Published in: Linear Alg. Appl., Vol 226–228, pp. 553–567.

The cocycle lattice of binary matroids, II

László Lovász
Eötvös University, Budapest, Hungary, H-1088
Yale University, New Haven, CT

Ákos Seress*
The Ohio State University, Columbus, OH 43210

Abstract: We continue the study initiated in [LS] of the lattice (grid) generated by the incidence vectors of cocycles of a binary matroid and its dual lattice. In [LS], we proved that every denominator in the dual lattice is a power of 2, and characterized those binary matroids M for which the largest exponent $k(M)$ is 1. In this paper, we characterize the matroids with $k(M) = 2$ and, for each constant k, give a polynomial time algorithm to decide whether $k(M) \geq k$.

1. Introduction

Let $G = (V, E)$ be a simple graph and $w : E \to \mathbb{R}$ such that $w(X)$ is an integer for all cuts X. (For a subset $X \subseteq E$, we set $w(X) := \sum_{x \in X} w(x)$.) It is well-known that all such weight functions take only integer and half-integer values, and the edges with non-integer weights define an Eulerian subgraph of G. M. Laurent observed that this statement can not be generalized to all binary matroids and in [LS] we characterized *Eulerian matroids*, i.e., the matroids satisfying that all weight functions taking integer values on cocycles are necessarily half-integral. We also started the study of weight functions which take integer values on cocycles on an arbitrary binary matroid M. The purpose of this paper is to continue this investigation.

First, let us fix some notation. "Matroid" always means a *binary and simple* matroid (i.e., without cycles of length 1 or 2). F^r denotes the r-dimensional projective space over $GF(2)$; in particular, F^2 is the Fano matroid F_7. The *dimension* $\dim(M)$ of a matroid M is the smallest r such that $M \subseteq F^r$ (so $\dim(M)$ is one less that the rank of M). We shall always consider matroids as subsets of projective spaces.

* Research partially supported by NSF Grant CCR-9201303 and NSA Grant MDA904-92-H-3046

Let the *cocycle lattice* $L(M)$ of the matroid M consist of all linear combinations of incidence vectors of cocycles in M with integral coefficients. We define the *dual cocycle lattice* by

$$L^*(M) = \{w \in \mathbb{R}^M \,|\, w(S) \in \mathbb{Z} \text{ for all cocycles } S\}.$$

As it is well-known, every cocycle is the disjoint union of cocircuits, so it would suffice to require integrality on cocircuits. (Recall that cocircuits are just the complements of hyperplanes of M.) It is shown in [LS] that $L^*(M)$ is a discrete set and hence it is a lattice (we use the word lattice in the sense of "grid" and not in the sense of "special poset").

Many structural properties of a lattice and its dual are closely related; for example, $L(M)$ contains all vectors whose entries are multiples of N if and only if every vector in $L^*(M)$ has denominators that are divisors of N. It is also known that $L(M)$ and $L^*(M)$ are equivalent from an algorithmic point of view (cf. e.g. Lovász [L1]). For example, if we can test membership in one in polynomial time then we can test membership in the other.

It is an important general question to characterize lattices generated by combinatorially defined 0-1 vectors. In a sense, this is dual to the basic issue of polyhedral combinatorics, which deals with characterizating convex hulls of combinatorially defined 0-1 vectors. The lattice generated by perfect matchings of a graph was described by Lovász [L2]. Note that the convex hull of cocircuits of a binary matroid is NP-hard to describe even in the graphic case, since optimizing over it would contain the Max-Cut problem.

In [LS], we proved that for each matroid M, there exists a non-negative integer k such that $2^k\mathbb{Z}^M \subseteq L(M)$. Equivalently, $2^k w$ is integral for all $w \in L^*(M)$.

We denote the least integer k with this property by $k(M)$. It is easy to see that $k(M) = 0$ if and only if the matroid is free. The matroid is Eulerian if and only if $k(M) = 1$, and in [LS] we gave various characterizations of this case. We also gave polynomially computable upper and lower bounds for $k(M)$, and conjectured that the upper bound is the true value. Unfortunately, this conjecture is not true and we shall give a counterexample.

In this paper, we characterize matroids with $k(M) = 2$. The characterization uses certain binary linear spaces defined on projective spaces, namely the binary spaces $C_{r,k}$ generated by the (incidence vectors of) flats of dimension k in F^r. These subspaces are known in algebraic coding theory as (punctured) Reed–Muller codes. Also, for each fixed k, we give a polynomial time algorithm to decide whether $k(M) \geq k$.

