On a Pair of Dual Subschemes of the Hamming Scheme $H_n(q)$

A. R. Calderbank* and J.-M. Goethals

We consider codes in the Hamming association scheme $H_n(q)$ with interesting metric properties. We describe how a uniformly packed linear code $C$ determines a pair of dual subschemes. The existence of this pair of subschemes is used to establish restrictions on the possible distances between codewords in the dual code $C^\perp$. These restrictions also apply to arbitrary codes with degree $e+1$ and strength $2e$ or $2e+1$. An analogous result gives necessary conditions for the existence of non-linear uniformly packed codes. When $q = 2$ we determine the possible parameters of uniformly packed 2-error-correcting linear codes.

1. Introduction

This paper analyzes codes within the framework of the Hamming association scheme $H_n(q)$. The main theorem is stated below in the language of association schemes.

**Theorem 1.** Let $C$ be a subset of $H_n(q)$ with degree $e+1$ and strength $2e$ or $2e+1$. If $w_1, w_2, \ldots, w_{e+1}$ are the non-zero distances between elements of $C$ then

$$q^{e(e+1)/2} \prod_{i>j} (w_i - w_j) \prod_{k=1}^e (k!)$$

is an integer dividing $|C|^{e+1}$.

When $C$ is a linear code, $w_1, \ldots, w_{e+1}$ are the non-zero weights of codewords in $C$ (the degree being the number of non-zero weights), and the strength of $C$ is one less than the minimum weight in $C^\perp$. Delsarte [3] proved Theorem 1 for two-weight linear codes $C$ by a different argument. The definitions for arbitrary subsets $C$ are given in Section 2 where we also present results established by Delsarte in [4] that are required to prove the main theorem.

When $C$ is a linear code, the hypotheses of Theorem 1 can be reformulated as metric properties of the dual code $C^\perp$. This is described in Section 3. The dual code $C^\perp$ is a uniformly packed $e$-error-correcting code.

Section 4 begins with the proof of Theorem 1. As a corollary we obtain restrictions on the weight distribution of a 3 weight code $C$ with the property that $C^\perp$ is 2-error-correcting. We also prove an analog of Theorem 1 giving necessary conditions for the existence of non-linear uniformly packed codes in the Hamming scheme $H_n(q)$. We conclude by determining the possible parameters of uniformly packed 2-error-correcting binary linear codes.

**Theorem 3.** Let $C^\perp$ be a 2-error-correcting $[n,n-k]$ binary code that is uniformly packed with parameters $\lambda$ and $\mu$. Let $w_1, w_2, \ldots, w_3$ be the non-zero weights in the dual code $C$. Then

\begin{align*}
(1) \quad n &= 2^{2m+1} - 1, \quad k = 4m + 2, \quad \lambda = (2^{2m} - 4)/3, \quad \mu = (2^{2m} - 1)/3, \quad w_1 = 2^{2m} - 2^m, \quad w_2 = 2^{2m}, \quad w_3 = 2^{2m} + 2^m.
\end{align*}

* A. R. Calderbank gave a preliminary report on this work at the special conference on coding theory held at AT&T Bell Laboratories, 17-18 December 1981 to mark the retirement of F. Jessie MacWilliams.
The parameters listed as (1) are those of the binary BCH codes. The [6, 5] zero-sum code has the parameters listed as (2). Codes with the parameters listed as (3) and (4) are obtained by puncturing and twice puncturing the [23, 12, 7] Golay code. The existence of a code with the parameters listed as (5) is an open problem. Goethals and van Tilborg had observed that these parameters were admissible in [6].

2. A Pair of Dual Association Schemes

The proof of the main theorem assumes results established by Delsarte in [4]. In this section we present those results. In particular we describe how a linear code with certain properties determines a pair of dual association schemes.

An association scheme with \( n \) classes on a set \( X \) is a partition of the set of 2-element subsets of \( X \) into \( n \) classes \( \Gamma_1, \Gamma_2, \ldots, \Gamma_n \) satisfying

1. given \( x \in X \) the number \( \nu_i \) of \( y \in X \) with \( \{x, y\} \in \Gamma_i \) depends only on \( i \);
2. given \( x, y \in X \) with \( \{x, y\} \in \Gamma_k \), the number of \( z \in X \) with \( \{x, z\} \in \Gamma_j \) and \( \{y, z\} \in \Gamma_j \) is a constant \( P_{ij}^k \) depending only on \( i, j, \) and \( k \).

The Hamming scheme \( H(n, q) \) is an association scheme with \( n \) classes. Here \( F = GF(q) \), \( X = F^n \) and a pair of vectors \( \{x, y\} \) is in \( \Gamma_j \) if and only if the Hamming distance \( d(x, y) = i \).

Let \( D_0 = I \) and let \( D_i \) be the adjacency matrix of the graph \( (X, \Gamma_i) \). The commuting symmetric matrices \( D_0, D_1, \ldots, D_n \) span an \( n + 1 \) dimensional real algebra called the Bose-Mesner algebra of the scheme. Since the Bose-Mesner algebra is semisimple it admits a unique basis of mutually orthogonal idempotent matrices \( J_0, J_1, \ldots, J_n \). Here \( J_0 = |X|^{-1}J \) where \( J \) is the matrix with every entry 1. Writing \( D_k = \sum_{i=0}^{n} p_k(i)J_i \), for \( k = 0, 1, \ldots, n \), we have \( D_kJ_i = p_k(i)J_i \). Thus \( p_k(i) \) is the eigenvalue of \( D_k \) associated with the eigenspace \( V_i \) spanned by the columns of \( J_i \). The \( (n + 1) \times (n + 1) \) matrix \( P \) with \( ik \)-th entry \( p_k(i) \) is called the eigenmatrix of the scheme. The matrix \( Q = IXP^{-1} \), with \( ik \)-th entry \( q_k(i) \), is called the dual eigenmatrix. For any choice of \( n + 1 \) distinct real numbers \( z_0 = 0, z_1, \ldots, z_n \) we can find polynomials \( \Phi_0, \Phi_1, \ldots, \Phi_n \) each of degree at most \( n \) such that \( \Phi_k(z_j) = p_k(i) \) for \( 0 \leq i, k \leq n \). The association scheme is said to be \( P \)-polynomial if there is a choice of \( z_0 = 0, z_1, \ldots, z_n \) for which \( \Phi_k \) has degree \( k \) for \( 0 \leq k \leq n \). \( Q \)-polynomial schemes are defined similarly with \( Q \) replacing \( P \) in the definition. The Hamming scheme \( H(n, q) \) is both \( P \) and \( Q \)-polynomial with \( z_i = i, i = 0, 1, \ldots, n \) and

\[
p_k(i) = q_k(i) = K_k(i),
\]

where

\[
K_k(z) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{n-z}{k-j}
\]

is the \( k \)-th Krawtchouk polynomial.

