WEIGHT ENUMERATORS OF CODES

N.J.A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974, USA

ABSTRACT

A tutorial paper dealing with the weight enumerators of codes, especially of self-dual codes. We prove MACWILLIAMS' theorem on the weight distribution of the dual code, GLEASON's theorem on the weight distribution of a self-dual code, some generalizations of this theorem, and then use GLEASON's theorem to show that very good self-dual codes do not exist.

1. INTRODUCTION

We shall mostly consider codes which are *binary* (have symbols from F_2, the field with two elements) or *ternary* (have symbols from F_3, the field with 3 elements). Let F_q^n denote the vector space of all vectors of length n, i.e., having n components, from F_q.

An $[n,k]$ *code* C over F_q is a subspace of F_q^n of dimension k. The vectors of C are called *codewords*. So a binary code is a set of vectors which is closed under addition. A ternary code is closed under addition and under multiplication by -1.

The *(Hamming) weight* of a vector $x = (x_1,\ldots,x_n) \in F_q^n$, denoted by $\mathrm{wt}(x)$, is the number of non-zero x_i; and the *(Hamming) distance* between vectors $x,y \in F_q^n$ is $\mathrm{dist}(x,y) = \mathrm{wt}(x-y)$.

If every non-zero codeword in C has weight $\geq d$, the code is said to have *minimum weight* d, and is called an $[n,k,d]$ code; n,k,d are the basic parameters of the code. The codewords contain n symbols, and so the *rate* or *efficiency* of the code is $\frac{k}{n}$. Furthermore the code can correct $[\frac{d-1}{2}]$ errors.

M. Hall, Jr. and J. H. van Lint (eds.). Combinatorics, 115-142.

The *dual code* $C^\perp$ is the orthogonal subspace to C:

$$C^\perp = \{u \mid u\cdot v = \sum_{i=1}^{n} u_i v_i = 0, \text{ for all } v \in C\}.$$

$C^\perp$ is an $[n,n-k]$ code.

If $C \subset C^\perp$, C is called *self-orthogonal*, while if $C = C^\perp$ it is called *self-dual*. (See the examples below.)

Let A_i be the number of codewords in C with weight i. Then the set $\{A_0,\ldots,A_n\}$ is called the *weight distribution* of C. It is more convenient to make a polynomial out of the A_i's. The *weight enumerator* of C is

$$W_C(x,y) = A_0x^n + A_1x^{n-1}y + \ldots + A_ny^n =$$

$$= \sum_{i=0}^{n} A_i x^{n-i}y^i = \sum_{u\in C} x^{n-wt(u)}y^{wt(u)}.$$

This is a homogeneous polynomial of degree n in the indeterminates x and y. We could get rid of x by setting $x = 1$, but the theorems are simpler if W is homogeneous.

The weight enumerator gives a good deal of information about the code (see for example [1, §16.1] for some things you can do with the weight enumerator). But is has been calculated for only a few families of codes (e.g. Hamming codes [34], second order Reed Muller codes [41]).

OPEN PROBLEM 1. Find the weight enumerators of all Reed Muller codes (cf. [15]).

We mention in passing a related problem. The distribution of coset leaders by weight is also important for finding the error probability of a code, and for other reasons. But almost nothing is known about calculating it ([4],[12],[42]).

OPEN PROBLEM 2. Find the weight distribution of the coset leaders of the first order Reed Muller codes.

A code is *maximal self-orthogonal* if it is self-orthogonal and is not contained in any larger self-orthogonal code. For binary codes, a maximal self-orthogonal code has dimension $k = \frac{n-1}{2}$ if n is odd, or $k = \frac{n}{2}$ (and is self-dual) if n is even. This paper is concerned with weight enumerators of maximal self-orthogonal codes. First we give some examples.