We introduce the following further notation. Let $M_1 \subseteq M_2$ be two sets and $w : M_1 \to$

$\mathbb{R}$. Abusing notation, we shall also denote by w the extension $w' : M_2 \to \mathbb{R}$ defined by

$$w'(e) = \begin{cases} w(e), & e \in M_1 \\ 0, & e \notin M_1. \end{cases}$$

We shall further abuse notation and denote by M the incidence vector of the set M.

Let $a \oplus b$ denote mod 2 sum, $a + b$ denote real sum, and $a \circ b$ denote coordinate-wise product of the 0-1 vectors a and b. For sets A and B of vectors, let $A \circ B = \{a \circ b : \ a \in A, b \in B\}$. Also set $A^k = A \circ \ldots \circ A$ (k factors). If a is a 0-1 vector then $a \circ a = a$ and hence if A consists of 0-1 vectors then $A \subseteq A^2 \subseteq A^3 \subseteq \ldots$.

For $A \subseteq \mathbb{R}^n$, let $\mathrm{lat}(A)$ denote the lattice generated by the vectors in A. If $A = \{a_1, \ldots, a_r\} \subseteq \{0,1\}^n$, then let $\mathrm{lin}_2(A)$ denote the linear span of A over $GF(2)$ (viewed as a set of 0-1 vectors).

2. Previous results

We summarize some properties of Reed–Muller codes and the results of [LS] which are relevant to the present discussion.

We consider the linear spaces (over $GF(2)$) $C_{r,k}$, $0 \le k \le r$, generated by the set $\mathcal{K}_k$ of (incidence vectors of) flats of F^r of dimension k. For example, $C_{r,1}$ is just the familiar cycle space of the matroid F^r. We shall also consider the linear space $\overline{C}_{r,k}$ which is generated by the complements of the sets in $\mathcal{K}_k$.

The subspaces $C_{r,k}$ are called *punctured Reed–Muller codes* (see MacWilliams and Sloane [MS], Chapter 13 for a treatment of these codes). It is often convenient to append a "parity check bit" to each vector in $C_{r,k}$; more precisely, we consider the *unpunctured Reed-Muller code* $RM_{r,k}$, which is the binary space generated by the incidence vectors of the $(k+1)$-dimensional linear subspaces of $GF(2)^{r+1}$. Then $C_{r,k}$ can be obtained from $RM_{r,k}$ by deleting the coordinate corresponding to the 0 vector, while $\overline{C}_{r,k}$ can be obtained by considering those vectors in $RM_{r,k}$ that have a 0 in position 0, and deleting position 0 from them.

Next we describe a basis of $C_{r,k}$. Let $e_1, e_2, ..., e_{r+1}$ be a basis of F^r; then we define a set $\mathcal{L}_k$ of k-dimensional flats of F^r as follows. $L \subseteq F^r$, $L \cong F^k$ is in $\mathcal{L}_k$ if and only if there are indices $1 \le i_1 < i_2 < ... < i_k \le r$ such that L is generated by $e_{i_1}, e_{i_2}, ..., e_{i_k}$ and an element $e_L \in \langle e_{i_k+1}, e_{i_k+2}, ..., e_{r+1} \rangle$. Notice that L uniquely determines e_L since $|L \cap \langle e_{i_k+1}, e_{i_k+2}, ..., e_{r+1} \rangle| = 1$.

Proposition 2.1.

(a) $|\mathcal{L}_k| = \sum_{j=k+1}^{r+1} \binom{r+1}{j}$.

(b) *$\mathcal{L}_k$ is a basis of $C_{r,k}$.*

We shall call $\mathcal{L}_k$ the *standard basis* of $C_{r,k}$.

Let $C^\perp$ denote the orthogonal complement of the subspace $C \subseteq GF(2)^{F^r}$. Then the following relations are well known:

Proposition 2.2.

(a) $RM_{r,k}^\perp = RM_{r,r-k}$;

(b) $C_{r,k}^\perp = \overline{C}_{r,r-k}$;

(c) for $k < k'$, $C_{r,k} \supset C_{r,k'}$;

(d) the minimal weight (i.e., the minimal number of 1's in codewords) of $C_{r,k}$ *is* $2^{k+1} - 1$.

The following lemma gives a useful necessary condition for $M \in C_{r,k}$. Note that every $M \in C_{r,k}$ may be considered as a subset of F^r and, thus, as a binary matroid.

Lemma 2.3. *Every $M \in C_{r,k}$ has an F^k minor.*

The binary subspace $C_{r,k}$ itself may be considered as the cycle space of a binary matroid F_k^r with underlying set F^r. Thus F_k^r is the matroid whose underlying set is F^r and in which a subset is independent if and only if it does not contain the binary sum of k-flats of F^r. In particular, F_0^r is the matroid with rank 0, $F_1^r = F^r$ and F_r^r is a circuit. In terms of linear codes, a useful matrix representation of this matroid is well known. This, in particular, will yield an efficient way to decide whether a given subset of F^r is independent in this matroid.