Let \( C \) be a subset of the point set \( X \) of a \( Q \)-polynomial scheme. The inner distribution \( a = (a_0, a_1, \ldots, a_n) \) of \( C \) is given by

\[
a_i = |C|^{-1} \sum_{x, y \in C} D_i(x, y),
\]

which is the average valency of \( \Gamma_i |C \). Let \( L = \{i | 1 \leq i \leq n \) and \( a_i \neq 0 \} \). The dual distribution \( b = (b_0, b_1, \ldots, b_n) \) of \( C \) is the vector \( |C|^{-1}aQ \). Delsarte proved that \( b_0 = 1 \) and \( b_i \geq 0 \) for \( 1 \leq i \leq n \). The degree \( s(C) \) of \( C \) is the number of non-zero components of the inner
distribution not counting \( a_0 = 1 \). The subset \( C \) is said to have strength \( t \) if \( b_1 = b_2 = \cdots = b_t = 0 \). The maximum strength \( t(C) \) is the largest \( t \) for which \( C \) has strength \( t \). If \( C \subseteq GF(q)^n \) is a linear code in the Hamming scheme \( H(n, q) \), then \( a_i \) is the number of codewords of weight \( i \) in \( C \) and \( b_i \) is the number of codewords of weight \( i \) in \( C^\perp \). Thus \( s(C) \) is the number of non-zero weights in \( C \) and \( t(C) + 1 \) is the minimum weight in the dual code \( C^\perp \). The following theorem is given as Theorem 5.25 of [4] and as Theorem 3.17 of [5].

**Theorem (Delsarte).** Let \( C \) be a subset of the point set of an association scheme that is Q-polynomial with respect to real numbers \( z_0 = 0, z_1, \ldots, z_n \). Let \( a = (a_0, a_1, \ldots, a_n) \) be the inner distribution of \( C \) and let \( L = \{i | 1 \leq i \leq n \text{ and } a_i \neq 0 \} \). If the degree \( s(C) = s \) and the maximum strength \( t(C) = t \) of \( C \) satisfy \( t \leq 2s - 2 \) then the restriction to \( C \) of the given scheme is an association scheme on \( C \) that is Q-polynomial with respect to \( z_0 = 0 \) and \( \{z_i \mid i \in L \} \).

Delsarte also proved that the dual eigenmatrix \( Q' = [q_k(i)] \) (where \( 0 \leq k \leq s \) and \( i \in \{0\} \cup L \)) of the restricted scheme is related to the dual eigenmatrix \( Q \) of the original scheme by

\[
q'_k(i) = q_k(i), \quad k = 0, 1, \ldots, s - 1, \quad i \in \{0\} \cup L,
\]

\[
q'_i(i) = \begin{cases} |C| - \sum_{k=0}^{s-1} q_k(0) & \text{if } i = 0, \\ - \sum_{k=0}^{s-1} q_k(i) & \text{if } i \in L. \end{cases}
\]

Suppose that \( C \) is a linear code with \( e + 1 \) non-zero weights \( w_1, w_2, \ldots, w_{e+1} \) and that \( C^\perp \) is an \( e \)-error-correcting code. Then \( s(C) = e + 1 \), \( t(C) = 2e \) or \( 2e + 1 \) and the theorem given above implies that we can define an association scheme on \( C \) with \( e + 1 \) classes \( \Gamma_1, \Gamma_2, \ldots, \Gamma_{e+1} \). A pair of codewords \( \{x, y\} \) is in \( \Gamma_i \) if and only if \( d(x, y) = w_i \). This association scheme we call the distance scheme. Now (1) and (3) imply that the dual eigenmatrix \( Q' = [q'_k(w_i)] \) (where \( w_0 = 0 \)) is given by

\[
q'_k(w_i) = K_k(w_i), \quad k = 0, 1, \ldots, e, \quad i = 0, 1, \ldots, e + 1,
\]

\[
q'_{e+1}(w_i) = \begin{cases} |C| - \sum_{k=0}^{e} K_k(0) & \text{if } i = 0, \\ - \sum_{k=0}^{e} K_k(w_i) & \text{if } i = 1, 2, \ldots, e + 1. \end{cases}
\]

Since the distance scheme is invariant under translation by codewords of \( C \) it is possible to define a dual scheme with \( e + 1 \) classes \( \Gamma_1^*, \Gamma_2^*, \ldots, \Gamma_{e+1}^* \) (see Example 3.19 of [5]). The points of this dual scheme are the cosets of \( C^\perp \), represented by their coset leaders. The weight of a coset is the weight of a coset leader. A pair of cosets \( \{x, y\} \) is in \( \Gamma_i^* \) if and only if the coset \( C^\perp + (x - y) \) has weight \( i \). (The covering radius of \( C^\perp \) is bounded above by \( s(C) = e + 1 \).) This association scheme we call the coset scheme. To show that we have really defined an association scheme and that the two schemes are dual in the usual sense ([4, Section 2.6] or [5, Section 2]) we perform a calculation.

