Hence

$$W(2) = \sum_{i=1}^{t-1} n^2 (n-t-i)! + \frac{n^2(n-2t+1)}{2}(n-2t+1)!,$$

$$n \geqq 2t+1.$$

Three runs of length $t$ can occur in one of three ways: (i) one run of length $t+2, t+3, \cdots, 3t-2$, (ii) one run of length $t$ and one of length $t+1, t+2, \cdots, 2t-1$, or (iii) three disjoint runs of length $t$. In the first case, as before, one run of length $t+i$ can begin on any one of $n$ symbols, leaving $(n-t-i)!$ ways of permuting the $n-t$ remaining symbols and $n$ ways of shifting each permutation cyclically. Now, however, we get an additional factor of $i-1$, as there are $i-1$ places on which the middle run can begin. In the second case, there are $n(n-2t+1-i)$ ways of choosing two disjoint runs of length $t$ and $t+i$, $(n-2t+1-i)!$ ways of permuting the $n-2t+1-i$ subsets that remain when one run is fixed in place, and $n$ ways of shifting each permutation cyclically. In the third case, there are $n(n-3t+2)(n-3t+1)/6$ ways of choosing three disjoint runs of length $t$, $(n-3t+2)!$ ways of permuting the $n-3t+2$ subsets that remain when one run is fixed in place, and $n$ ways of shifting each permutation cyclically.

Hence

$$W(3) = \sum_{i=2}^{2t-2} (i-1) n^2 (n-t-i)!$$

$$+ \sum_{i=1}^{t-1} n^2 (n-2t+1-i)(n-2t+1-i)!$$

$$+ \frac{n^2(n-3t+2)(n-3t+1)}{6}(n-3t+2)!,$$

$$n \geqq 3t+1.$$

We leave it to the intrepid reader to expand $1 - W(1)/n! + W(2)/n! - W(3)/n!$ in a power series in $1/n$ and verify that the terms given in the statement of the theorem are correct. With this the proof of Theorem 2 is complete.

It is evident that the above procedure can be continued to give the asymptotic expansion of $F(n,t)/n!$ to any desired accuracy.

# C. Coding Theory: Moments of Weight Distributions

R. Stanley

## 1. Introduction

In Section 2 of this report, a general combinatorial formula is developed which allows calculation of sums of the type

$$\sum_{v \in S} [\sigma(v)]^t, \qquad 0 \leqq t \leqq r$$

where $S$ is a set of vectors $v$, $\sigma(v)$ is the sum of the coordinates of $v$, and $r$ is an integer depending on a special property of the set $S$. In Section 3, this formula is applied to $(n,k)$ binary codes and yields explicit formulas for the sums

$$\sum_{i=0}^{n} i^t a_i, \qquad 0 \leqq t < d$$

where $a_i$ words of the code have weight $i$, and $d$ is the minimum weight of the dual code. When enough information about a code is known, these equations may suffice to determine its weight distribution. As an example, we calculate the weight distribution of the dual Golay (23, 11) code without using J. MacWilliams' formula.

## 2. A Combinatorial Formula

Let $P = \{x_1, \cdots, x_p\}$ be a subset of a commutative ring $R$, and let $S$ be a subset of order $s$ of the direct product $P^n = P \times P \times \cdots \times P$ ($n$ times). Assume that $S$ has the following property for some integer $r \leqq n$:

(1) The restriction of $S$ to any $r$ coordinates contains all $p^r$ $r$-tuples of elements of $P$ the same number of times. (This necessitates $p^r | s$.)

Let $\sigma(v)$ denote the sum (in $R$) of the coordinates of the element $v$ of $S$. We then have:

*Theorem 1.* For $0 \leqq t \leqq r$, the sum

$$\sum_{v \in S} [\sigma(v)]^t$$

depends only on $P, n, s$ (not on $S$), and we have

$$\frac{p^n}{s} \sum_{v \in S} (\sigma(v))^t = \sum_{v \in P^n} (\sigma(v))^t. \qquad (2)$$

*Proof.* Denote the vectors in $S$ by

$$\begin{matrix}(v_{11}, v_{12}, \cdots, v_{1n})\\ (v_{21}, v_{22}, \cdots, v_{2n})\\ \vdots\\ (v_{s1}, v_{s2}, \cdots, v_{sn}).\end{matrix} \tag{3}$$