Let B be any 0-1 matrix, and let $A = \{a_1, \ldots, a_{r+1}\}$ be the set of row vectors of B. We define the *k-extension* $B^{(k)}$ of B as the matrix whose rows are all vectors in $A^k = A \circ \ldots \circ A$. Thus $B^{(k)}$ has $\sum_{j=1}^{k} \binom{r+1}{j}$ rows. Note that every column of $B^{(k)}$ can be easily computed from the corresponding column of B: the rows are indexed by sets $I = \{i_1, \ldots, i_t\}$ with $1 \le i_1 < \ldots < i_t \le r+1$, $1 \le t \le k$, and the entry in position I is the product of the entries in positions $i_1, \ldots, i_t$.

Proposition 2.4. *If B is a 0-1 matrix of size $(r+1) \times (2^{r+1} - 1)$ representing F^r over $GF(2)$, then $B^{(k)}$ represents F_k^r over $GF(2)$.*

(Note that by Proposition 2.1, $B^{(k)}$ has the "right size".)

An important application of Proposition 2.4 is the following.

Theorem 2.5. *Given an $(r+1) \times n$ 0-1 matrix B and a number $1 \leq k \leq r$, a row basis of $B^{(k)}$ can be computed in time polynomial in n and r. Consequently, we can decide whether the columns of B are independent in F_k^r.*

Assume that we perform the above test and find that the set M of columns of B are dependent in F_k^r. Then we can express some subset of M as the modulo 2 sum of flats of rank at most k (such a subset can be found easily be deleting elements from M as long as the dependence of M in F_k^r is preserved). But how long is such an expression, and how to find it? Our next theorem gives an upper bound, and an algorithm.

Theorem 2.6. *Suppose that $M \subseteq F^r$, $|M| = n$, $0 \leq k \leq r$, and $M \in C_{r,k}$. Then M can be expressed as the sum of at most $\binom{r}{k}n$ elements of the standard basis $\mathcal{L}_k$, and such an expression can be found in $O\left(n\binom{r+k}{k+1}\right)$ time.*

Next, we describe some results concerning cocycle lattices. Let M be a binary matroid of dimension r, coordinatized by an $(r+1) \times n$ matrix B over $GF(2)$. Let $A = \{a_1, \ldots, a_{r+1}\} \subseteq \{0,1\}^n$ be the set of rows of B; then $\mathrm{lin}_2(A)$ is the cocycle space of M and we are interested in the lattice $L(M) = \mathrm{lat}(\mathrm{lin}_2(A))$.

Lemma 2.7. *$L(M)$ contains $2^r\mathbb{Z}^n$. In other words, the denominators in any $w \in L^*(M)$ are divisors of 2^r.*

Let $k(M)$ denote the least integer k for which $2^k\mathbb{Z}^n \subseteq L(M)$. The next two theorems give an upper and lower bound for $k(M)$.

Theorem 2.8. *If $\mathrm{lin}_2(A^{s+1}) = GF(2)^n$ then $2^s\mathbb{Z}^n \subseteq L(M)$. Equivalently, if $M \subseteq F^r$ and $k(M) > k$ then M is dependent in F_{k+1}^r.*

Corollary 2.9. *If M has no F^s minor then $k(M) \leq s-1$. In particular, it follows that $k(M) \leq \log_2(n+1) - 1$.*

Theorem 2.10. *If $2^s\mathbb{Z}^n \subseteq L(M)$ then $\mathrm{lin}_2(A^{2^s}) = GF(2)^n$. Equivalently, if $M \subseteq F^r$ and $k(M) \leq k$ then M is independent in $F_{2^k}^r$.*

These upper and lower bounds suffice to characterize Eulerian matroids.

Theorem 2.11. *Let $M \subseteq F^r$ be the binary matroid defined by the columns of the matrix B. Then the following are equivalent.*

(i) *$L(M)$ contains all even vectors;*

(ii) *every vector in $L^*(M)$ is half-integral;*

(iii) *a vector* $v \in \mathbb{R}^M$ *is in* $L(M)$ *if and only if* v *is integral and the sum of entries of* v *over every circuit is even ("the obvious necessary conditions for* $v \in L(M)$ *are also sufficient");*

(iv) *a vector* $w \in \mathbb{R}^M$ *is in* $L^*(M)$ *if and only if* $w = w' + (1/2)C$*, where* w' *is integral and* C *is a cycle ("the obvious sufficient conditions for* $w \in L^*(M)$ *are necessary");*

(v) *the 2-extension matrix* $B^{(2)}$ *has rank* $|M|$*;*

(vi) M *does not contain the binary sum of any set of planes of* F^r*.*

We finish this section by describing properties of $L(M)$ related to the embedding of M into F^r. The first observation shows that in a sense it suffices to describe the cocycle lattices of projective spaces.

