1980

Incidence Codes of Posets: Eulerian Posets and Reed-Muller Codes

Kenneth P. Bogart
Dartmouth College

Discrete Mathematics 31 (1980) 1–7

INCIDENCE CODES OF POSETS: EULERIAN POSETS AND REED–MULLER CODES

Kenneth P. BOGART

Department of Mathematics, Dartmouth College, Hanover, NH 03755, USA

Received 14 February 1979
Revised June 1979

This paper shows how to construct analogs of Reed–Muller codes from partially ordered sets. In the case that the partially ordered set is Eulerian the length of the code is the number of elements in the poset, the dimension is the size of a selected order ideal and the minimum distance is the minimum size of a principal dual ideal generated by a member of the order ideal. In this case, the majority logic method of decoding Reed–Muller codes works for incidence codes. A number of interesting combinatorial questions arise from the study of these codes.

1. Introduction

An (n, k, d) linear code C over a field F is a k-dimensional subspace of F^n such that each nonzero vector in C has at least d nonzero entries. In this paper, we present a method for constructing codes from partially ordered sets. When this method is applied to the subsets of a set, ordered by set inclusion, it yields the well known Reed–Muller codes. When applied to a larger class of posets (Eulerian posets with the least upper bound property), it yields majority logic decodable codes quite analogous to Reed–Muller codes. Although this construction is extremely elementary and has not as yet yielded new information about Reed–Muller codes, it leads to a number of interesting combinatorial questions involving polytopes and Möbius algebras of partially ordered sets.

We use the notation $P=(X, \leqslant)$ to stand for the set X partially ordered by a relation $\leqslant$. We assume X is finite and labeled as $\{x_1, x_2, \ldots, x_n\}$. The Möbius function of P [5] will be of fundamental importance in our work. If Z is the matrix given by

$$Z_{ij} = \zeta(x_i, x_j) = \begin{cases} 1 & \text{if } x_i \leqslant x_j, \\ 0 & \text{otherwise,} \end{cases}$$

then Z has an inverse M (over the integers) and the Möbius function of P is given by

$$\mu(x_i, x_j) = M_{ij}.$$

The fundamental theorem of Möbius inversion (denoted by FTMI hereafter) is:

(FTMI) *If f and g are functions defined on X with values in an abelian group, then*

$$f(x) = \sum_{y : y \geqslant x} g(x)$$

if and only if

$$g(x) = \sum_{y : y \geq x} \mu(x, y) f(y).$$

(Note that since μ is integer valued this sum makes sense in any abelian group.)

2. Constructing codes from posets

For each $x \in X$ we define vectors v_x and e_x by

$$v_x(i) = \zeta(x, x_i) = \begin{cases} 1 & \text{if } x \leq x_i, \\ 0 & \text{otherwise} \end{cases}$$

and

$$e_x(i) = \delta(x, x_i) = \begin{cases} 1 & \text{if } x = x_i, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 1. *The vectors v_x form a basis for the vector space F^n.*

Proof. By FTMI each e_x is a linear combination of the vectors v_x. □

Proposition 2. *If $v = \sum_{x \in X} a_x v_x = \sum_{x \in X} b_x e_x$, then $a_x = \sum_{z : z \leq x} \mu(z, x) b_z$.*

Proof. By FTMI, $e_x = \sum_{y : y \geq x} \mu(x, y) v_y$. Thus

$$v = \sum_{x \in X} b_x \sum_{y : y \geq x} \mu(x, y) v_y = \sum_{y \in X} \sum_{z : z \leq y} b_z \mu(z, y) v_y$$

$$= \sum_{y \in X} \Big(\sum_{z : z \leq y} b_z \mu(z, y) \Big) v_y.$$

By equating coefficients, we obtain the conclusion of the proposition. □

For each subset S of X, let RM(P, S) be the subspace of F^n spanned by the elements v_s for $s \in S$. This is an $|S|$ dimensional code. We shall call the codes RM(P, S) the *incidence codes* of P.