Let \( |C| = |F^n / C^\perp| = N \). We order the coset leaders \( v_1, v_2, \ldots, v_N \) of \( C \) and use the ordering to define the adjacency matrix \( A = [a_{ij}] \) of the graph \( (C, \Gamma^*) \). Let \( \chi: F^* \rightarrow C \) be any non-principal character of the additive group \( F^* \). If \( x \in C \) then the map \( \chi_x: y \rightarrow \chi(x \cdot y) \), for all \( y \in F^n \), is a character of the quotient group \( F^n / C^\perp \) and distinct elements \( x \) of \( C \) define distinct characters of \( F^n / C^\perp \). Define a vector \( e_x \in C^N \) by setting

\[
(e_x)_i = \chi_x(v_i), \quad \text{for } i = 1, 2, \ldots, N.
\]
Let \( u_i \in F^n, i = 1, 2, \ldots, n \), denote the vector with a 1 in position \( i \) and zeros elsewhere. If \( x = (x_1, \ldots, x_n) \) is any codeword of \( C \) then \( x \cdot u_i = x_i \), for \( i = 1, 2, \ldots, n \). Now

\[
(e_x A)_j = \sum_{i=1}^{N} \chi_x(u_i) a_{ij} = \sum_{\text{wt}(C^i + u_i - x) = 1} \chi_x(v_i)
\]

\[
= \sum_{\lambda \in GF(q)^*} \sum_{k=1}^{n} \chi_x(v_j + \lambda u_k) = \left( \sum_{\lambda \in GF(q)^*} \sum_{k=1}^{n} \chi(x \cdot \lambda u_k) \right) \chi_x(v_j)
\]

\[
= (n(q-1) - qwt(x))(e_x)_j.
\]

Hence the matrix \( A \) has \( e + 2 \) different eigenvalues and the eigenvectors in each eigenspace correspond to codewords of a given weight as required. Finally we recall that the eigenvalues of the coset scheme are obtained by interchanging the role of the matrices \( P \) and \( Q \) of the distance scheme.

**Example.** Let \( m \geq 2 \) and let \( C \) be the dual of the binary 2-error-correcting BCH code of length \( n = 2^{2m+1} - 1 \) and dimension \( 2^{2m+1} - 4m - 3 \). Kasami [8] proved that \( C \) is a 3 weight code with weights

\[
w_1 = 2^{2m} - 2^m, \quad w_2 = 2^{2m}, \quad \text{and} \quad w_3 = 2^{2m+2}.
\]

The \( Q \) matrix of the distance scheme (\( P \) matrix of the coset scheme) is given below.

\[
Q' = \begin{bmatrix}
1 & 2^{2m+1} - 1 & 2^{4m+1} - 3 \cdot 2^{2m+1} & 2^{4m+1} + 2^{2m+1} - 1 \\
1 & 2^{m+1} - 1 & (2^m - 1)^2 & -(2^{2m+1} + 1) \\
1 & -1 & -(2^{2m+1} - 1) & 2^{2m+1} - 1 \\
1 & -(2^{m+1} + 1) & (2^m + 1)^2 & -(2^{2m+1})
\end{bmatrix}
\]

Since \( K_0(z) = 1 \) all entries in column 1 are 1. By (4) the entries in column 2 are obtained by evaluating \( K_1(z) = n - 2z \) at \( w_0 = 0, w_1, w_2 \) and \( w_3 \). The entries in column 3 are obtained by evaluating \( K_2(z) = \frac{1}{2}(K_1^2(z) - n) \) at \( w_0 = 0, w_1, w_2, \) and \( w_3 \), and the entries in column 4 are obtained via (5). The \( P \) matrix of the distance scheme (\( Q \) matrix of the coset scheme) is given below.

\[
P' = \begin{bmatrix}
1 & 2^{m-1}(2^{3m+1} + 2^{2m+1} - 2^m - 1) & 2^{4m+1} + 2^{2m+1} - 1 & 2^{m-1}(2^{3m+1} - 2^{2m+1} - 2^{m+1} + 1) \\
1 & 2^{m-1}(2^{3m+1} + 2^{2m+1} - 2^m - 1) & -2^{2m+1} - 1 & 2^{m-1}(2^{3m+1} - 2^{2m+1} - 2^{m+1}) \\
1 & -2^{m-1}(2^m - 1) & -2^{2m+1} - 1 & 2^{m-1}(2^{m+1} + 1) \\
1 & -2^{m-1}(2^m + 1) & 2^{2m+1} - 1 & -2^{m-1}(2^{m+1})
\end{bmatrix}
\]

The entries of \( P' \) and \( Q' \) satisfy

\[
\rho_k p'_i(k) = v_i q'_k(i)
\]

where \( \rho_k \) is the dimension of the eigenspace \( V_k \), and \( v_i \) is the number of codewords of weight \( w_i \) (see [5, Corollary 1.2]). Hence the entries \( p'_i(0) \) in the first row of \( P' \) are the number of codewords of \( C \) of weight \( w_i \), \( i = 0, 1, 2, 3 \) and the entries \( q'_i(0) \) in the first row of \( Q' \) are the number of cosets of \( C^\perp \) of weight \( i, i = 0, 1, 2, 3 \).

### 3. Uniformly Packed Codes

In Section 2 we described how a linear code \( C \) satisfying certain conditions determines a pair of dual association schemes. In this section we describe how to reformulate these conditions as metric properties of the dual code \( C^\perp \).
In a perfect $e$-error-correcting code the spheres of radius $e$ about the codewords are disjoint and they cover the whole space. MacWilliams ([11] and [12]) proved that an $e$-error-correcting linear code is perfect if and only if there are exactly $e$ non-zero weights in the dual code. For example, the ternary [11, 6, 5] Golay code is perfect and non-zero codewords in the dual code have weight 6 or 9.

Uniformly packed codes are a generalization of perfect codes and were introduced by Semakov, Zinovjev, and Zaitzev in [13]. In a uniformly packed $e$-error-correcting code the spheres of radius $e+1$ about the codewords cover the whole space and these spheres overlap in a very regular way. There are constants $\lambda$ and $\mu$ (with $\lambda < (n-e)(q-1)/(e+1)$) such that vectors at distance $e$ from the code are in $\lambda+1$ spheres and vectors at distance $e+1$ from the code are in $\mu$ spheres. If the restriction on $\lambda$ were removed, a perfect code would also be uniformly packed. Goethals and van Tilborg [6] proved that an $e$-error-correcting linear code is uniformly packed if and only if there are exactly $e+1$ non-zero weights in the dual code. For example, the binary [24, 12, 8] Golay code is uniformly packed with parameters $\lambda = 0$ and $\mu = 6$. This code is self-dual and non-zero codewords have weight 8, 12, 16 or 24. The 2-error-correcting BCH code of length $n = 2^{2m+1}-1$ ($m \geq 2$) is another example. Gorenstein, Peterson, and Zierler [7] proved that this code is quasi-perfect. Goethals and van Tilborg [6] proved that it is uniformly packed with parameters $\mu = (2^{2m}-1)/3$ and $\lambda = \mu - 1$.