Lemma 2.12. *Let* $\dim(M) = r$*,* $M \subseteq F^r$ *and* $w \in L^*(M)$*. Then* $w \in L^*(F^r)$*.*

(Recall that $w(e) = 0$ for $e \in F^r \setminus M$ by convention.)

Corollary 2.13. *Let* $\dim(M) = r$ *and* $M \subseteq F^r$*. Then the elements of* $L^*(M)$ *are exactly the restrictions of those* $w \in L^*(F^r)$ *that are zero on* $F^r \setminus M$*. The elements of* $L(M)$ *are exactly the restrictions of elements of* $L(F^r)$*.*

The lattice $L^*(F^r)$ can be easily characterized. Note that for each flat $K \subseteq F^r$, we have $2^{-\dim(K)}K \in L^*(F^r)$. It turns out that these vectors generate $L^*(F^r)$.

Theorem 2.14. *Suppose that* $w \in L^*(F^r)$ *and* $2^k w$ *is integer valued. Then* w *is contained in the lattice generated by the vectors* $2^{-d}K$*, where* K *is a flat of* F^r *with* $\dim(K) = d \leq k$*.*

For vectors with bounded denominators, it is possible to test membership in $L^*(F^r)$ in polynomial time.

Theorem 2.15. *Let the non-negative integer* k *be fixed. Then given* $M \subseteq F^r$ *with* $|M| = n$ *and a vector* $w \in 2^{-k}\mathbb{Z}^M$*, it can be decided whether* $w \in L^*(M)$*, in time polynomial in* r *and* n*.*

3. The case $k(M) = 2$

Theorems 2.8 and 2.10 show that the dependency of M in F_2^r determines whether M is Eulerian. For non-Eulerian matroids, we conjectured in [LS] that the dependency of M in F_3^r determines whether $k(M) = 2$. This conjecture turns out to be false. On one hand, if M is independent in F_3^r then, by Theorem 2.8, $k(M) = 2$. On the other hand, however, if M is dependent in F_3^r then both $k(M) = 2$ and $k(M) > 2$ are possible. For example, the matroid $M = F^3$ has $k(M) > 2$. Our first aim in this section is to provide a matroid M which is dependent in F_3^r but $k(M) = 2$.

We start with some general remarks which are pertinent for matroids $M \subseteq F^r$ with larger values of $k(M)$ as well. By Theorem 2.14, every $w \in L^*(F^r)$ can be written in the form

$$w = \sum_i 2^{-\dim(K_i)} K_i, \tag{1}$$

for some flats $K_i \subseteq F^r$. This decomposition is not unique, and the following lemma states that we have some freedom in its construction.

Lemma 3.1. *Suppose that $w \in L^*(F^r)$ and $L_1, ..., L_s$ are flats of F^r such that $2^m(w - \sum_{i=1}^s 2^{-\dim(L_i)} L_i)$ is integer valued. Then there exist flats $\{K_i : i \in I\}$ in F^r, $\dim(K_i) \leq m$ for all $i \in I$ such that $w = \sum_{i=1}^s 2^{-\dim(L_i)} L_i + \sum_{i \in I} 2^{-\dim(K_i)} K_i$.*

Proof. Since $w - \sum_{i=1}^s 2^{-\dim(L_i)} L_i \in L^*(F^r)$, this is an immediate consequence of Theorem 2.14. ∎

Our other remark concerns the embedding of M into projective spaces. Suppose that $\dim(M) = r$. When trying to decompose some $w \in L^*(M)$ in the form described in (1) or trying to construct w as a linear combination of characteristic functions of flats, we can always assume that all flats are in F^r. In other words, this means that considering flats of a projective space larger than the minimal one containing M does not provide more elements of $L^*(M)$. This observation follows both from Corollary 2.13 (applied for $F^r \subset F^{r'}$ and Lemma 3.1 (applied with $s = 0$).

Now we are ready to describe the promised counterexample. Let L_1, L_2, L_3 be 3-dimensional flats of F^r for some $r \geq 5$ such that their pairwise intersections are lines and $L_1 \cap L_2 \cap L_3 = \emptyset$. Define $M := L_1 \oplus L_2 \oplus L_3$.

