Abstract.

We study the lattice (grid) generated by the incidence vectors of cocycles of a binary matroid and its dual lattice. We characterize those binary matroids for which the obvious necessary conditions for a vector to belong to the cocycle lattice are also sufficient. This characterization yields a polynomial time algorithm to check whether a matroid has this property, and also to construct a basis in the cocycle lattice. For the general case, we prove that every denominator in the dual lattice is a power of 2, and derive upper and lower bounds for the largest exponent.

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 $X \subset E$, 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: for example, the constant $1/4$ function on the Fano matroid F_7 takes integer values on all cocycles of F_7. Cunningham (1977) proved, however, that if a binary matroid M has no parallel elements and M has no F_7 minor then every element arises as the intersection of two cocycles and, as Laurent observed, this implies that all weight functions taking integer values on cocycles are necessarily half-integral.

The purpose of this paper is to study those weight functions on a binary matroid M which take integer values on cocycles. We call a binary matroid *eulerian*, if every such weight function is half-integral. We give polynomial time algorithm to decide whether or not a given binary matroid is eulerian.

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.

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 will follow from our results 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, we shall often use the (trivial) fact that $L(M)$ 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 (1985)). For example, if we can test membership in one in polynomial time then we can test membership in the other. Hence in formulating our results we may consider whichever is more convenient.

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

(1987). 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.

Our main results on the lattice $L(M)$ are the following.

(1.1) *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 $w \in L^*(M)$.*

The least integer k with this property will be denoted by $k(M)$. It is easy to see that $k(M) = 0$ if and only the matroid is free. The matroid is eulerian iff $k(M) = 1$, and we shall give various characterizations of this case. The following will turn out the most useful for algorithmic purposes.

(1.2) *Let M be a binary matroid of dimension r and $\{C_1, \ldots, C_{r+1}\}$, a basis of its cocycle space. M is eulerian if and only if the sets $C_i \cap C_j$ $(1 \le i \le j \le r+1)$ generate every subset of M over $GF(2)$.*

Another characterization of eulerian matroids describes the exact connection with Fano planes:

(1.3) *A binary matroid $M \subseteq F^r$ is eulerian if and only if M does not contain the binary sum of any set of planes of F^r.*

We shall give a (polynomially computable) upper bound on $k(M)$ for every binary matroid, and conjecture that this is in fact the true value. Unfortunately, we can only prove a much weaker lower bound.

As (1.2) suggests, to obtain these results we have to study 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, and we begin in section 2 with a survey of some of their properties.

We need the following further notation. For $e \in M$, M/e denotes the matroid obtained by contracting e. A contraction may create parallel elements; we always identify these elements, ensuring that M/e is simple. Hence contraction is the same as projection on a hyperplane in F^r from the contracted element. Any $w : M \to \mathbb{R}$ naturally defines a function $w_e : M/e \to \mathbb{R}$ by the rule $w_e(x') = \sum\{w(x) | x'$ is the image of x at the contraction$\}$. It is clear that if $w \in L^*(M)$ then $w_e \in L^*(M/e)$. Let $M_1 \subset M_2$ 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).

Acknowledgement. We are indebted to András Sebő for fruitful discussions on the subject and for the careful reading of the manuscript. We also thank to the referees for many valuable suggestions, in particular for pointing out the connection with Reed-Muller codes.

2. Reed-Muller codes

In this section, which serves as a preparation, we study 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 (1977), 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. $L \subset F^r$, $L \cong F^k$ is in $\mathcal{L}$ if and only if there are indices $1 \le i_1 < i_2 < \ldots < i_k \le r$ 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* $C_{r,k}$.

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) $MR_{r,k}^\perp = MR_{r,r-k}$;

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

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

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.*

Proof. Let $e \in M$ and define M_e as the matroid obtained by projecting M ¿from e on a hyperplane H, and deleting those elements which arise as images of two elements of M. We claim that $M_e \in C_{r-1,k}$. In fact, consider any $(r-1-k)$-dimensional flat L in H, and let L' denote the flat spanned by L and e. Then

$$|M_e \cap (H \setminus L)| \equiv |M \cap (F^r \setminus L')| \equiv 0 \qquad (\text{mod } 2),$$

which implies by Proposition 2.2(b) that $M_e \in C_{r-1,k}$.