3. Codes constructed from Eulerian posets

We say P is *Eulerian* if in each interval of P, all maximal chains have the same length and the Möbius function is given by

$$\mu(x, y) = (-1)^{l[x, y]},$$

when x is less than or equal to y, ($l[x, y]$ stands for the length of the interval from

x to y). (The term is due to Richard Stanley.) Standard examples of Eulerian Posets, from [6] are:

(1) The subsets of a set, ordered by set inclusion.

(2) The faces of a convex polytope, ordered by set inclusion.

(3) the simplexes of a simplicial polytope, ordered by set inclusion.

In addition, a partially ordered set whose Möbius function is always odd is Eulerian in the 2 element field.

We assume for the remainder of this section that our partially ordered set is Eulerian (in the field under consideration) and that given two elements x and y with an upper bound, they have a least upper bound, denoted by $x \vee y$. The 3 examples above all have this property.

Now let x be a maximal element of S, and let $w \geqslant x$. Then for the vector $v = \sum a_t v_t$, $a_w = 0$ for $w > x$, so

$$\begin{aligned} a_w = \delta(x, w)a_x &= \sum_{z:z\leqslant w} \mu(z, w)b_z \\ &= \sum_{y:x\leqslant y\leqslant w} \sum_{z:z\vee x=y} \mu(z, w)b_z \\ &= \sum_{y:x\leqslant y\leqslant w} \sum_{z:z\vee x=y} \mu(z, y)\mu(y, w)b_z \\ &= \sum_{y:x\leqslant y\leqslant w} \mu(y, w)f(y), \end{aligned}$$

where $f(y) = \sum_{z:z\vee x=y} \mu(z, y)b_z$. Then the dual form of FTMI gives us

$$f(w) = \sum_{y:x\leqslant y\leqslant w} \delta(x, y)a_x = a_x,$$

which gives us

Proposition 3. *For each x maximal in S and each $w \geqslant x$,*

$$a_x = \sum_{z:z\vee x=w} \mu(z, w)b_z.$$

Proposition 4. *The minimum distance d of $\mathrm{RM}(P, S)$ is the minimum number of elements of X greater than or equal to any element x of S.*

Proof. Let $\sum_{x\in X} a_x v_x = v \in \mathrm{RM}(P, S)$ and assume that $a_x \neq 0$ for some maximal x in S. Then each of the equations given in Proposition 3 must contain at least one nonzero b_t. However, no b_t occurs in more than one equation, so there must be at least one nonzero b_t for each $w \geqslant x$. If a_x is zero for each maximal element x of S, simply remove all maximal elements from S to get S', note that $v \in \mathrm{RM}(P, S')$ and repeat the argument. □

Proposition 5. *If a vector v in F^n differs from $v' \in \mathrm{RM}(P, S)$ in fewer than $\frac{1}{2}d$ coordinates, v' may be obtained from v by the following decoding process. For a*

maximal element x of S, let a_x be what a majority of the equations in Proposition 3 say it should be. Subtract $a_x v_x$ from v, delete x from S and repeat the process.

Proof. By assumption, fewer than $\frac{1}{2}d$ of the b_t's are incorrect, so fewer than $\frac{1}{2}d$ of the equations are incorrect. □

Proposition 6. *If S is not an order ideal of P, we can add elements of X below elements of S to S and thereby increase the dimension of* RM(P, S) *without changing n or d.*

Proof. n is the number of elements of X and d is not changed if we change S without changing its maximal elements. □

4. Examples

We let X consist of the empty set, the vertices of a square, the edges of the square and the square itself. We let $\leqslant$ be set inclusion. If S consists of the empty set and the four vertices, then $R(P, S)$ is a $(10, 5, 4)$ code. If we delete the square itself from X, then $R(P, S)$ is a $(9, 5, 3)$ code. If we delete the empty set (but not the square itself) from both X and S, then $R(P, S)$ is a $(9, 4, 4)$ code. (As is always the case for posets Eulerian over the integers, any choice of field is appropriate.)

If we take P to be the subsets of an m element set, ordered by set inclusion, and take S to be the subsets of size r or less, we obtain a code of length 2^m and minimum distance 2^{m-r} whose dimension is the sum of the first r binomial coefficients.. (It should be clear that if F is the 2 element field, these are the Reed–Muller codes.) In particular if $m = 2s+1$, and $r = s$ then $k = 2^{2s}$, and $d = 2^{s+1}$, so that $k = \frac{1}{2}n$ and $d = \sqrt{2n}$.