Lemma 3.2. *The matroid M is dependent in F_3^r and $k(M) = 2$.*

Proof. The first statement follows from the definition of F_3^r. For the second, suppose that $w \in L^*(M)$, $8w$ is integral, but $4w$ is not. Then, by Theorem 2.14, there exist 3-dimensional flats $F_1, ..., F_s$ and flats $K_1, ..., K_t$ of dimension at most 2 such that

$$w = \frac{1}{8}\sum_{i=1}^{s} F_i + \sum_{i=1}^{t} 2^{-\dim(K_i)} K_i. \tag{2}$$

Since $\dim(M) = 5$, we can assume by the preceding remark that all flats are in F^5.

On the set $F := F_1 \oplus \cdots \oplus F_s$, w takes values with denominator 8. This implies that $F \subseteq M$ and, of course, $F \in C_{5,3}$. Also, $M \in C_{5,3}$ and $|M| = 27$. From this, we conclude that $F = M$, since otherwise either F or $M \oplus F$ would be an element of $C_{5,3}$ of size at most 13, contradicting Proposition 2.2(d).

Since $F = M$, we obtain that $4(w - (L_1 + L_2 + L_3)/8)$ is integral. So, by Lemma 3.1, we can suppose that in the decomposition (2), $s = 3$ and $F_i = L_i$ for $i = 1,2,3$. The function $(L_1 + L_2 + L_3)/8$ takes value $1/4$ on 9 points of $F^5 \setminus M$. Adding $1/4$ times 2-dimensional flats of F^5, we have to obtain values with denominator 2 at all points of $F^5 \setminus M$. However, $F^5 \setminus M \in \overline{C}_{5,3}$ and, by Proposition 2.2(b), $\overline{C}_{5,3}^{\perp} = C_{5,2}$. Hence any combination $(K_1 + \cdots + K_\ell)/4$ of 2-dimensional flats K_i will take values with denominator 4 at an even number of points of $F^5 \setminus M$, and cannot cancel denominator 4 at exactly 9 points. This contradiction proves that $k(M) = 2$. ∎

In the rest of this section, we characterize matroids with $k(M) = 2$. Suppose that M is a non-Eulerian matroid with $\dim(M) = r$, coordinatized by an $(r+1) \times n$ matrix B over $GF(2)$. Let $e_1, ..., e_{r+1}$ be a basis of F^r such that $e_i \in M$ for $1 \leq i \leq r+1$. Let X denote the subspace of $GF(2)^{r+1+\binom{r+1}{2}}$ spanned by the columns of the 2-extension matrix $B^{(2)}$. Finally, for $F \in C_{r,3}$ and $F \subseteq M$, let $F = \bigoplus_{L \in \mathcal{J}} L$ ($\mathcal{J} \subseteq \mathcal{L}_3$) be the expression of F in the standard basis $\mathcal{L}_3$. We consider the set Y_F of those $y \in F^r \setminus M$ such that y occurs in $4k+2$ of the L's, $L \in \mathcal{J}$, for some nonnegative integer k. Then let $x_F \in GF(2)^{r+1+\binom{r+1}{2}}$ denote the 2-extension of the vector $\bigoplus_{y \in Y_F} y$.

Theorem 3.3. *Let M be a non-Eulerian matroid. Then $k(M) = 2$ if and only if for all $\emptyset \neq F \in C_{r,3}$ for which $F \subseteq M$, $x_F \notin X$.*

Proof. $\rightarrow$ Suppose, on the contrary, that there exists $F \in C_{r,3}$, $F \subseteq M$, such that $x_F \in X$. Then we can construct $w \in L^*(M)$ with $4w$ non-integral the following way. Let $F = \bigoplus_{L \in \mathcal{J}} L$ be the expression of F in the standard basis and define $w_1 := (1/8)\sum_{L \in \mathcal{J}} L$.

Then w_1 has denominator 4 in $F^r \setminus M$ exactly at the points of Y_F. By Proposition 2.4, the fact that $x_F \in X$ means that there exists $M' \subseteq M$ such that $M' \cup Y_F \in C_{r,2}$. Let $M' \cup Y_F = \bigoplus_{L \in \mathcal{K}} L$ ($\mathcal{K} \subseteq \mathcal{L}_2$) be the expression of $M' \cup Y_F$ in the standard basis $\mathcal{L}_2$ and define $w_2 := w_1 + (1/4)\sum_{L \in \mathcal{K}} L$. Then w_2 has denominator at most 2 in $F^r \setminus M$. In a final step, we add $(1/2)L$ to w_2 for some lines L, in order to cancel the denomimators 2 occuring outside M. Namely, for each $e \in F^r \setminus (M \cup \langle e_1, ..., e_r \rangle)$ for which $w_2(e)$ has denominator 2, we add $(1/2)$ times the line spanned by e and e_{r+1}. Call the resulting function w_3. Next, for each $e \in \langle e_1, ..., e_r \rangle \setminus (M \cup \langle e_1, ..., e_{r-1} \rangle)$ for which $w_3(e)$ has denominator 2, we add $(1/2)$ times the line spanned by e and e_r. Continuing this process, eventually we obtain some $w \in L^*(F^r)$ which takes integer values on $F^r \setminus M$, but still has denominators 8 on M, since the basis vectors $e_1, e_2, ..., e_{r+1}$ are in M. This contradicts the assumption that $k(M) = 2$.