Since $M_e \subseteq M/e$, we are done unless $M_e = \emptyset$. But if $M_e = \emptyset$ for every $e \in M$ then M is a flat, i.e., $M \equiv F^s$ for some s. To conclude, it suffices to remark that $s \geq k$, since otherwise any $(r-k)$-dimensional flat disjoint from M would contradict Proposition 2.2(b). ∎

The binary subspace $C_{r,k}$ itself may be considered as the cycle space of a binary matroid F^r_k with underlying set F^r. Thus F^r_k 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^r_0 is the matroid with rank 0, $F^r_1 = F^r$ 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 $\sum_{j=1}^{k} \binom{r+1}{k}$ 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 $1 \leq i_1 < \ldots < i_t \leq r+1$, $1 \leq t \leq k$, 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^r_k 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 $1 \leq k \leq r$, we can decide whether the columns of B are independent in F^r_k, in time polynomial in n and r.*

Proof. By Proposition 2.4, we have to decide whether or not the columns of the k-extension matrix $B^{(k)}$ of B are linearly independent over $GF(2)$. Note that n may be much smaller than 2^r, and so we cannot in general write up the whole matrix $B^{(k)}$. The trick will be that we can select and compute a row basis of $B^{(k)}$ in polynomial time.

Select a row basis A_1 of B and define sets $A_2, \ldots, A_k$ recursively as follows. For $i = 1, \ldots, k-1$, consider all vectors in $A_1 \circ A_i$, and select a maximal subset of them linearly independent from $A_1 \cup \ldots \cup A_i$; let this subset be A_{i+1}.

Claim. $A_1 \cup \ldots \cup A_k$ is a basis of $B^{(k)}$. In fact, let $b_1 \circ \ldots \circ b_s$ be a row of $B^{(k)}$, where $b_1, \ldots, b_s$ are rows of B and $s \le k$. We prove by induction on s that

$$b_1 \circ \ldots \circ b_s \in \mathrm{lin}_2(A_1 \cup \ldots \cup A_s).$$

For $s = 1$ this follows by the definition of A_1. Assume that $s > 1$. Then we can write

$$b_s = a_1 \oplus \ldots \oplus a_p, \qquad a_1, \ldots a_p \in A_1,$$

by the definition of A_1 and

$$b_1 \circ \ldots \circ b_{s-1} = c_1 \oplus \ldots \oplus c_q, \qquad c_1, \ldots, c_q \in A_1 \cup \ldots A_{s-1},$$

by the induction hypothesis. So

$$b_1 \circ \ldots \circ b_s = (c_1 \circ a_1) \oplus (c_1 \circ a_2) \oplus \ldots \oplus (c_q \circ a_p),$$

and hence it suffices to show that if $c \in A_i$ and $a \in A_1$ then $c \circ a \in \mathrm{lin}_2(A_1 \cup \ldots \cup A_{i+1})$. But this is immediate by the definition of A_{i+1}.

It follows from the Claim that to decide whether or not the columns of $B^{(k)}$ are linearly independent, it suffices to decide this for the columns of the matrix B' with rows $A_1 \cup \ldots \cup A_k$. The rows of B' are linearly independent, and hence B' has at most n rows. Thus this test can be performed in $O(n^3)$ time.

To conclude, it suffices to remark that to select A_1 takes $O(n^2 r)$ time and to find each A_i takes $O(n^3 \cdot |A_i|)$ steps, which gives a total of $O(n^3(n+r))$ steps to compute B'. ∎

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

Proof. We use induction on r. The cases $k = 0$ and $k = r$ are obvious. Let $M = \bigoplus_{L \in \mathcal{J}} L$ ($\mathcal{J} \subseteq \mathcal{L}_k$) be the expression of M in the basis $\mathcal{L}_k$; we prove that $|\mathcal{J}| \le \binom{r}{k} n$.

Let H be the hyperplane spanned by $\{e_2, \ldots, e_{r+1}\}$. Set $\mathcal{J}_1 = \{L \in \mathcal{J} \mid e_1 \in L\}$ and $\mathcal{J}_2 = \mathcal{J} \setminus \mathcal{J}_1$, and consider the sets $M_i = \bigoplus_{L \in \mathcal{J}_i} L$. Clearly, for every line $\{e_1, e, f\}$ through e_1, either both or neither of e and f belong to M_1, and at most one of them (the one on H) belongs to M_2. Using that $M_1 \oplus M_2 = M$, we see that $|M_1 \cap H| \le n$ and $|M_2| \le n$. Since $\mathcal{J}_2$ is contained in $\mathcal{L}_k$ of H, this implies by the induction hypothesis that $|\mathcal{J}_2| \le \binom{r-1}{k} n$.

