. Seymour, editors, *Graph Structure Theory*, volume 147 of *Contemporary Mathematics*, pp. 419–440, 1993.

[7] W. Hochstättler and M. Loebl. On Bases of Cocycle Lattices and Submatrices of a Hadamard Matrix *to appear in: J. Nešetril, J. Kratochvil, F. S. Roberts, R. L. Graham, eds., The Future of Discrete Mathematics*, AMS publication, 1998. DIMACS-Series.

[8] L. Lovász. Matching structure and the matching lattice. *Journal of Combinatorial Theory B*, 43 (1987), 187–222.

[9] L. Lovász and M. Plummer. *Matching Theory*, vol. 29 of *Annals of Discrete Mathematics*, North-Holland, 1986.

[10] L. Lovász and A. Seress. The cocycle lattice of binary matroids. *European Journal of Combinatorics,* 14 (1993), pp. 241–250.

[11] ——. The cocycle lattice of binary matroids II. *Linear Algebra and its Applications*, 226/228 (1995), pp. 553–565.

[12] U.S.R. Murty. The matching lattice and related topics. Report, 1994.

[13] M. H. Carvalho, C.L. Lucchesi, and U.S.R. Murty. Optimal ear decompositions of matching covered graphs and a basis of the matching lattice. Under preparation, 1998.

[14] J. Oxley. *Matroid Theory.* Oxford University Press, 1992.

[15] A. Schrijver. *Theory of Linear and Integer Programming.* Wiley, 1986.

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

[17] P.D. Seymour. Matroids and multicommodity flows. *European Journal of Combinatorics*, 2 (1981), pp. 257–290.

[18] D.J.A. Welsh. *Matroid Theory.* Academic Press, London, 1976.