$\leftarrow$ The converse can be proved similarly. Suppose that $k(M) > 2$; then there exists $w \in L^*(M)$ such that $8w$ is integral but $4w$ is not. By Theorem 2.14, the set $F := \{z \in M : w(z) \text{ has denominator } 8\}$ is in $C_{r,3}$. Let $F = \bigoplus_{L \in \mathcal{J}} L$ be the expression of F in the standard basis; then, by Lemma 3.1, $w' := w - (1/8)\sum_{L \in \mathcal{J}} L$ can be decomposed as a linear combination of at most 2-dimensional flats of F^r. In $F^r \setminus M$, w' has denominator 4 exactly at the points in Y_F; therefore, there exists $M' \subseteq M$ such that $M' \cup Y_F \in C_{r,2}$. By Proposition 2.4, this is equivalent to $x_F \in X$. ∎

Theorem 3.4. *The necessary and sufficient condition of Theorem 3.3 can be checked in time polynomial in n.*

Proof. Let $F_1, ..., F_s$ be a basis for the cycle space of M in F_3^r, i.e., a basis for the subspace consisting of the sets $F \subseteq M$, $F \in C_{r,3}$. Such basis can be constructed from the 3-extension matrix $B^{(3)}$. By Theorem 2.6, the decompositions $F_i = \bigoplus_{L \in \mathcal{J}_i} L$, $\mathcal{J}_i \subseteq \mathcal{L}_3$ can be computed in polynomial time. ¿From these decompositions, the vectors x_{F_i} are easily obtained. Then we decide whether there exists $I \subseteq \{1, 2, ..., s\}$, $I \neq \emptyset$ such that $\bigoplus_{i \in I} x_{F_i} \in X$. This happens if and only if either the vectors x_{F_i}, $1 \leq i \leq s$ are not linearly independent or the subspace generated by them intersects X nontrivially. Both of these conditions can be checked in polynomial time. Finally, the following claim finishes the proof.

Claim. Let $I \subseteq \{1, 2, ..., s\}$, $I \neq \emptyset$, and $F := \bigoplus_{i \in I} F_i$. Then $x_F \in X$ if and only if $\bigoplus_{i \in I} x_{F_i} \in X$.

Proof of Claim. Let $F = \bigoplus_{L\in\mathcal{J}} L$ be the expression of F in the standard basis $\mathcal{L}_3$. Then the multiset $\bigcup_{i\in I}\{L : L \in \mathcal{J}_i\}$ contains the set $\{L : L \in \mathcal{J}\}$, and their difference can be written in the form $2\{L : L \in \mathcal{K}\}$, where $\mathcal{K}$ is a multiset from elements of $\mathcal{L}_3$. By Proposition 2.2(c), $C := \bigoplus_{L\in\mathcal{K}} L \in C_{r,2}$. By the definition of the subspaces Y_F, Y_{F_i}, $\bigoplus_{i\in I} Y_{F_i}$ can be obtained by deleting the coordinates belonging to M from $Y_F \oplus C$. Hence

$$x_F \in X \iff \exists M' \subseteq M(M' \cup Y_F \in C_{r,2}) \iff \exists M' \subseteq M\big((M' \cup Y_F) \oplus C \in C_{r,2}\big) \iff$$

$$\exists M'' \subseteq M(M'' \cup \bigoplus_{i\in I} Y_{F_i} \in C_{r,2}) \iff \bigoplus_{i\in I} x_{F_i} \in X. \qquad \blacksquare$$

4. Deciding $k(M) \geq k$

Let k be a fixed positive integer. Given $M \subseteq F^r$ by the columns of a matrix B with $\dim(M) = r$, $|M| = n$, we describe a polynomial time algorithm to decide whether $k(M) \geq k$. In fact, we construct a generating set for the sublattice of $L^*(M)$ consisting of weight functions w with denominators at most 2^k.