On the other hand, $M_1 \cap H = \bigoplus_{L \in \mathcal{J}_1} L \cap H$ is a representation of $M_1 \cap H$ in $\mathcal{L}_{k-1}$ in H, and hence by the induction hypothesis we have $|\mathcal{J}_1| \le \binom{r-1}{k-1} n$. Adding up these inequalities, the assertion follows.

To show the algorithmic computability of this decomposition, it suffices to note that M_1 (and hence M_2) can be determined without knowing the representation of M in the basis $\mathcal{L}_k$, in time $O(rn)$: we have e.g. $M_2 = M_e$. We can then recursively find the decompositions of M_1 and M_2 in the time stated. ∎

3. Lattices and binary subspaces

We consider a binary matroid M 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 $L(M) = \mathrm{lat}(\mathrm{lin}_2(A))$. It is clear that the difficulty lies in the fact that we have to mix operations over the integers with operations modulo 2; the following simple "inclusion-exclusion type" formulas help to express these with each other.

Lemma 3.1. *For any set of 0-1 vectors $a_1, \ldots, a_p$, we have*

$$a_1 \oplus \ldots \oplus a_p = \sum_{t=1}^{p} (-1)^{t-1} 2^{t-1} \sum_{1 \le i_1 < \ldots < i_t \le p} (a_{i_1} \circ \ldots \circ a_{i_t})$$

and

$$2^{p-1} a_1 \circ \ldots \circ a_p = \sum_{t=1}^{p} (-1)^{t-1} \sum_{1 \le i_1 < \ldots < i_t \le p} (a_{i_1} \oplus \ldots \oplus a_{i_t}).$$

Proof. Routine by considering the number of times a given entry is counted on both sides. ∎

Lemma 3.1 implies

Corollary 3.2.

$$L(M) = \mathrm{lat}(\mathrm{lin}_2(A)) = \mathrm{lat}(A \cup 2A^2 \cup \ldots \cup 2^r A^{r+1}).$$

(It would be enough to include those vectors in A^j which are products of j distinct vectors in A, since the others appear already in A^{j-1}.)

Using "ordinary" inclusion-exclusion and the assumption that M is a simple matroid (i.e., any two columns of B are different), we see that $\mathrm{lat}(A^{r+1}) = \mathbb{Z}^n$. Hence

Corollary 3.3. *$L(M)$ contains $2^r \mathbb{Z}^n$.*

(In other words, the denominators in any $w \in L^*(M)$ are divisors of 2^r.)

Unfortunately, the set of generators for $L(M)$ provided by Corollary 3.2 may be exponentially large in n, while we know that every lattice in $\mathbb{R}^n$ can be generated by n

elements. We try to find a formula analogous to the one in Corollary 3.2 but having a smaller number of terms. Let $k(M)$ denote the least integer k for which $2^k\mathbb{Z}^n \subseteq L(M)$. Corollary 3.2 implies that

$$L(M) = \mathrm{lat}(A \cup 2A^2 \cup \ldots \cup 2^{k(M)-1}A^{k(M)}) + 2^{k(M)}\mathbb{Z}^n.$$

Looking at our arguments more carefully we see that $k(M)$ is less than the maximum number of distinct vectors a_i whose coordinate-wise product is not 0. Thus

Corollary 3.4. *If the cocycle space of M has a system of generators such that the intersection of any $s+1$ of them is 0, then $2^{s-1}\mathbb{Z}^n \subseteq L(M)$ and*

$$L(M) = \mathrm{lat}(A \cup 2A^2 \cup \ldots \cup 2^{s-3}A^{s-2}) + 2^{s-1}\mathbb{Z}^n.$$

For example, if $a_1, \ldots, a_{r+1}$ are the stars of vertices of a graph G, then this number is 2, and hence $L(M)$ contains $2\mathbb{Z}^n$, and $L(M) = \mathrm{lat}(A) + 2\mathbb{Z}^n$.

To obtain a better bound, we need one more lemma relating the linear span over $GF(2)$ and the lattice generated by a set of integral vectors.

