THREE-WEIGHT CODES AND ASSOCIATION SCHEMES

by A. R. CALDERBANK*) and J.-M. GOETHALS**) 

*) AT&T Bell Laboratories, Murray Hill, New Jersey, USA 
**) Philips Research Laboratory, B-1170 Brussels, Belgium

Abstract

Three-weight projective codes C are considered for which the restriction to C of the Hamming association scheme \(H_n(q)\) is an association scheme with three classes. Sufficient conditions are established and restrictions on the three weights of C are obtained.

It is shown in the binary case that the three-weight subcodes of the shortened second-order Reed-Muller codes provide a large class of examples. Previously known examples were the duals of perfect 3-error-correcting or uniformly packed 2-error-correcting codes.

Math. Rev.: 94B25, 05B30

1. Introduction

Codes C with few distances having the property that the restriction to C of the Hamming association scheme is itself an association scheme were studied by Delsarte\(^1\)), who for linear codes obtained a necessary and sufficient condition: if C is a code with s weights, then the restriction to C of the Hamming scheme is an association scheme with s classes if and only if, among the cosets of its dual code \(C^\perp\), exactly \(s + 1\) distinct weight distributions occur. Previously known examples were obtained from the observation made by Delsarte\(^1\)) that if the minimum distance \(d\) of \(C^\perp\) satisfies \(d \geq 2s - 1\), then the weight distribution of any coset of \(C^\perp\) is uniquely determined by its minimum weight. It was shown by Goethals and van Tilborg\(^2\)) that this situation occurs if and only if \(C^\perp\) is a uniformly packed quasi perfect code.

In this paper, we investigate further the implications of Delsarte’s condition in the case of three-weight codes. We obtain, in particular, a new sufficient condition which applies also when \(d < 5\). Along the way we also obtain restrictions on the weights of C by a method similar to the one used by Calderbank and Goethals\(^3\)) for the case when \(d \geq 2s - 1\). We also find a large class of examples satisfying our new condition in the binary case.

The paper is organized as follows. In sec. 2, we examine the conditions for a three-weight projective code to yield a 3-class association scheme and obtain
in theorem 2.2 a new sufficient condition. In sec. 3, we obtain a large class of examples by showing that all three-weight cyclic subcodes of the shortened second-order Reed-Muller codes satisfy our new condition. Finally, in sec. 4, we analyze in more detail the parameters of the association schemes thus obtained.

Our study of three-weight cyclic codes was motivated by the fact that these codes provide periodic sequences with good crosscorrelation properties, as it was shown by Sarwate and Pursley.

2. Three-weight projective codes and association schemes

Let $C$ be a three-weight projective code of length $n$ and dimension $k$ over the finite field $\mathbb{F}_q$. Thus we assume:

(i) only three distinct nonzero distances occur among codewords of $C$;
(ii) the dual code $C^\perp$ has minimum distance at least equal to 3.

The distribution matrix of $C^\perp$ has as its set of rows the weight distributions of all of the cosets of $C^\perp$. Delsarte (cf. theorem 6.10, p. 91) proved that the distance relations in an $s$-weight linear code $C$ define an association scheme $A$ with $s$ classes on $C$ if and only if the distribution matrix of the dual code $C^\perp$ contains $s + 1$ distinct rows. In this case the set of cosets of $C^\perp$ can be partitioned into $s + 1$ disjoint subsets, each characterized by a given weight distribution, which we denote by $S_0 = \{C^\perp\}, S_1, S_2, \ldots, S_s$. The $s + 1$ relations $R_0, R_1, \ldots, R_s$, defined by

$$(C^\perp + x, C^\perp + y) \in R_i \iff C^\perp + (x + y) \in S_i,$$

then yield an $s$-class association scheme $B$ which is dual to $A$ (cf. Delsarte, Goethals, and Calderbank and Goethals).

It is our purpose to study the classes of three-weight projective codes which yield a pair of dual association schemes as above. From the abovementioned result of Delsarte, it is sufficient to examine which of these codes have the property that among the cosets of their duals only four distinct weight distributions occur.

Since only three weights occur in $C$, the covering radius of $C^\perp$ is at most equal to 3 (cf. Delsarte). Thus the minimum weight of any coset of $C^\perp$ can only be one of the following values: 0, 1, 2 or 3. If we assume that all four values, and only four distinct weight distributions, occur among the cosets of $C^\perp$, we have to conclude that the weight distribution of any coset is uniquely determined by its minimum weight. Although it is in principle possible to think of other possibilities, we shall restrict our attention to this case.

We know already from a result of Delsarte (cf. MacWilliams and Sloane, theorem 20, p. 169) that the weight distribution $A_0(x), A_1(x), \ldots, A_n(x)$ of
any coset $C^\perp + x$ is uniquely determined by the first three values $A_0(x)$, $A_1(x)$ and $A_2(x)$, where $A_i(x)$ denotes the number of codewords of $C^\perp$ at distance $i$ from $x$. To be more precise we restate here Delsarte’s result in the form of a lemma adapted to our case.

**Lemma 2.1 (Delsarte)**

Let the Krawtchouk expansion *) of the polynomial

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

be given by

$$F(z) = \sum_{i=0}^{3} \alpha_i K_i(z),$$

where $w_1$, $w_2$, $w_3$ are the three weights occurring in $C$. Moreover, for $k = 1, 2, \ldots, n - 3$, let the Krawtchouk expansion of $z^k F(z)$ be given by

$$z^k F(z) = \sum_{i=0}^{k+3} \beta_i K_i(z).$$

Then, for any coset $C^\perp + x$, the coefficients $A_i(x)$ of its weight enumerator are related by

$$\sum_{i=0}^{3} \alpha_i A_i(x) = 1,$$

$$\sum_{i=0}^{k+3} \beta_i A_i(x) = 0.$$  \hspace{1cm} (2) \hspace{1cm} (3)

The relations (2) and (3), clearly show how all coefficients of the weight enumerator can be obtained from the first three. Let us now examine what the possibilities are for $A_0(x)$, $A_1(x)$ and $A_2(x)$. We first observe that:

(i) for $C^\perp$ itself, we have $A_0 = 1$, $A_1 = A_2 = 0$, since the minimum distance is at least 3.