If we take P to be the subspaces of a vector space over a q-element field (q an odd prime power), then $\mu(x, y)$ is odd (a power of q) whenever $x \leqslant y$ [1], and so over a field of characteristic 2, P is Eulerian. In general, the codes that arise in this way are not particularly impressive in comparison with Reed–Muller codes. If, for example, we use a 3-dimensional vector space (i.e., a projective plane of order q) and let S be the subspaces of dimension 0 and 1 (i.e., the empty set and the points), then $n = 2(q^2+q+2)$, $k = q^2+q+2$ and $d = q+3$. Thus $k = \frac{1}{2}n$ and $d = \frac{1}{2}\sqrt{2n-7} - \frac{1}{2}$. Thus for large values of n, these codes will have about half the error correcting capacity of Reed–Muller codes. For $q = 5$, $n = 64$, $k = 32$ and $d = 8$. The third order Reed–Muller code of length 64 has $d = 8$ also, but has $k = 42$. Other codes constructed from subspace lattices over odd order fields are similarly disappointing (or more so). A similar construction utilizing block designs gives no better results.

We can obtain interesting codes from non-Eulerian posets. For example, let P be the points and lines of the projective plane of order 2 and the plane itself ordered by set inclusion. Then over a field of characteristic 3, $\mu(x, y) = 1$ if $x = y$

and otherwise $\mu(x, y) = -1$. Thus P is not Eulerian. If we take S to be the set of points, then RM(P, S) has length 15 and dimension 7. (A generator matrix for RM(P, S) may be obtained from the dual of a difference set or projective plane code [4] by adding a column of ones and identity matrix to the generator matrix for the dual described in [4].)

Now each basis vector v_i of the code has weight 5. Given 2 points of a projective plane, there is only one line they have in common, so a linear combination of two of the basis vectors v_i must have weight at least 6, since each of the 2 points is incident with 2 lines that do not contain the other point. If 3 points lie on a line, each of the 6 other lines contains exactly one of these points, so a linear combination of the three basis vectors corresponding to these points will have weight at least 9. If 3 points are not colinear there are 3 lines that each contain exactly one of the points, so a linear combination of the corresponding basis vectors must have weight at least 6. Given 4 points, if 3 are colinear, then there are 3 lines containing only one of them, so any linear combination of the corresponding basis vectors must have weight at least 7. Finally given 4 points, no 3 of which are colinear, all lines except for one contain a 2 element subset of the 4 points, and all 6 2 element subsets are contained by exactly one of these lines. Thus for a linear combination of the four corresponding basis vectors to have weight 4 or less, each basis vector must occur with a sign opposite each other basis vector – which is impossible! Since any linear combination of 5 or more of the basis vectors has weight at least 5 the code has minimum distance 5.

With the exception of some of the Reed–Muller Codes, none of these examples are the best known codes.

5. Möbius algebras and Reed–Muller codes

The vector space F^n is an algebra under componentwise multiplication.

Proposition 7. *If x and y have a least upper bound in P, then $v_x \cdot v_y = v_{x \vee y}$.*

Proof. $v_{x\vee y}(i) = 1$ if and only if $x \vee y \leqslant x_i$ if and only if $x \leqslant x_i$ and $y \leqslant x_i$ iff $v_x(i) = 1$ and $v_y(i) = 1$. □

From Proposition 7 it is immediate that F^n together with the basis of incidence vectors of P is isomorphic to the Möbius algebra [2] of P in the case that P is a join semilattice. In the case of a more general partially ordered set, the product of two elements u and w of X in the Möbius algebra of P is given by

$$u \cdot w = \sum_{x \in X} \sum_{\substack{t : t \geqslant u \\ t \geqslant w}} \mu(t, x) x.$$

(This is the dual form of the product formula given in [2].)