Lemma 3.5. *Let $b_1, \ldots, b_r \in \mathbb{Z}^n$. Assume that $\mathrm{lin}_2\big((b_1 \bmod 2), \ldots, (b_r \bmod 2)\big) = GF(2)^n$ and $\mathrm{lat}(b_1, \ldots, b_r)$ contains $2^N\mathbb{Z}^n$ for some $N \geq 0$. Then $\mathrm{lat}(b_1, \ldots, b_r) = \mathbb{Z}^n$.*

Proof. Trivially $r \geq n$ and we may assume that $(b_1 \bmod 2), \ldots, (b_n \bmod 2)$ are linearly independent over $GF(2)$. Then $M = \det(b_1, \ldots, b_n)$ is odd.

Now let $w \in \mathbb{Z}^n$. From Cramer's rule it follows that $Mw \in \mathrm{lat}(b_1, \ldots, b_n) \subseteq \mathrm{lat}(b_1, \ldots, b_r)$. By hypothesis, $2^N w \in \mathrm{lat}(b_1, \ldots, b_r)$ and since $g.c.d.(M, 2^N) = 1$, this implies that $w \in \mathrm{lat}(b_1, \ldots, b_r)$. ∎

From this lemma we obtain a useful algebraic upper bound on $k(M)$.

Theorem 3.6. *If $\mathrm{lin}_2(A^{s+1}) = GF(2)^n$ then $2^s\mathbb{Z}^n \subseteq L(M)$.*

Proof. By Corollary 3.2, we have

$$\mathrm{lat}(A^{s+1} \cup 2A^{s+2} \cup \ldots \cup 2^{r-s}A^{r+1}) \supseteq L(M) \supseteq 2^r\mathbb{Z}^n,$$

and so Lemma 3.5 implies that

$$\mathrm{lat}(A^{s+1} \cup 2A^{s+2} \cup \ldots \cup 2^{r-s}A^{r+1}) = \mathbb{Z}^n.$$

So by Corollary 3.2,

$$L(M) \supseteq 2^s\mathrm{lat}(A^{s+1} \cup 2A^{s+2} \cup \ldots \cup 2^{r-s}A^{r+1}) = 2^s\mathbb{Z}^n.$$

∎

Combining this theorem with Proposition 2.4, we obtain

Theorem 3.7. *If $M \subset F^r$ and $k(M) \geq k$, then M is dependent in F_k^r.* ∎

Combining also with Lemma 2.3, we can state:

Corollary 3.8. *If M has no F^s minor then $k(M) \leq s-1$. In particular, it follows that $k(M) \leq \log_2(n+1) - 1$.*

We conjecture that the converse of Theorems 3.6 and 3.7 also holds. Unfortunately, we can only prove a very weak converse of Theorem 3.6 (or 3.7).

Theorem 3.9. *If $2^s\mathbb{Z}^n \subseteq L(M)$ then* $\mathrm{lin}_2(A^{2^s}) = GF(2)^n$.

Proof. By Corollary 3.2,

$$\mathrm{lat}(\mathrm{lin}_2(A^2)) = \mathrm{lat}(A^2 \cup 2A^4 \cup \ldots \cup 2^{j-1}A^{2j} \cup \ldots) \supseteq \mathrm{lat}(A^2 \cup 2A^3 \cup 4A^4 \cup \ldots).$$

We claim that $\mathrm{lat}(A^2 \cup 2A^3 \cup 4A^4 \cup \ldots)$ contains $2^{s-1}\mathbb{Z}^n$. In fact, let $w \in \mathbb{Z}^n$. Since $2^s\mathbb{Z}^n \subseteq L(M)$, we can write

$$2^s w = \sum_i \lambda_i a_i + 2\sum_{i,j} \lambda_{ij}(a_i \circ a_j) + 4\sum_{i,j,l} \lambda_{ijl}(a_i \circ a_j \circ a_l) + \ldots,$$

where all the λ's are integers. Considering both sides modulo 2, we se that $\lambda_1, \ldots, \lambda_r$ are even. Hence

$$2^{s-1}w = \sum_i \frac{\lambda_i}{2} a_i + \sum_{i,j} \lambda_{ij}(a_i \circ a_j) + 2\sum_{i,j,l} \lambda_{ijl}(a_i \circ a_j \circ a_l) + \ldots \in A^2 + 2A^3 + 4A^4 + \ldots$$

Thus $\mathrm{lat}(\mathrm{lin}_2(A^2))$ contains $2^{s-1}\mathbb{Z}^n$. By induction on s, we know that $\mathrm{lin}_2((A^2)^{2^{s-1}}) = GF(2)^n$, which implies the assertion. ∎

While the upper and lower bounds on $k(M)$ provided by these theorems are far apart, they do coincide in the case $k(M) = 1$.