Van Lint and Tietaväinen proved that a non-trivial perfect code over any field $GF(q)$ must have the same parameters as one of the Hamming or Golay codes (see [10] and [14]). Van Tilborg [15] proved that there are no uniformly packed $e$-error-correcting codes for $e \geq 4$ and that the extended binary Golay code is the only binary uniformly packed 3-error-correcting code. For $e = 1$ and 2 examples do exist. For $e = 1$, the known examples are described in [2].

4. Restrictions on Distances Between Codewords

4.1. Codes that determine a subscheme

We have seen that if $C$ is a subset of the Hamming scheme $H_n(q)$, with degree $e+1$, and strength $2e$ or $2e+1$, then the restriction to $C$ of the classes of $H_n(q)$ is an association scheme on $C$ with $e+1$ classes. If $(a_0, \ldots, a_e)$ is the inner distribution of $C$ then $a_0 = 1$, $a_i = 0$ for $i = 1, \ldots, e$ and $a_e = 0$ otherwise. In this section we establish restrictions on the integers $w_1, \ldots, w_{e+1}$ that can occur in this way.

**Theorem 1.** Let $C$ be a subset of $H_n(q)$ with degree $e+1$ and strength $2e$ or $2e+1$. If $w_1, w_2, \ldots, w_{e+1}$ are the non-zero distances between elements of $C$ then

$$ q^{e(e+1)/2} \prod_{i>j} (w_i - w_j) \prod_{k=1}^{e} (k!) $$

is an integer dividing $|C|^{e+1}$.

**Proof.** The polynomial

$$ F(x) = |C| \prod_{i=1}^{e+1} \left( 1 - \frac{x}{w_i} \right) $$

is called the annihilator polynomial of $C$. We have $F(0) = |C|$ and $F(w_i) = 0$ for $i = 1, 2, \ldots, e+1$. By (1), (2), and (3) the Q matrix of the restricted scheme is an integral
matrix of the following form.

\[
Q' = \begin{bmatrix}
1 & K_1(0) & \ldots & K_e(0) \\
1 & K_1(w_1) & \ldots & K_e(w_1) \\
\vdots & \vdots & \ddots & \vdots \\
1 & K_1(w_{e+1}) & \ldots & K_e(w_{e+1})
\end{bmatrix}
\left[
F(0) - \sum_{k=0}^{e} K_k(0) \\
F(w_1) - \sum_{k=0}^{e} K_k(w_1) \\
\vdots \\
F(w_{e+1}) - \sum_{k=0}^{e} K_k(w_{e+1})
\right]
\]

For \( k \geq 1 \), the Krawtchouk polynomial \( K_k(x) \) can be written as a polynomial in \( K_1(x) \) with leading coefficient

\[
\frac{(-q)^k}{k!} = \frac{1}{k!}
\]

Hence there is a lower triangular matrix \( T \) with diagonal entries \( T_{00} = 1, T_{kk} = 1/k! \) for \( 1 \leq k \leq e \), and

\[
T_{(e+1)(e+1)} = \frac{(-1)^{e+1}|C|}{(-q)^{e+1}} \left( \prod_{k=1}^{e+1} w_k \right) = \frac{|C|}{q^{e+1} \left( \prod_{k=1}^{e+1} w_k \right)}
\]

such that

\[
Q' = \begin{bmatrix}
1 & K_1(0) & \ldots & K_e^{e+1}(0) \\
1 & K_1(w_1) & \ldots & K_e^{e+1}(w_1) \\
\vdots & \vdots & \ddots & \vdots \\
1 & K_1(w_{e+1}) & \ldots & K_e^{e+1}(w_{e+1})
\end{bmatrix}
\begin{bmatrix}
K_1(0) & K_1(0) & \ldots & K_e(0) \\
K_1(w_1) & K_1(w_1) & \ldots & K_e(w_1) \\
\vdots & \vdots & \ddots & \vdots \\
K_1(w_{e+1}) & K_1(w_{e+1}) & \ldots & K_e(w_{e+1})
\end{bmatrix}
\]

If \( P' \) is the \( P \) matrix of the restricted scheme then \( Q'P' = |C|I \) so the entries of \( P' \) are rational. But the entries of \( P' \) are algebraic numbers since they are eigenvalues of \((0, 1)\) adjacency matrices. Hence \( P' \) is an integral matrix and \( \det Q' \) is an integer dividing \( |C|^{e+2} \). Since \( QT^{-1} \) is a Vandermonde matrix,

\[
\det Q' = q^{e+1} \left( \prod_{k=1}^{e+1} w_k \right) q^{e(e+1)/2} \left( \prod_{i>j} (w_i - w_j) \right) \det T
\]

that is

\[
\det Q' = \frac{q^{e(e+1)/2} \prod_{i>j} (w_i - w_j)}{\prod_{k=1}^{e} (k!)} \cdot \frac{1}{|C|}.
\]

This finishes the proof.

EXAMPLE 1. Here \( C \) is the dual of the binary 2-error-correcting BCH code of length \( n = 2^{2m+1} - 1 \) \( (m \geq 2) \) and dimension \( 2^{2m+1} - 4m - 3 \). Then \( |C| = 2^{4m+3} \) and \( C \) has 3 non-zero weights

\[ w_1 = 2^{2m} - 2^m, \quad w_2 = 2^m, \quad \text{and} \quad w_3 = 2^{2m} + 2^m. \]

We have

\[
\frac{q^{e(e+1)/2} \prod_{i>j} (w_i - w_j)}{\prod_{k=1}^{e} (k!)} = 2^{2m} \cdot 2^m \cdot (2 \cdot 2^m) = 2^{3m+3}.
\]
EXAMPLE 2. Here $C$ is a Kerdock code in $H(2^m - 1, 2)$ where $m \geq 4$ is even. $C$ is a non-linear code, $|C| = 2^{2m-1}$, and the possible distances between distinct codewords are

$$w_1 = 2^{m-1} - 2^{(m-2)/2}, \quad w_2 = 2^{m-1}, \quad \text{and} \quad w_3 = 2^{m-1} + 2^{(m-2)/2}.$$ 

We have

$$q^{e(e+1)/2} \prod_{i>j} (w_i - w_j) = 2^{3 \cdot 2^{(m-2)/2} \cdot 2^{(m-2)/2} \cdot (2 \cdot 2^{(m-2)/2})} \cdot 2^{2m-1} \cdot \prod_{k=1}^{e} (k!)$$

$$= 2^{7m/2 - 1}.$$

The $P$ and $Q$ matrices of the restricted scheme are given by Delsarte in [4, Section 5.3.3]. We specialize Theorem 1 to give results about linear codes that are the duals of 1- and 2-error-correcting uniformly packed codes.

