

### 3. The code associated with f

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **40 (1994)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **30.06.2024**

#### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

#### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

3. THE CODE ASSOCIATED WITH  $f$ 

We will denote by  $M_n$  the set of square-free monomials in the variables  $x_1, \dots, x_n$ . We consider  $M_n$  as a multiplicative group, by imposing the relations  $x_i^2 = 1$  for all  $i = 1, \dots, n$ . Note that  $M_n$  is then isomorphic to  $\{1, -1\}^n$ .

Let  $f = u_1 + \dots + u_N$  be a polynomial in  $x_1, \dots, x_n$  with non-negative integral coefficients, and with monomials  $u_1, \dots, u_N \in M_n$ . The  $u_i$  need not be distinct, nor necessarily distinct from 1.

*Definition.*

1. The matrix  $\Phi_f = (\Phi_{i,j})$  associated with  $f$  is the  $n \times N$  matrix over  $\mathbf{F}_2$ , defined by

$$\Phi_{i,j} = \begin{cases} 1 & \text{if } x_i \text{ divides } u_j, \\ 0 & \text{if not.} \end{cases}$$

Note that  $\Phi_f$  is defined up to a permutation of its columns.

2. The binary code  $L_f$  associated with  $f$  is the subcode of  $\mathbf{F}_2^N$  generated by the  $n$  rows of the matrix  $\Phi_f$ .

Note that the dual code  $K_f := L_f^\perp$  sits in the following exact sequence:

$$0 \rightarrow K_f \rightarrow \mathbf{F}_2^N \xrightarrow{\Phi_f} \mathbf{F}_2^n.$$

Indeed,  $K_f$  admits  $\Phi_f$  as a parity check matrix. Note also that any binary code  $C$  is of the form  $C = L_f$  for some polynomial  $f$  with non-negative coefficients in  $x_1, \dots, x_n$ . Indeed, such an  $f$  can be obtained as the sum of the monomials corresponding to the columns of any generator matrix for  $C$ .

We will now give a second description of the code  $L_f$ . With any  $p \in \{1, -1\}^n$ , we associate

- a subset  $v_f(p)$  of  $\{1, \dots, N\}$ , defined as

$$v_f(p) = \{i = 1, \dots, N \mid u_i(p) = -1\}, \text{ and}$$

- a codeword  $c_f(p)$  in  $\mathbf{F}_2^N$ , defined as

$$c_f(p) = \sum_{i \in v_f(p)} E_i,$$

where  $\{E_1, \dots, E_N\}$  denotes the standard basis of  $\mathbf{F}_2^N$ .

We claim, among other things, that the image of the map

$$c_f: \{1, -1\}^n \rightarrow \mathbf{F}_2^N$$

is exactly the code  $L_f$  associated with  $f$ .

PROPOSITION 1. Let  $f = u_1 + \dots + u_N$  with  $u_i \in M_n$  for all  $i$ . Let  $c = c_f$  and  $L = L_f$  denote its associated map and code. Then we have:

1. The map  $c : \{1, -1\}^n \rightarrow \mathbf{F}_2^N$  is a group homomorphism;
2.  $\text{Im}(c) = L$ ;
3.  $\text{Ker}(c) = \{p \mid f(p) = N\}$ ;
4. For every  $p \in \{1, -1\}^n$ , the weight of  $c(p)$  is related to the value  $f(p)$  by

$$f(p) = N - 2 |c(p)|.$$

*Proof.*

1. Let  $p, p' \in \{1, -1\}^n$ . Then  $v_f(pp')$  is obviously equal to the symmetric difference of  $v_f(p)$  and  $v_f(p')$ , hence

$$c(pp') = c(p) + c(p').$$

2. For every  $i = 1, \dots, n$ , let  $p_i \in \{1, -1\}^n$  denote the point which has a  $-1$  at the  $i$ -th coordinate, and a  $1$  elsewhere. Since the  $n$  points  $p_1, \dots, p_n$  generate  $\{1, -1\}^n$  as a group, their images under  $c$  generate  $\text{Im}(c)$ . Now,

$$\begin{aligned} v_f(p_i) &= \{j \mid u_j(p_i) = -1\} \quad (\text{by definition}) \\ &= \{j \mid x_i \text{ divides } u_j\}. \end{aligned}$$

Therefore,  $c(p_i)$  coincides with the  $i$ -th row of the matrix  $\Phi_f$ . Since these rows generate  $L$  by definition, the claim is proved.

3. If  $p \in \{1, -1\}^n$ , then

$$c(p) = 0 \Leftrightarrow v_f(p) = \emptyset \Leftrightarrow u_i(p) = 1 \forall i \Leftrightarrow f(p) = N.$$

4. Let  $r = |c(p)| = |v_f(p)|$ . Then

$$f(p) = \sum_{i=1}^N u_i(p) = (r)(-1) + (N-r)(1) = N - 2r. \quad \square$$

We will now show that the value enumerator of  $f$ , defined as

$$V_f(T) = \sum_{p \in \{\pm 1\}^n} T^{f(p)},$$

is completely determined by the weight enumerator of  $L_f$ . (And of  $L_f^\perp$  as well, by the MacWilliams identity.)