Expanding by the multinomial theorem, we get

$$\sum_{v\in S}(\sigma(v))^t = \sum_{i=1}^{s}(v_{i1}+v_{i2}+\cdots+v_{in})^t$$

$$= \sum_{i=1}^{s}\sum_{\substack{a_1+a_2+\\ \cdots+a_n=n\\ 0\le a_i\le n}} \frac{n!}{a_1!\,a_2!\cdots a_n!}\, v_{i1}^{a_1} v_{i2}^{a_2}\cdots v_{in}^{a_n}$$

$$= \sum_{\substack{a_1+a_2+\\ \cdots+a_n=n\\ 0\le a_i\le n}} \frac{n!}{a_1!\,a_2!\cdots a_n!}\left(\sum_{i=1}^{s} v_{i1}^{a_1} v_{i2}^{a_2}\cdots v_{in}^{a_n}\right).$$

In the sum in parenthesis, at most $t$ of the exponents $a_1, a_2, \cdots, a_n$ are nonzero, say $a_{i_1}, a_{i_2}, \cdots, a_{i_m}$. As $i$ ranges from 1 to $s$, it follows by property (1) that the set $v_{i_1}, v_{i_2}, \cdots, v_{i_m}\}$ ranges through a complete set of $p^m$ $m$-tuples, with each $m$-tuple occurring the same number $(p^{s-m})$ of times. Hence, the sum in parenthesis depends only on $P$, $s$, and $a_1, a_2, \cdots, a_n$. Therefore, the entire sum depends only on $P$, $s$, and $n$, as asserted.

Consider the array obtained by repeating Eq. (3) $p^n/s$ times. This array contains $p^n$ vectors and satisfies property (1). The set $P^n$ also contains $p^n$ vectors and satisfies property (1) for any $r \le n$. Hence, by what we have just proved, we must have Eq. (2) holding, and the proof of Theorem 1 is complete.

The proofs of the following simple observations are left to the reader.

**(A)** If a set $S$ satisfies property (1), then the set obtained by restricting the vectors of $S$ to any $m < n$ coordinates also satisfies property (1). (This corresponds to *puncturing* a code.)

**(B)** Assume that the set $P$ is closed under addition, so that it forms an additive group, and that a set $S \subseteq P^n$ satisfies property (1). If $v$ is any vector in $P^n$, then the set $S + v = \{v_0 + v : v_0 \in S\}$ also satisfies property (1). In particular, if $S$ is a subspace of $P^n$ over $R$ satisfying property (1), then all its cosets satisfy (1).

*Example.* Define two $n \times n$ matrices of 0's and 1's to be *equivalent* if one can be transformed into the other by complementing appropriate rows and columns. It is easily verified that this definition of equivalence indeed gives an equivalence relation. In fact, if we regard the 0's and 1's as belonging to the field $GF(2)$, then the equivalence class containing the 0 matrix forms an additive group of order $2^{2n-1}$ whose cosets are the other equivalence classes. These equivalence classes always satisfy property (1) for $r = 3$ (but never for $r = 4$). If we now regard the underlying ring $R$ as the ordinary integers, and if $C$ is any equivalence class, then Theorem 1 tells us that

$$\sum_{v\in C}\sigma(v) = \frac{2^{2n-1}}{2^{n^2}}\sum_{k=0}^{n^2} k\binom{n}{k} = n^2\,2^{2n-2},$$

$$\sum_{v\in C}[\sigma(v)]^2 = \frac{2^{2n-1}}{2^{n^2}}\sum_{k=0}^{n^2} k^2\binom{n}{k} = n^2(n^2+1)\,2^{2n-3},$$

$$\sum_{v\in C}[\sigma(v)]^3 = \frac{2^{2n-1}}{2^{n^2}}\sum_{k=0}^{n^2} k^3\binom{n}{k} = n^4(n^2+3)\,2^{2n-4}.$$

## 3. Applications to Group Codes

Let $V$ be an $(n, k)$ group code over the field $GF(q)$, i.e., a $k$-dimensional subspace of the vector space of all $n$-tuples over $GF(q)$. The next theorem then gives the largest value of $r$ for which property (1) is valid.

*Theorem* 2. The set $V$ satisfies property (1) for $r = d - 1$ but not $r = d$, where $d$ is the minimum weight of the dual code.

*Proof.* Let $v$ be a word in the dual code with exactly $d$ nonzero entries. Since $v$ is orthogonal to every word of $V$, this specifies a linear relation which must hold among some $d$ coordinates of the words in $V$. Hence, these $d$ coordinates cannot be chosen arbitrarily, so $r \le d - 1$.

Conversely, assume that property (1) fails for some $r \le d - 1$. Thus, there are some $r$ coordinates whose entries cannot be chosen arbitrarily. If we restrict the vectors in $V$ to these $r$ coordinates, we get a proper subspace of the space of all $r$-tuples over $GF(q)$. The orthogonal complement of this subspace contains more than one vector and hence a vector $v_n$ of positive weight $\le r$. If we now extend $v_0$ to an $n$-tuple by putting 0's in the $n - r$ missing coordinates, we get a word of positive weight $\le r$ orthogonal to $V$, a contradiction. Theorem 2 is proved.