Proposition 8. *The algebra F^n with the basis of incidence vectors is the Möbius algebra of P.*

Proof. The product formula given above follows immediately from

$$v_u \cdot v_w = \sum_{\substack{t : t \geq u \\ t \geq w}} e_t$$

since $e_t = \sum_{x : x \geq t} \mu(t, x) v_x$ as in Proposition 2.

Proposition 9. *If P is a join semilattice in which each element is a join of atoms, and S consists of the elements of rank r or less in P, then* RM(*P, S*) *consists of all polynomials of degree r or less in the vectors v_a with a an atom of P.*

Proof. Immediate from the definitions. □

The algebra of Boolean polynomials in m variables over a field F is

$$F[X_1, X_2, \ldots, X_m]/(X_1^2 - X_1, X_2^2 - X_2, \ldots, X_m^2 - X_m),$$

i.e., the algebra generated by n idempotent indeterminates.

Proposition 10. *If P is the lattice of subsets of an m-element set M, then the map sending $v_{\{i\}}$ to X_i for each $i \in M$ extends to an isomorphism of the Möbius algebra of P over F onto the algebra of Boolean polynomials over F.*

Proof. Immediate from the definitions. □

MacWilliams and Sloane [4] define the binary rth order Reed–Muller code of length 2^m to be Boolean polynomials of degree r or less regarded as a subspace of the space of all Boolean polynomials over the 2 element field. Thus from Proposition 9 and 10 it is clear that RM(*P, S*) is a Reed–Muller code when P is the lattice of subsets of a set and S is the collection of subsets of size r or less.

6. Some conjectures and questions

A number of largely combinatorial problems, motivated by the theory of error correcting codes, arise from the study of incidence codes. The two motivations from coding theory are:

Given n and d, find the largest value of k for which an (n, k, d) code (perhaps of a special type) exists.

Find families of (n_m, k_m, d_m) codes C_m, one member of the family for each integer, and numbers ε_1 and ε_2 such that for all m, $k_m/n_m > \varepsilon_1$ and $d_m/n_m > \varepsilon_2$.

Conjecture 1. If an incidence code of a convex polytope has length 2^n, and minimum distance 2^{n-r}, then either the dimension of the code is less than that of the rth order Reed–Muller code or else the polytope is a simplex (and the code is thus the rth order Reed–Muller code.)

Question 2. What is the maximum dimension of an incidence code of length n and minimum distance d?

Conjecture 3. If $\{P_m \mid m \in I\}$ is a sequence of Eulerian partially ordered sets and the parameters n_m and k_m of one incidence code for each member of the sequence satisfy $k_m/n_m > \varepsilon$, then $\lim_{n\to\infty} d_m/n_m = 0$.

Question 4. What can one say about Eulerian posets in general? What about posets that are Eulerian mod p? In particular, what can one say about a poset whose Möbius function $\mu(x, y)$ is odd whenever $x \leqslant y$?

Question 5. Are the codes consisting of polynomials of degrees r or less in the incidence vectors of the atoms of a poset (regarded as a subspace of the Möbius algebra) better than incidence codes when the poset is not a join semilattice?

Question 6. Are the codes constructed by Liebler [3], using Möbius function to construct orthogonal parity checks, either incidence codes or a natural generalization of incidence codes?

Question 7. Projective and Euclidean geometry codes may be defined by using a different kind of incidence relation [4]. Our final example suggests that the relationships between the two kinds of incidence relations might prove fruitful. Is there a useful common generalization?

References

[1] E.A. Bender and J.R. Goldman, On the applications of Möbius inversion in combinatorial analysis, American Mathematical Monthly 82 (1975) 789.
[2] C. Green, On the Möbius algebra of a partially ordered set, Advances in Math. 10 (1973) 177.
[3] R.A. Liebler, On codes in the natural representation of the symmetric group, Proceedings of Young Day, 1978.
[4] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland Math. Libr., Vol. 16 (North-Holland, Amsterdam–New York, 1977).
[5] G.-C. Rota, On the foundations of combinatorial theory I: Theory of Möbius functions, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 2 (1964) 340.
[6] R.P. Stanley, Combinatorial reciprocity theorems, Advances in Math. 14 (1974) 194.