COROLLARY 1 (Delsarte). Let $q = p^m$ where $p$ is prime. Let $C$ be an $[n, k]$ code over $GF(q)$ with exactly 2 non-zero weights $w_1, w_2$, and with the property that the minimum weight in the dual code $C^\perp$ is 3 or 4. Then there are integers $a$ and $t$ such that

$$w_1 = ap^t \quad \text{and} \quad w_2 = (a+1)p^t.$$

PROOF. Theorem 1 implies that $w_2 - w_1 = p^t$ for some integer $t$. The $Q$ matrix of the restricted scheme is

$$Q' = \begin{bmatrix} 1 & n(q-1) & q^k - n(q-1) - 1 \\ 1 & n(q-1) - qw_1 & -n(q-1) + qw_1 - 1 \\ 1 & n(q-1) - qw_2 & -n(q-1) + qw_2 - 1 \end{bmatrix}$$

The $P$ matrix of the restricted scheme is given by $P' = qk Q'^{-1}$, and

$$P_{33}' = \frac{q^kqw_1}{\det Q'} = \frac{-w_1}{ap^t q^k} = \frac{-w_1}{p^t}.$$ 

Now $P_{33}'$ is an integer and so the result follows.

REMARKS. The code $C$ is the dual of a single-error-correcting uniformly packed code. Corollary 1 is due to Delsarte and is given as Theorem 2.1 of [3]. It is the starting point for the characterization of uniformly packed $[n, k, 4]$ codes obtained by Calderbank in [1].

COROLLARY 2. Let $q = p^m$ where $p$ is prime. Let $C$ be an $[n, k]$ code over $GF(q)$ with exactly 3 non-zero weights $w_1 < w_2 < w_3$, and with the property that the minimum weight in the dual code $C^\perp$ is 5 or 6. Then there is an integer $t$ such that either

1. $w_3 - w_2 = w_2 - w_1 = p^t$,

2. $p = 3$, $w_3 - w_2 = 2.3$, and $w_2 - w_1 = 3'$, or

3. $p = 3$, $w_3 - w_2 = 3'$, and $w_2 - w_1 = 2.3'$.

PROOF. By Theorem 1, $(w_2 - w_1)(w_3 - w_2)(w_3 - w_1)/2$ is a power of $p$ and the result follows.

COROLLARY 3. Let $q = p^m$ where $p$ is prime. Let $C$ be an $[n, k]$ code over $GF(q)$ with exactly 3 non-zero weights $w_1, w_2, w_3$ satisfying $w_3 - w_2 = w_2 - w_1 = p^t$, and with the property
that the minimum weight in the dual code $C^\perp$ is 5 or 6. Then there is an integer $a$ such that

$$w_1 = (a-1)p', \quad w_2 = ap', \quad \text{and} \quad w_3 = (a+1)p'.$$

**Proof.** The $Q$ matrix of the restricted scheme is

$$Q' = \begin{bmatrix}
1 & K_1(0) & K_2(0) & (q^k - K_2(0) - K_1(0) - 1) \\
1 & K_1(w_1) & K_2(w_1) & (-K_2(w_1) - K_1(w_1) - 1) \\
1 & K_1(w_2) & K_2(w_2) & (-K_2(w_2) - K_1(w_2) - 1) \\
1 & K_1(w_3) & K_2(w_3) & (-K_2(w_3) - K_1(w_3) - 1)
\end{bmatrix}$$

Now

$$K_2(x) = \frac{1}{2}(K_1^2(x) - (q-2)K_1(x) - n(q-1))$$

and by hypothesis

$$K_1(w_1) = K_1(w_2) + qp'$$

and

$$K_1(w_3) = K_1(w_2) - qp'.$$

The $P$ matrix of the restricted scheme is integral and is given by $P' = q^kQ'^{-1}$. A straightforward calculation shows that

$$P'_{43} = \frac{-p'q(p^{2q-2}q^2 - q^2w_2^2) \cdot q^k}{\det Q'}$$

Since

$$\det Q' = q^3p^3q^k$$

we have proved that $p'$ divides $w_2$ and the result follows.

**Remarks.** If $p = 3$, $w_3 - w_2 = 2.3'$, and $w_2 - w_1 = 3'$ (case (2) of Corollary 2) then a similar analysis of the $P$ and $Q$ matrices of the restricted scheme shows that

$$w_1 = a3', \quad w_2 = (a+1)3', \quad \text{and} \quad w_3 = (a+3)3'$$

where $a \not\equiv 1 \pmod{3}$. If $p = 3$, $w_3 - w_2 = 3'$, and $w_2 - w_1 = 2.3'$ (case (3) of Corollary 2) then

$$w_1 = a3', \quad w_2 = (a+2)3', \quad \text{and} \quad w_3 = (a+3)3'$$

where $a \not\equiv 2 \pmod{3}$. We have been unable to eliminate these possibilities.

4.2. Non-Linear Uniformly Packed Codes

Now we prove an analog of Theorem 1 for non-linear uniformly packed codes in the Hamming scheme $H_n(q)$. Let $C$ be an $e$-error-correcting code that is uniformly packed with parameters $\lambda$ and $\mu$. Let $b = (b_0, b_1, \ldots, b_n)$ be the dual distribution of $C$ and let $\Delta$ be the diagonal matrix $\Delta = \text{diag} \{b_0, b_1, \ldots, b_n\}$. For any $x \in F^n$ let $b_i(x)$ denote the number of elements of $C$ at distance $i$ from $x$, and let $B_i$ denote the column vector with entries indexed by the vectors in $F^n$ and with $x$-entry equal to $b_i(x)$. The outer distribution (or distribution matrix) of $C$ is the matrix $B = (B_0, B_1, \ldots, B_n)$. The following identity is given as Lemma 3.2 of [5].

$$q^n B^T B = |C|^2 P^T \Delta P,$$  \hspace{1cm} (9)
where $P = [K_k(i)]$ is the eigenmatrix of the Hamming scheme $H_n(q)$. Let $L = \{k| 1 \leq k \leq n$ and $b_k \neq 0\}$. then the polynomial

$$F(x) = \frac{q^n}{|C|} \prod_{k \in L} \left(1 - \frac{x}{k}\right)$$

is called the characteristic polynomial of $C$ (If $C$ is linear then $F(x)$ is also the annihilator polynomial of $C^\perp$). Goethals and van Tilborg ([6], Theorem 12) proved that $F(x)$ can be rewritten as

$$F(x) = K_0(x) + K_1(x) + \cdots + K_e(x) + \frac{1}{\mu} (K_{e+1}(x) - \lambda K_e(x)).$$