Now assume that $q = 2$, so that $V$ is a binary code. If we regard the 0's and 1's as ordinary integers for the purpose of applying Theorem 1, then $\sigma(v)$ is simply the

weight of the word $v$. Hence, from Theorem 1 and 2 there follows:

*Theorem 3.* If an $(n,k)$ binary code has $a_i$ words of weight $i$ and if $d$ is the minimum weight of the dual code, then

$$\sum_{i=0}^{n} i^t a_i = \frac{1}{2^{n-k}} \sum_{j=0}^{n} j^t \binom{n}{j}, \qquad 0 \leq t \leq d-1.$$

Theorem 3 then gives $d$ linear equations which the $a_i$ satisfy. In Table 3, expressions for the function

$$f(t) = \sum_{j=0}^{n} j^t \binom{n}{j}$$

for $0 \leq t \leq 6$, are given for reference.

**Table 3. Values of $f(t) = \sum_{j=0}^{n} j^t \binom{n}{j}$**

| $t$ | $f(t)$ |
|---|---|
| 0 | $2^n$ |
| 1 | $n2^{n-1}$ |
| 2 | $n(n+1)2^{n-2}$ |
| 3 | $n^2(n+3)2^{n-3}$ |
| 4 | $n(n+1)(n^2+5n-2)2^{n-4}$ |
| 5 | $n^3(n^2+10n^2+15n-10)2^{n-5}$ |
| 6 | $n(n+1)(n^4+14n^3+31n^2-46n+16)2^{n-6}$ |

For practical purposes, it can always be assumed that the minimum weight of the dual of a binary $(n,k)$ code satisfies $d > 2$. For, if $d = 1$, then one coordinate of $V$ is always 0, while if $d = 2$, then $V$ has repeated columns. Since $d > 2$, we can calculate the variance $\mu$ of the weight distribution:

$$\mu = \frac{1}{2^k} \sum_{i=0}^{n} i^2 a_i - \left( \frac{1}{2^k} \sum_{i=0}^{n} i a_i \right)^2$$

$$= \frac{1}{2^n} \sum_{j=0}^{n} j^2 \binom{n}{j} - \left[ \frac{1}{2^n} \sum_{j=0}^{n} j \binom{n}{j} \right]^2$$

$$= \frac{n}{4}.$$

This is necessarily the variance of the binomial distribution on $n$ tries with success probability ½.

*Example.* Using the methods of Solomon and McEliece (*SPS 37-35*, Vol. IV, pp. 340–348), it can be shown that the words of the dual Golay (23, 11) code have weight 0, 8, 12, or 16. And the dual of this code has minimum weight 7, so by Theorem 3,

$$a_8 + a_{12} + a_{16} = 2^{11} - 1$$

$$8a_8 + 12a_{12} + 16a_{16} = 23 \cdot 2^{10}$$

$$64a_8 + 144a_{12} + 256a_{16} = 23 \cdot 24 \cdot 2^8.$$

These equations are easily solved, giving

$$a_8 = 506 = 22 \cdot 23,$$

$$a_{12} = 1288 = 56 \cdot 23,$$

$$a_{16} = 253 = 11 \cdot 23.$$

# D. Coding Theory: Efficient Solutions of Equations for Decoding

*R. McEliece*

## 1. Introduction

In *SPS 37-39*, Vol. IV, pp. 219–226, Berlekamp, Rumsey, and Solomon presented methods of solving certain algebraic equations over finite fields of characteristic 2; such equations turn up in decoding procedures for Bose-Chaudhuri codes. We give here a more general approach to the same problem, and succeed in giving explicit solutions to many equations. These solutions are easily mechanized. In section 3, we indicate how these solutions represent a considerable saving of effort over previous methods. References to the fundamentals of linear algebra and Galois theory can be found in Ref. 6.

## 2. Theoretical Results

Throughout this section, $K$ and $k$ represent fields.

***Theorem 1.*** Suppose $K$ is a normal extension of $k$, and let $\sigma$ be an automorphism of $K/k$. View $K$ as a vector space over $k$ and consider the linear transformations $\rho = \sigma - 1$ and $\tau = 1 + \sigma + \sigma^2 + \cdots + \sigma^{r-1}$, where $r$ is the order of $\sigma$. Then the range of $\rho$ is precisely the null space of $\tau$.

*Proof.* Let $|K:k| = n$, and denote by $R_0$, $R_1$ and $T_0$, $T_1$ the null space and range of $\rho$ and $\tau$, respectively. Now $\rho(x) = 0$, if and only if $\sigma(x) = x$, so that $R_0 = k_\sigma$, the