1. REDUCTION TO ONE SPECIAL EQUATION

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **21.09.2024**

of f, involving the value at -1 of a high order derivative of the weight enumerator of $L_f^{\perp}$.

The main result is a general enumeration formula, stated in Theorem 4. This formula is then applied to enumerate Hadamard matrices (Theorem 6), and the proper 4-colorings of a graph (Theorem 7), in terms of the weight enumerators of suitable binary codes. For Hadamard matrices, there seems to be no other enumeration formula in the literature.

As hinted in Section 1, similar enumeration formulas could be obtained for other combinatorial objects, such as conference matrices, Barker sequences, Golay complementary sequences, block designs, labelled regular graphs, proper graph q-colorings, and more.

1. Reduction to one special equation

Throughout the paper, we will consider a single polynomial f in n variables, with integral and non-negative coefficients, and with square-free monomials only.

This situation should be sufficiently general for most combinatorial applications. Indeed, many objects in combinatorics are defined as the solution set in $\{1, -1\}^n$, or in $\{0, 1\}^n$, of some system of polynomial equations

$$\{f_1(p) = \cdots = f_r(p) = 0\}$$

in n variables with integral coefficients. Think of Hadamard matrices, conference matrices, Barker sequences [B], Golay pairs [G, EKS], block designs, labelled regular and strongly regular graphs, proper graph colorings, etc.

By a suitable change of variables if necessary, we may and will restrict our attention to equations on $\{1, -1\}^n$. Since we are only interested in binary and hence real solutions, the system $\{f_1(p) = \cdots = f_r(p) = 0\}$ can be reduced to an equivalent single equation

$$\{f(p) = 0\},$$

where $f = f_1^2 + \cdots + f_r^2$.

Furthermore, we may assume that f has non-negative coefficients only. Indeed, suppose $f = f_1 - f_2$, where f_1, f_2 have non-negative coefficients. Introducing a new variable x_0, the system $\{f = 0\}$ is equivalent to the system $\{x_0 + 1 = 0, f_1 + x_0 f_2 = 0,\}$, which in turn is equivalent to the single equation

$$\{\hat{f} = 0\},$$

where $\hat{f} = (x_0 + 1)^2 + (f_1 + x_0 f_2)^2$. Of course, all coefficients of $\hat{f}$ are non-negative, as desired.

Finally, we may assume that all monomials in f are square-free, by removing any square in any monomial if necessary. The values assumed by f on binary points will not be altered, for if u, v are monomials, then $u^2v - v$ takes the constant value 0 on $\{1, -1\}^n$.

2. Coding Theory

To fix the notation and terminology, we briefly recall a few notions from coding theory. For more information, see [MS].

Consider the vector space $\mathbf{F}_2^N$ with its canonical basis fixed. The *(Hamming) weight* $|z|$ of a vector $z \in \mathbf{F}_2^N$ is the number of non-zero coordinates of z. A *binary linear code* (or *code,* for short) is a vector subspace C of $\mathbf{F}_2^N$. The integer N is called the *length* of C. The *weight enumerator* of C is the polynomial

$$P_C(T) = \sum_{z \in C} T^{|z|} .$$

A *generator matrix* for C is a $k \times N$ matrix G over $\mathbf{F}_2$ whose rows span C. A *parity check matrix* for C is an $(N-k) \times N$ matrix H over $\mathbf{F}_2$ such that

$$C = \{z \in \mathbf{F}_2^N, \quad H \cdot z^{\mathsf{T}} = 0\} .$$

Equivalently, C is the kernel of the map $h : \mathbf{F}_2^N \to \mathbf{F}_2^{N-k}$ whose matrix in the standard bases is H. The *dual* of C is the space

$$C^{\perp} = \{y \in \mathbf{F}_2^N \mid y \cdot z = 0 \text{ for all } z \in C\} ,$$

where $y \cdot z$ denotes the usual dot product of y and z with value in $\mathbf{F}_2$. We have:

$$\dim C^{\perp} = N - \dim C, \text{ and } C^{\perp\perp} = C .$$

A binary matrix H is a generator matrix for C if and only if it is a parity check matrix for $C^{\perp}$. Finally, the weight enumerator of C determines the weight enumerator of its dual $C^{\perp}$ by the *MacWilliams identity* [M]:

$$P_{C^{\perp}}(T) = \frac{1}{|C|} \cdot (1 + T)^N \cdot P_C\left(\frac{1 - T}{1 + T}\right) .$$