The procedure uses a generalization of the ideas described in Theorems 3.3 and 3.4. Unfortunately, it cannot be used to determine the exact value of $k(M)$ if it is not bounded, mostly because of the time and space requirement of the standard basis decomposition described in Theorem 2.6. We note, however, that by Corollary 2.9, $k(M) \leq \log_2(n+1)-1$ and so we obtain a subexponential algorithm for arbitrary values of k. Also, if n is large enough such that we can afford to list all elements of F^r (and, consequently, of its k-extension matrices) then $k(M)$ can be determined in polynomial time.

Recursively for $m = k-1, k-2, ..., 0$, we construct sets $V_{k,m} \subseteq L^*(F^r)$ satisfying the following properties.

(i) for all $w \in V_{k,m}$, $2^k w$ is integer valued;

(ii) for all $w \in V_{k,m}$ and $e \in F^r \setminus M$, $w(e)$ has denominator at most 2^m;

(iii) for all $v \in L^*(M)$ with denominators at most 2^k, there exists a linear combination of $V_{k,m}$ with integer coefficients a_w such that $2^m(v - \sum_{w\in V_{k,m}} a_w w)$ is integer valued.

After this construction, it is easy to decide whether $k(M) \geq k$: all we have to check is whether the denominator 2^k occurs in some $w \in V_{k,0}$.

Let $F_1, ..., F_s$ be a basis of the cycle space of M in F_k^r. By Proposition 2.4 and Theorem 2.5, such basis can be constructed in polynomial time from the k-extension matrix $B^{(k)}$. For $1 \leq i \leq s$, let $F_i = \bigoplus_{L\in\mathcal{J}_i} L$, $\mathcal{J}_i \subseteq \mathcal{L}_k$, be the decomposition of F_i in the standard

basis. We define $V_{k,k-1} := \{(1/2^k)\sum_{L\in\mathcal{J}_i} L : 1 \le i \le s\}$. Clearly, (i) and (ii) are satisfied, and (iii) follows from Corollary 2.13 and Theorem 2.14.

Now suppose that $V_{k,m} = \{w_1, ..., w_s\}$ is already constructed for some $m > 0$. Let $q = \sum_{j=1}^{m} \binom{r+1}{j}$ and let X denote the subspace of $GF(2)^q$ spanned by the columns of the m-extension matrix $B^{(m)}$. For $w \in V_{k,m}$, let Y_w consist of those $y \in F^r \setminus M$ such that $w(y)$ has denominator 2^m. Moreover, let x_w denote the m-extension of $\bigoplus_{y\in Y_w} y$.

Let $e_1, ..., e_s$ be a basis of $GF(2)^s$. We define a linear transformation $\varphi : GF(2)^s \to GF(2)^q$ by setting $\varphi(e_i) := x_{w_i}$ for $1 \le i \le s$. Let $f_1, ..., f_\ell$ be a basis for the preimage $\varphi^{-1}(X)$, and let $f_j = \bigoplus_{i=1}^{s} \varepsilon_{j,i} e_i$ the decomposition of f_j in the basis of $GF(2)^s$, $\varepsilon_{j,i} \in GF(2)$ for $1 \le j \le \ell, 1 \le i \le s$.

For $1 \le j \le \ell$, we define $v_j := \sum_{i=1}^{s} \varepsilon_{j,i} w_i$. As usual, we denote by Y_{v_j} the set of those $y \in F^r \setminus M$ such that $v_j(y)$ has denominator 2^m and we define x_{v_j} as the m-extension of $\bigoplus_{y\in Y_{v_j}} y$. Then $x_{v_j} \in X$ and so we can find $M_j \subseteq M$ such that $M_j \cup Y_{v_j} \in C_{r,m}$. We construct the decompositions $M_j \cup Y_{v_j} = \bigoplus_{L\in\mathcal{J}_j} L$, $\mathcal{J}_j \subseteq \mathcal{L}_m$ in the standard basis and define $z_j := v_j + (1/2^m)\sum_{L\in\mathcal{J}_j} L$, for $1 \le j \le \ell$.

Next, we compute a basis $G_1, ..., G_t$ for M in F_m^r, and for each G_i, we construct the decomposition $G_i = \bigoplus_{L\in\mathcal{K}_i} L$, $\mathcal{K}_i \subseteq \mathcal{L}_m$ in the standard basis.

The set $V_{k,m-1}$ is defined as $\{z_j : 1 \le j \le \ell\} \cup \{2w : w \in V_{k,m}\} \cup \{(1/2^m)\sum_{L\in\mathcal{K}_i} L : 1 \le i \le t\}$. Clearly, (i) and (ii) are satisfied (note that the functions z_j are obtained from v_j by adding a function which cancels the denominators equal to 2^m in v_j). We have to check that (iii) also holds.