Thus $|L| = e + 1$ and we write $L = \{w_1, w_2, \ldots, w_{e+1}\}$. Let $K = \{0, 1, \ldots, e + 1\}$, and let $\tilde{P}$, $\tilde{\Delta}$ denote the restriction of $P$, $\Delta$ to the sets $L \cup \{0\} \times K$ and $L \cup \{0\} \times L \cup \{0\}$ respectively. If $\tilde{B} = (B_0, B_1, \ldots, B_{e+1})$ then by (9) we have

$$q^n \tilde{B}^T \tilde{B} = |C|^2 \tilde{P}^T \tilde{\Delta} \tilde{P}. \quad (10)$$

Let

$$Q' = \begin{bmatrix}
1 & K_1(0) & \cdots & K_e(0) & (1/\mu)(K_{e+1}(0) - \lambda K_e(0)) \\
1 & K_1(w_1) & \cdots & K_e(w_1) & (1/\mu)(K_{e+1}(w_1) - \lambda K_e(w_1)) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & K_1(w_{e+1}) & \cdots & K_e(w_{e+1}) & (1/\mu)(K_{e+1}(w_{e+1}) - \lambda K_e(w_{e+1}))
\end{bmatrix}$$

Note that $(1/\mu)(K_{e+1}(x) - \lambda K_e(x)) = F(x) - \sum_{k=1}^e K_k(x)$.

**THEOREM 2.** Let $D = \text{diag} [K_0(0), K_1(0), \ldots, K_e(0), (1/\mu)(K_{e+1}(0) - \lambda K_e(0))]$. Then

$$Q'^T(\text{adj} D)Q' = q^n D, \quad \text{and} \quad \det Q' = \frac{q^n q^{(e+1)/2} \prod_{i<j} (w_i - w_j)}{|C| \prod_{k=1}^e (k!)}. \quad (11)$$

**PROOF.** The matrices $Q'$ and $\tilde{P}$ are related by

\[
\begin{array}{ccc|ccc}
1 & 0 & 0 & 0 & 0 & -\lambda \\
0 & 1 & 0 & \frac{1}{\mu} \frac{1}{\mu} & 1 & \frac{1}{\mu} \\
0 & 1 & 0 & 0 & 1 & 0
\end{array}
\]
It follows from (10) that

\[
Q^T \left( C | \bar{D} \right) Q' = \frac{q^n}{|C|}
\]

\[
\begin{array}{ccc}
1 & 0 & 0 \\
0 & 1 & \frac{-\lambda}{\mu} \\
0 & \frac{1}{\mu} & 1
\end{array}
\]

\[
\begin{array}{ccc}
1 & 0 & 0 \\
1 & 0 & \frac{-\lambda}{\mu} \\
0 & \frac{1}{\mu} & 1
\end{array}
\]

Now

\[
(\bar{B}^T \bar{B})_{ij} = \begin{cases} 
1 & \text{for some } c \in C \text{ and } \ d(x, c) = j, \text{ for some } c' \in C \\
0 & \text{otherwise}
\end{cases}
\]

Since \( C \) has minimum distance at least \( 2e + 1 \) we have

\[
(\bar{B}^T \bar{B})_{ij} = 0 \quad \text{if } i \neq j \quad \text{and} \quad i + j < 2e + 1,
\]

Thus

\[
Q^T = \left( \left| C | \bar{D} \right) Q' = q^n
\]

\[
\begin{array}{c}
1 \\
K_1(0) \\
0 \\
K_{e+1}(0) \\
0 \\
K_e(0)
\end{array}
\]

\[
\begin{array}{c}
0 \\
\gamma \\
\delta
\end{array}
\]

where

\[
|C| \beta = |C| \gamma = \frac{-\lambda}{\mu} (\bar{B}^T \bar{B})_{e,e} + \frac{1}{\mu} (\bar{B}^T \bar{B})_{e+1,e+1},
\]

and

\[
|C| \delta = \frac{1}{\mu} \left( \frac{-\lambda}{\mu} (\bar{B}^T \bar{B})_{e,e+1} + \frac{1}{\mu} (\bar{B}^T \bar{B})_{e+1,e+1} \right)
\]

Consider spheres of radius \( e + 1 \) about the codewords of \( C \). A vector at distance \( e \) from \( C \) is in \( \lambda + 1 \) spheres and so it is at distance \( e + 1 \) from \( \lambda \) codewords of \( C \). Hence \( \beta = \gamma = 0 \). Vectors at distance \( e + 1 \) from \( C \) are in \( \mu \) spheres so

\[
|C| \delta = \frac{1}{\mu} \left( \frac{-\lambda}{\mu} (\bar{B}^T \bar{B})_{e,e+1} + \frac{1}{\mu} (\bar{B}^T \bar{B})_{e+1,e+1} \right)
\]

and \( \delta = (1/\mu)(K_{e+1}(0) - \lambda K_e(0)) \).
Part 2 is proved in the same way as Theorem 1. There is a lower triangular matrix $T$ with diagonal entries $T_{00} = 1$, $T_{kk} = 1/k!$ for $1 \leq k \leq e$ and

$$T_{(e+1)(e+1)} = \frac{(-1)^{e+1}(q^n/|C|)}{(-q)^{e+1} \prod_{k=1}^{e+1} w_k},$$

such that

$$Q' = \begin{bmatrix} 1 & K_1(0) & K_2^*(0) & \ldots & K_{e+1}^*(0) \\ 1 & K_1(w_1) & K_2^*(w_1) & \ldots & K_{e+1}^*(w_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & K_{e+1}(w_{e+1}) & K_2^*(w_{e+1}) & \ldots & K_{e+1}^*(w_{e+1}) \end{bmatrix} \begin{bmatrix} T \end{bmatrix}.$$

Taking determinants gives part 2.

**Example.** Here $q = 2$, $n = 11$, $e = 2$, $|C| = 24$, $\lambda = 2$ and $\mu = 3$. This code was constructed from the rows of a $12 \times 12$ Hadamard matrix by van Lint in [9].