Corollary 3.10. *$L(M)$ contains all even vectors (equivalently, all vectors in L^* are half-integral) if and only if* $\mathrm{lin}_2(A^2) = GF(2)^n$.

4. The cocycle lattice of a projective space

In the previous section we derived algebraic bounds on $k(M)$; in this section we prove 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 4.1. *Let* $\dim(M) = r$, $M \subset F^r$ *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.)

Proof. Let H be an arbitrary hyperplane of F^r. We shall prove that $w(F^r \setminus H)$ is an integer by induction on $\dim(H \cap M)$. If $\dim(H \cap M) = r-1$ then H is also a hyperplane of M and we are done. Suppose that $w(F^r \setminus H')$ is integer for all hyperplanes H' of F^r with $\dim(H' \cap M) > \dim(H \cap M) = k$. Let H_0 be an $r-2$-dimensional flat of H containing $H \cap M$ and $F^r \setminus H = A \dot\cup B$ a partition of $F^r \setminus H$ such that $H_0 \dot\cup A$ and $H_0 \dot\cup B$ are hyperplanes of F^r. We have to prove that $w(A) + w(B) \in \mathbb{Z}$. $M \cap A \neq \emptyset$ and $M \cap B \neq \emptyset$ otherwise M would be contained in a hyperplane of F^r. Hence, from the induction hypothesis, $w(A) + w(H \setminus H_0) \in \mathbb{Z}$ and $w(B) + w(H \setminus H_0) \in \mathbb{Z}$. $w(H \setminus H_0) = 0$ since $M \cap (H \setminus H_0) = \emptyset$; so $w(A) + w(B) \in \mathbb{Z}$. ∎

Corollary 4.2. *Let* $\dim(M) = r$ *and* $M \subset F^r$. *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* $L(F^r)$. ∎

Next, we give a characterization of $L^*(F^r)$. Note that for each flat $K \subset F^r$, we have $2^{-\dim(K)} K \in L^*(F^r)$. We proceed to show, among others, that these vectors generate $L^*(M)$.

Lemma 4.3. *Let* H *be a hyperplane of* F^r *and* $w \in L^*(F^r)$. *Then* $2w|_H \in L^*(H)$.

Proof. Let H_0 be an $r-2$-dimensional flat of H; we have to prove that $2w(H \setminus H_0) \in \mathbb{Z}$. Let $F^r \setminus H = A \dot\cup B$ be a partition of $F^r \setminus H$ such that $H_0 \dot\cup A$ and $H_0 \dot\cup B$ are hyperplanes of F^r. Then $w(A) + w(H \setminus H_0) \in \mathbb{Z}$, $w(B) + w(H \setminus H_0) \in \mathbb{Z}$, and $w(A) + w(B) \in \mathbb{Z}$. Adding the first two of these equations and subtracting the third, we obtain $2w(H \setminus H_0) \in \mathbb{Z}$. ∎

Theorem 4.4. *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* $\dim(K) = d \leq k$.

Proof. . We use induction on r. For $r \leq 2$, the assertion is obviously true.

Let $w \in L^*(F^r)$ such that $2^k w$ is integer valued and let H_1 a hyperplane of F^r. By Lemma 4.3, $2w|_{H_1} \in L^*(H_1)$. Therefore, by the induction hypothesis, there are flats K_i of H_1 with $\dim(K_i) = d_i \leq k-1$ and integers c_i such that

$$2w|_{H_1} = \sum_i c_i 2^{-d_i} K_i.$$

Now choose any $e \in F^r \setminus H_1$. For each i, let K_i' be the $(\dim(K_i)+1)$-dimensional flat of F^r spanned by e and K_i. Consider

$$w_1 = w - \sum_i c_i 2^{-d_i-1} K_i'.$$

For this vector, $2^k w_1$ is integral and it is enough to prove that w_1 belongs to the lattice as claimed in the theorem. The gain is that w_1 has value 0 at all elements of H_1. Observe that if $f \in H_1$ and $\{e, f, f'\}$ is a line then $w_1(f') = w(f') - w(f)$.