Let $w \in L^*(M)$ such that $2^k w$ takes only integer values. Since $V_{k,m}$ satisfies (iii), there are integers a_i, $1 \le i \le s$, such that $w - \sum_{i=1}^{s} a_i w_i$ has denominators at most 2^m.

Claim. The function $\sum_{i=1}^{s} a_i w_i$ can be expressed as a linear combination of $\{v_j : 1 \le j \le \ell\} \cup \{2w : w \in V_{k,m}\}$ with integer coefficients.

Proof of Claim. Let $I \subseteq \{1, ..., s\}$ defined as the set of indices for which a_i is odd. In $F^r \setminus M$, the function $w - \sum_{i=1}^{s} a_i w_i$ has denominator 2^m exactly at the points of $\bigoplus_{i\in I} Y_{w_i}$. By Lemma 3.1, $w - \sum_{i=1}^{s} a_i w_i$ can be expressed as a linear combination of flats of dimension at most m; this linear combination cancels the denominators 2^m at the points of $\bigoplus_{i\in I} Y_{w_i}$, so there exists $M' \subseteq M$ such that $M' \cup \bigoplus_{i\in I} Y_{w_i} \in C_{r,m}$. This means that $\bigoplus_{i\in I} x_{w_i} \in X$.

The last statement implies that $\bigoplus_{i\in I} e_i \in \langle f_1, ..., f_\ell \rangle$, say $\bigoplus_{i\in I} e_i = \bigoplus_{j=1}^{\ell} \alpha_j f_j$ for some $\alpha_j \in GF(2)$. Recall that $f_j = \bigoplus_{i=1}^{s} \varepsilon_{j,i} e_i$ and $v_j = \sum_{i=1}^{s} \varepsilon_{j,i} w_i$. This means that in the expression $\sum_{j=1}^{\ell} \alpha_j v_j$, exactly those w_i occur an odd number of times for which $i \in I$.

So $\sum_{i\in I} w_i - \sum_{j=1}^{\ell} \alpha_j v_j$ is an integer linear combination of $\{2w : w \in V_{k,m}\}$. ∎

Let $\sum_{i=1}^{s} a_i w_i = \sum_{j=1}^{\ell} \alpha_j v_j + \sum_{i=1}^{s} b_i(2w_i)$ for some integers b_j. Since v_j and z_j differ by a function which has denominators at most 2^m, the difference $w' := w - \big(\sum_{j=1}^{\ell} \alpha_j z_j + \sum_{i=1}^{s} b_i(2w_i)\big)$ has denominators at most 2^m as well. Also, at the points of $F^r \setminus M$, the function $\sum_{j=1}^{\ell} \alpha_j z_j + \sum_{i=1}^{s} b_i(2w_i)$ has denominators at most 2^{m-1}. Thus we obtain that for the set F consisting of those $y \in F^r$ such that $w'(y)$ has denominator 2^m, $F \in C_{r,m}$ and $F \subseteq M$. This means that subtracting an appropriate subset of $\{(1/2^m)\sum_{L\in\mathcal{K}_i} L : 1 \le i \le t\}$ from w', we obtain a function with denominators at most 2^{m-1}. Hence (iii) holds for $V_{k,m-1}$.

To justify the polynomial timing, observe that $|V_{k,k-1}| \le n$ and $|V_{k,m-1}| \le 2|V_{k,m}|+n$. This implies that $|V_{k,m}| < 2^k n$ for all m. Also, we need a polynomial upper bound for the number of non-zero values in the constructed functions. Let K be an upper bound for the number of non-zero values in functions in $V_{k,m}$. Then, by Theorem 2.6, the number of non-zero values in functions in $V_{k,m-1}$ is at most $K|V_{k,m}|\binom{r}{m}(2^{m+1}-1)$. Solving this recursion, we obtain that the number of non-zero values in any of the functions constructed is at most $2^{2(k+1)k} n^{k+1} \binom{r}{k}^k$.

By Theorems 2.5, 2.6 and by elementary linear algebra, all procedures applied at the construction of $V_{k,m}$ run in time polynomial in their input length. In the preceding paragraph, we have justified that these input lengths are polynomial in n; hence the entire procedure runs in time polynomial in n.

References:

[L1] L. Lovász: Some algorithmic problems on lattices, in: *Theory of Algorithms*, (eds. L. Lovász and E. Szemerédi), Coll. Math. Soc. J. Bolyai 44(1985), North-Holland, 323–337.

[L2] L. Lovász: Matching structure and the matching lattice, *J. Comb. Theory B* **43**(1987), 187–222.

[LS] L. Lovász and Á. Seress: The cocycle lattice of binary matroids, *Europ. J. Comb.* **14**(1993), 241–250.

[MS] F.J. MacWilliams and N.J. Sloane: *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.