The non-zero components of the inner distribution are $a_0 = a = 1$, $a_5 = a_6 = 11$, and the non-zero components of the dual distribution are $b_0 = 1$, $b_4 = \frac{10}{3}$, $b_5 = \frac{88}{3}$, $b_8 = \frac{55}{3}$. We have

$$Q' = \begin{bmatrix} 1 & 11 & 55 & 55/3 \\ 1 & 3 & -1 & -3 \\ 1 & -1 & -5 & 5 \\ 1 & -5 & 7 & -3 \end{bmatrix}$$

and

$$Q'^T(\lambda |C| \Delta) Q' = 2^{11} \text{ diag } [1, 11, 55, 55/3].$$

In this example $w_1 = 4$, $w_2 = 6$, $w_3 = 8$ and $w_j - w_i$ is always a power of 2.

### 4.3. Conditions for the existence of uniformly packed 2-error-correcting linear codes

Corollary 3 gives necessary conditions for the existence of 2-error-correcting linear codes that are uniformly packed with parameters $\lambda$ and $\mu$. We conclude this section by deriving further conditions. We assume that $w_3 - w_2 = w_2 - w_1 = p'$.

The annihilator polynomial of $C$ is

$$F(x) = |C| \prod_{i=1}^{3} \left(1 - \frac{x}{w_i}\right). \quad (12)$$

The dual code $C^\perp$ is a 2-error-correcting code that is uniformly packed with parameters $\lambda$ and $\mu$. Goethals and van Tilborg ([6], Theorem 12) have shown that $F(x)$ can be rewritten as

$$F(x) = 1 + K_1(x) + K_2(x) + \frac{1}{\mu} (K_3(x) - \lambda K_2(x)). \quad (13)$$

Now

$$K_2(x) = \frac{1}{2}(K_1^2(x) - (q-2)K_1(x) - n(q-1))$$

and

$$K_3(x) = \frac{1}{2}(K_1^2(x) - 3(q-2)K_1(x) - (3n(q-1) - 2q^2 + 6q - 6)K_1(x) + 2(q-2)(q-1)n).$$
Since \( F(w_i) = 0 \), for \( i = 1, 2, 3 \), and since \( 6\mu F(x) \) is a monic polynomial in \( K_1(x) \), we may write

\[
F(x) = \frac{1}{6\mu} \prod_{i=1}^{3} (K_1(x) - K_1(w_i)).
\]  

Observe that evaluating \( F(0) \) using (12) and (14) gives

\[
\mu = \frac{q^3 w_1 w_2 w_3}{6|C|}. \tag{15}
\]

The coefficient of \( K_1^2(x) \) in \( 6\mu F(x) \) is seen to be

\[
- \sum_{i=1}^{3} K_1(w_i) = -3(\lambda - \mu + (q-2)) \tag{16}
\]

by comparing (13) and (14). Since \( w_3 = w_2 + p' \) and \( w_1 = w_2 - p' \) we conclude from (15) that

\[
n(q-1) - qw_2 = \lambda - \mu + (q-2). \tag{17}
\]

In the special case \( q = 2 \) we are able to determine the possible parameters.

**Theorem 3.** Let \( C^\perp \) be a 2-error-correcting \([n, n-k]\) binary code that is uniformly packed with parameters \( \lambda \) and \( \mu \). Let \( w_1, w_2, \) and \( w_3 \) be the non-zero weights in the dual code \( C \). Then

1. \( n = 2^{2m+1} - 1, \ k = 4m + 2, \ \lambda = (2^m - 4)/3, \ \mu = (2^m - 1)/3, \ w_1 = 2^{2m} - 2^m, \ w_2 = 2^{2m}, \ w_3 = 2^{2m} + 2^m, \)
2. \( n = 6, \ k = 5, \ \lambda = 0, \ \mu = 2, \ w_1 = 2, \ w_2 = 4, \ w_3 = 6, \)
3. \( n = 21, \ k = 9, \ \lambda = 1, \ \mu = 4, \ w_1 = 8, \ w_2 = 12, \ w_3 = 16, \)
4. \( n = 22, \ k = 10, \ \lambda = 0, \ \mu = 2, \ w_1 = 8, \ w_2 = 12, \ w_3 = 16, \) or
5. \( n = 70, \ k = 12, \ \lambda = 16, \ \mu = 10, \ w_1 = 24, \ w_2 = 32, \ w_3 = 40. \)

**Proof.** By Corollary 3 the weights \( w_1, w_2, w_3 \) are of the form \( w_1 = (a-1)2^i, \ w_2 = a2^i, \ w_3 = (a+1)2^i. \) Equation (15) becomes

\[
6\mu = \frac{a(a-1)(a+1)2^{3i+3}}{2^k} \tag{18}
\]

and (17) becomes

\[
\lambda - \mu = n - a2^{i+1}. \tag{19}
\]

Since

\[
K_1(w_2) = \lambda - \mu, \ K_1(w_1) = \lambda - \mu + 2^{i+1}, \quad \text{and} \quad K_1(w_3) = \lambda - \mu - 2^{i+1},
\]

it follows from (14) that

\[
6\mu F(x) = [K_1(x) - (\lambda - \mu)] [K_1^2(x) - 2(\lambda - \mu)K_1(x) + (\lambda - \mu)^2 - 2^{2i+2}]. \tag{20}
\]

However (13) gives

\[
6\mu F(x) = K_1^3(x) - 3(\lambda - \mu)K_1^2(x) + (6\mu - 3n + 2)K_1(x) + (6\mu + 3(\lambda - \mu)n). \tag{21}
\]

Equating coefficients in (20) and (21) gives

\[
6\mu - 3n + 2 = 3(\lambda - \mu)^2 - 2^{2i+2} \tag{22}
\]

and

\[
6\mu + 3(\lambda - \mu)n = (\lambda - \mu)(2^{2i+2} - (\lambda - \mu)^2) \tag{23}
\]
Eliminating $n$ from (22) and (23) gives
\[(\lambda - \mu + 1)((\lambda - \mu)^2 - (\lambda - \mu) - 3\mu) = 0\] (24)

Eliminating $6\mu$ from (22) and (23) gives
\[(\lambda - \mu + 1)((\lambda - \mu + 1)^2 + 3(n - 1) - 2^{2t+2}) = 0\] (25)

The codes with $\lambda - \mu + 1 = 0$ have been classified by Goethals and van Tilborg ([6], appendix B). The only linear codes that occur have the same parameters as a 2-error-correcting BCH code. This is case (1) of the theorem.