Next, we apply the same argument to another hyperplane H_2 of F^r, with $e' \in H_1 \setminus H_2$. We obtain that it suffices to prove the assertion for a vector w_2; this vector has values 0 on all elements of H_2 and it follows from the observation above that it still has values 0 on H_1. So all the support of w_2 is contained in $F^r \setminus H_1 \setminus H_2$. Note that this set is contained in the hyperplane $H_3 = F^r \setminus (H_1 \oplus H_2)$.

To finish the proof, we claim that $w_2|_{H_3} \in L^*(H_3)$, and so the induction hypothesis can be applied. Let H be an arbitrary hyperplane of H_3 and let H' be the hyperplane of F^r generated by e_2 and H. Then $w_2|_{H_3}(H_3 \setminus H) = w_2(F^r \setminus H') \in \mathbb{Z}$. ∎

Theorem 4.5. *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.*

Proof. We describe the algorithm by recurrence on k. Let $M_0 = \{e \in M \,|\, 2^{k-1}w(e) \notin \mathbb{Z}\}$. By Theorem 4.4, if $w \in L^*(M)$ then M_0 is in the punctured Reed-Muller code $C_{r,k}$. So, our first task is to decide whether $M_0 \in C_{r,k}$, which we carry out by Theorem 2.5. If $M_0 \notin C_{r,k}$ then $w \notin L^*(M)$. Otherwise, using Theorem 2.6, we find a decomposition

$$M_0 = \bigoplus_{j=1}^{\binom{r}{k}n} L_j,$$

where each L_j is a flat in F^r with dimension $dim(L_j) = d_j \leq k$. Let $w_j = 2^{-d_j} L_j$. By Corollary 4.2 and Theorem 4.4, $w \in L^*(M)$ if and only if $w' = w - \sum_j w_j \in L^*(F^r)$.

The vector w' can be computed in polynomial time because $|\{e \in F^r \,|\, w'(e) \neq 0\}| \leq n + n\binom{r}{k}(2^{k+1}-1)$. Moreover, $2^{k-1}w'$ is integer valued. Hence, in polynomial time, we have reduced the decision problem $w \in L^*(M)$ to a decision problem on a matroid of size polynomial in n and to a weight function which becomes integer valued when we multiply it with 2^{k-1}. ∎

5. Eulerian matroids

The following theorem collects those properties characterizing eulerian matroids.

Theorem 5.1. *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.*

Proof. (i)$\Leftrightarrow$(ii), (iii)$\Leftrightarrow$(iv) and (iii)$\Rightarrow$(i) are obvious. Theorem (3.7) yields (i)$\Rightarrow$(v) and Theorem (3.6) yields (v)$\Rightarrow$(i). (v)$\Leftrightarrow$(vi) follows by Proposition 2.4. Thus it suffices to show that (i)$\Rightarrow$(iii).

Let $v \in \mathbb{Z}^n$ and assume that the sum of entries of v over every circuit is even; we want to show that $v \in L(M)$. By (i), we may assume that v is a 0-1 vector. But the assumption implies that v is orthogonal to every circuit (over $GF(2)$), thus v is a cocycle, and hence $v \in L(M)$. ∎

Property (v) of the theorem yields a polynomial time procedure to decide whether a given binary matroid is eulerian.

We can also construct a system of generators in $L(M)$. Consider any basis $a_1, \ldots, a_{r+1}$ of the cocycle space, together with the vectors $2\{v\}$ $(v \in M)$; then (i) implies that these vectors are in $L(M)$ and (iv) implies that they generate $L(M)$.

If we want to construct a basis of $L(M)$, we can choose a basis N in M, and consider the fundamental cocycle basis $\{a_1, \ldots, a_{r+1}\}$ with respect to N; every cocycle in this basis meets N at exactly one point. Add to this the vectors $2\{v\}$ for $v \in M \setminus N$. It is easy to see that these vectors are linearly independent, and the vectors $2\{v\}$ $(v \in N)$ are integral linear combinations of them, so they form a basis of $L(M)$. Once this basis is constructed, it is straightforward to construct a basis in $L^*(M)$, to test membership in $L(M)$ and $L^*(M)$, etc.

As another consequence of this construction, we obtain

Corollary 5.2. *If M is eulerian then* $\det(L(M)) = 2^{n-r+1}$.

It is not difficult to show that this property also characterizes eulerian matroids: if M is non-eulerian, then $\det(L(M)) > 2^{n-r+1}$.

References:

W. Cunningham (1977): Chords and disjoint paths in matroids, *Discrete Mathematics* **19**, 7-15.

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

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

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