**THEOREM 2.** *Let  $f = u_1 + \dots + u_N$  ( $u_i \in M_n$  for all  $i$ ) and let  $L = L_f$  be its associated code. Then*

$$V_f(T) = 2^{n - \dim L} \cdot T^N \cdot P_L \left( \frac{1}{T^2} \right).$$

*Proof.*

$$\begin{aligned} V_f(T) &= \sum_{p \in \{\pm 1\}^n} T^{f(p)} \\ &= \sum_p T^{N - 2|c(p)|} \quad (\text{by Proposition 1}) \\ &= T^N \sum_p \left( \frac{1}{T^2} \right)^{|c(p)|}. \end{aligned}$$

As  $p$  runs through  $\{1, -1\}^n$ ,  $c(p)$  runs through  $L$  by Proposition 1. Furthermore, since  $c$  is a homomorphism, the fiber  $c^{-1}c(p)$  of  $c(p)$  contains  $|\text{Ker } c|$  elements, for every  $p$ . Thus,

$$\begin{aligned} \sum_p \left( \frac{1}{T^2} \right)^{|c(p)|} &= |\text{Ker } c| \cdot \sum_{z \in L} \left( \frac{1}{T^2} \right)^{|z|} \\ &= |\text{Ker } c| \cdot P_L \left( \frac{1}{T^2} \right). \end{aligned}$$

As  $\dim(\text{Ker } c) = n - \dim(\text{Im } c) = n - \dim(L)$ , the claimed formula follows.  $\square$

*Notation.* For any  $v \in \mathbf{Z}$ , we will denote by  $f^{-1}(v)$  the “binary fiber” of  $v$ , i.e. the set

$$f^{-1}(v) = \{p \in \{1, -1\}^n \mid f(p) = v\}.$$

Note that  $f(p) \equiv N \pmod 2$  for every binary point  $p$ , for  $1 \equiv -1 \pmod 2$ .

**COROLLARY 3.** *For every  $v \in \mathbf{Z}$ , the cardinality of  $f^{-1}(v)$  is equal to  $2^{n - \dim L}$  times the number of codewords in  $L$  which are of weight  $(N - v)/2$ .*

*Proof.* The cardinality of  $f^{-1}(v)$  is equal to the coefficient  $b_v$  of  $T^v$  in the Laurent polynomial  $V_f(T)$ . By the theorem,

$$b_v = 2^{n - \dim L} \cdot a_w,$$

where  $v = N - 2w$ , and where  $a_w$  is the coefficient of  $T^w$  in  $P_L(T)$ .  $\square$

**EXAMPLE 1:** *the Hamming code.*

Let  $f = (1 + x_1) \cdots (1 + x_n) - 1$ . Developing  $f$  as a sum of monomials in  $M_n$ , we have

$$f = \sum_{u \in M_n \setminus \{1\}} u.$$

Thus the associated matrix  $\Phi_f$  is the  $n \times (2^n - 1)$  matrix over  $\mathbf{F}_2$  whose columns are the elements of  $\mathbf{F}_2^n$ , except 0. By definition, this matrix is the parity check matrix of the Hamming code  $H_n$ . Thus, in our terminology, the Hamming code  $H_n$  is *the dual of the code  $L_f$  associated with  $f$* .

The value enumerator of  $f$  is readily obtained. We have

$$f(p) = \begin{cases} 2^n - 1 & \text{if } p = (1, \dots, 1), \\ -1 & \text{if not.} \end{cases}$$

Therefore,

$$V_f(T) = (2^n - 1)T^{-1} + T^{2^n - 1}.$$

Let  $P_L(T)$  be the weight enumerator of  $L = L_f$ . By Theorem 2, we have

$$\begin{aligned} P_L(T^{-2}) &= T^{1-2^n} \cdot V_f(T) \\ &= T^{1-2^n} \cdot ((2^n - 1)T^{-1} + T^{2^n - 1}) \\ &= (2^n - 1)T^{-2^n} + 1, \end{aligned}$$

and hence  $P_L(T) = 1 + (2^n - 1)T^{2^n - 1}$ .

Finally, by the MacWilliams identity, the weight enumerator of the Hamming code  $H_n = L^\perp$ , is equal to

$$P_{H_n}(T) = \frac{1}{2^n} [(1 + T)^{2^n - 1} + (2^n - 1)(1 + T)^{2^n - 1 - 1}(1 - T)^{2^n - 1}].$$

EXAMPLE 2: *the Reed-Muller code  $\mathcal{R}(r, m)$ .*

Let  $m$  be a positive integer, and let  $[m] := \{1, \dots, m\}$ . We consider  $2^m$  variables  $\{x_a\}$ , indexed by the subsets  $a \subset [m]$ . If  $J$  is a set of subsets of  $[m]$ , we denote by  $u_J$  the monomial

$$u_J := \prod_{a \in J} x_a.$$

If  $a \subset [m]$  and if  $i \leq m$ , we denote by  $a^{(i)}$  the set of subsets of cardinality  $i$  in  $a$ . Now, given a non-negative integer  $r \leq m$ , we define the polynomial

$$f_{r,m} := \sum_{a \subset [m]} u_{a^{(0)}} \cdots u_{a^{(r)}}.$$

The code  $L_f$  associated with  $f = f_{r,m}$ , then, is known as the  $r$ th-order binary Reed-Muller code  $\mathcal{R}(r, m)$ . Checking the claim is left to the reader. The determination of the weight enumerator of  $\mathcal{R}(r, m)$  is an open problem for  $r \geq 3$ . [MS, Chapter 15.]