We may now suppose $\lambda - \mu + 1 \neq 0$. In this case (24) and (25) imply
\[(\lambda - \mu + 1)^2 = 3\lambda + 1,\] (26)
and
\[3n = 2^{2t+2} + 2 - 3\lambda.\] (27)

Now (19) and (26) imply
\[(n - a2^{t+1} + 1)^2 = 3\lambda + 1,\]
and substituting for $\lambda$ in (27) gives
\[n = \frac{a2^{t+2} - 5 \pm [2^{2t+4} - 6a2^{t+2} + 33]^{1/2}}{2}.\] (28)

If $t = 1$ then the discriminant $\Delta^2$ in (28) is $\Delta^2 = 16(4 - 3a) + 33$, and so $a = 2$. Now (28) implies $n = 5$ or $n = 6$. Since $w_3 = (a + 1)2^t = 6$ we must have $n = 6$, and the other parameters are listed in case (2) of the theorem.

If $t = 2$ then the discriminant $\Delta^2$ in (28) is $\Delta^2 = 32(8 - 3a) + 33$, and so $a = 3$. Now (28) implies $n = 21$ or $n = 22$ and the other parameters are listed in cases (3) and (4) of the theorem.

If $t = 3$ then the discriminant $\Delta^2$ in (28) is $\Delta^2 = 32(32 - 6a) + 33$, and so $a = 4$. Now (28) implies $n = 70$ or $n = 53$. If $n = 53$ then (19) implies $\lambda - \mu = -11$, and (26) implies $\lambda = 33$, so that $\mu = 44$. However (18) implies $5\mu$ and so $n \neq 53$. If $n = 70$, then (19) implies $\lambda - \mu = 6$, and (26) implies $\lambda = 16$, so that $\mu = 10$. This is case (5) of the theorem.

We may now suppose $t > 3$. Recall from the definition of a uniformly packed code that $\lambda < (n - 2)/3$. Now (27) implies $n > 2^{2t+1} + 1$. Since at least one of $n - 2w_1$, $n - 2w_2$, $n - 2w_3$ is negative we have $2(a + 1)2^t > 2^{2t+1} + 1$, and so $a \geq 2^{t+1}$. If $a = 2^{t+1}$ then the discriminant $\Delta^2$ in (28) is $\Delta^2 = 2^{2t+2} + 33$. But this is not a square since $t \neq 1$ or 3. Since the discriminant in (28) is non-negative we must have $3a < 2^{2t+1}$ and so
\[2^{t-1} < a < \frac{2^{t+1}}{3}.\] (29)

By (19) and (27)
\[3n = 2^{2t+2} + 2 - 3\mu - 3n + 3a2^{t+1},\]
and so by (18)
\[3n = 2^{2t+1} + 1 + 3a2^t - \frac{2a(a^2 - 1)}{2^{k-3t}}.\] (30)

We split the analysis into $3$ parts.

**Part 1.** $a$ is even.

Then $f = a2^{2t-k+1}$ is an integer and (30) becomes
\[3n = 2^{2t+1} + 1 + 3a2^t - f(a^2 - 1).\]
Since \( n > 2^{2t} + 1 \), it follows that

\[
2^{2t} + 2 < 3a2^{t} - f(a^2 - 1).
\]

Let \( f = f_12^g \) where \( f_1 \) is odd, and write \( a = f_12^m \). It follows from (29) that \( f_1 \neq 1, 3 \). But if \( f_1 \geq 5 \) then since \( a > 2^{t-1} \) we have

\[
3a2^t - f(a^2 - 1) < 3.2^{2t-1} - 5(2^{2t+2} - 1) = 2^{2t+2} + 5
\]

which contradicts (31).

**Part 2.** \( a \equiv 1 \pmod{4} \)

Then \( f = (a-1)2^{3r+2-k} \) is an integer. Since \( n > 2^{2t} + 1 \), it follows from (30) that

\[
2^{2t} + 2 < 3a2^{t} - \frac{fa(a+1)}{2}.
\]

Let \( f = f_1 2^g \) where \( f_1 \) is odd, and write \( a = f_12^m \). If \( f_1 = 1 \) then (29) implies \( a = 2^{t-1} + 1 \). The discriminant \( \Delta^2 \) in (28) is \( \Delta^2 = 2^{2t+2} - 12.2^{t+1} + 33 \), and since \( (2^{t+1} - 7)^2 < \Delta^2 < (2^{t+1} - 6)^2 \) it is not a square. Therefore \( f_1 \neq 1 \) and it follows from (29) that \( f_1 \neq 3 \). But if \( f_1 \geq 5 \) then since \( a > 2^{t-1} \) we have

\[
3a2^t - \frac{fa(a+1)}{2} < 2^{t-1}\left(3.2^t - \frac{52^{t-1}}{2}\right) = 7.2^{2t-3}
\]

which contradicts (32).

**Part 3.** \( a \equiv -1 \pmod{4} \)

Then \( f = (a+1)2^{3r+2-k} \) is an integer. Since \( n > 2^{2t} + 1 \), it follows from (30) that

\[
2^{2t} + 2 < 3a2^{t} - \frac{fa(a-1)}{2}.
\]

Let \( f = f_1 2^g \) where \( f_1 \) is odd, and write \( a = f_12^m \). It follows from (29) that \( f_1 \neq 1, 3 \), and if \( f_1 \geq 5 \) then since \( a > 2^{t-1} \) we have

\[
3a2^t - \frac{fa(a-1)}{2} < 2^{t-1}\left(3.2^t - \frac{52^{t-1}}{2}\right) = 2^{2t-3}
\]

which contradicts (33).

This finishes the proof.

**References**

1. A. R. Calderbank, On uniformly packed \([n, n-k, 4]\) codes over \( GF(q) \) and a class of caps in \( PG(k-1, q) \), *J. London Math. Soc.* (2), 26 (1982), 365-384.
On dual subschemes of the Hamming scheme $H_n(q)$


Received 15 December 1983 and in revised form 27 July 1984

A. R. CALDERBANK
AT&T Bell Laboratories, Murray Hill, NJ 07974, U.S.A.

and

J.-M. GOETHALS
Philips Research Laboratories, Avenue van Becelaere,
2B-1170 Brussels, Belgium