(ii) for any coset of minimum weight equal to 3, we have $A_0 = A_1 = A_2 = 0$.

Note that, in this case, we must have, from (2), $\alpha_3 A_3 = 1$.

In both cases the weight distribution is uniquely determined. For each of the remaining cosets $C^\perp + x$, let us assume that there exist integers $\lambda_1$, $\lambda_2$ such that the number of codewords from $C^\perp$ at distance 2 from $x$ is given by $\lambda_1$, respectively $\lambda_2$, if the minimum weight of $C^\perp + x$ is 1, respectively 2. This

*) For a definition of the Krawtchouk expansion, we refer, for example, to MacWilliams and Sloane*), p. 168.
means that for the weight distribution of $C^\perp + x$, we have either

$$A_0(x) = 0, \quad A_1(x) = 1, \quad A_2(x) = \lambda_1,$$

or

$$A_0(x) = A_1(x) = 0, \quad A_2(x) = \lambda_2,$$

and the conditions are fulfilled to have a pair of dual association schemes.

We now restate the above result in the form of a theorem, which also provides restrictions on the weights occurring in $C$.

**Theorem 2.2**

Let $C$ be a three-weight projective code with weights $w_1, w_2, w_3$, and let its dual $C^\perp$ have covering radius equal to 3. If there exist integers $\lambda_1, \lambda_2$ such that for any vector $x$, the number of codewords from $C^\perp$ at distance 2 from $x$ is given by

$$\begin{align*}
\lambda_1, & \text{ if } d(x, C^\perp) = 1, \\
\lambda_2, & \text{ if } d(x, C^\perp) = 2,
\end{align*}$$

and is zero otherwise, the restriction of the Hamming scheme to $C$ is an association scheme with 3 classes and

$$\frac{q^3}{2 \lambda_2} \prod_{i>j} (w_i - w_j)$$

is an integer dividing $|C|^3$.

**Proof**

From the assumptions, it follows that the weight distribution of any coset of $C^\perp$ depends only on its minimum weight. For the first three coefficients we have one of the following four possibilities, depending on the minimum weight:

- if the minimum weight is 0: $A_0 = 1, A_1 = A_2 = 0$;
- if the minimum weight is 1: $A_0 = 0, A_1 = 1, A_2 = \lambda_1$;
- if the minimum weight is 2: $A_0 = A_1 = 0, A_2 = \lambda_2$;
- if the minimum weight is 3: $A_0 = A_1 = A_2 = 0$.

The other coefficients $A_i$ are obtained by the relations (2), (3) of lemma 2.1. Hence, by theorem 6.10 of Delsarte, the distance relations define an association scheme $A$ on $C$. As indicated at the beginning of this section, we have also a 3-class association scheme $B$ on the set $X$ of cosets of $C^\perp$, and $A$ and $B$ are dual schemes. Let $S_i$ be the set of cosets of weight $i$, for $i = 1, 2, 3$, and let $D_i$ the adjacency matrix of the relation $R_i$ on $X$, with $R_i$ defined as above, i.e.

$$(C^\perp + x, C^\perp + y) \in R_i \iff C^\perp + (x + y) \in S_i.$$
The eigenvalues of $D_1$ are $n(q - 1)$ with multiplicity 1 and $n(q - 1) - q w_i$ with multiplicity $B_i$, where $B_i$ is the number of codewords of $C$ with weight $w_i$, for $i = 1, 2, 3$.

Thus

$$\prod_{i=1}^{3} [D_1 - (n(q - 1) - q w_i) I] = \frac{q^3 w_1 w_2 w_3 J}{|C|},$$

(4)

where $J$ denotes the all-one matrix of size $|C| = q^k$, and $(D_1 - n(q - 1) I) J = 0$.

From our assumptions, it follows that

$$D_1^2 = n(q - 1) I + (q - 2) D_1 + 2(\lambda_1 D_1 + \lambda_2 D_2).$$

Hence the eigenvalues of $D_2$ and of $D_3 = J - I - D_1 - D_2$ can be obtained from those of $D_1$. Defining the polynomials $F(z)$ and $P_i(z)$ for $i = 1, 2, 3$, as follows:

$$F(z) = |C| \prod_{i=1}^{3} \left( 1 - \frac{z}{w_i} \right) = \frac{|C|}{q^3 w_1 w_2 w_3} \prod_{i=1}^{3} (K_1(z) - K_1(w_i)),$$

$$P_1(z) = K_1(z) = n(q - 1) - q z,$$

$$P_2(z) = \frac{1}{2\lambda_2} \left( K_2(z) - 2\lambda_1 K_1(z) - (q - 2) K_1(z) - n(q - 1) \right),$$

$$P_3(z) = F(z) - (1 + P_1(z) + P_2(z)),$$

we can give the eigenmatrix of the coset scheme the form:

$$P = \begin{bmatrix}
1 & P_1(0) & P_2(0) & P_3(0) \\
1 & P_1(w_1) & P_2(w_1) & P_3(w_1) \\
1 & P_1(w_2) & P_2(w_2) & P_3(w_2) \\
1 & P_1(w_3) & P_2(w_3) & P_3(w_3) \\
1 & K_1(0) & K_1^2(0) & K_1^3(0) \\
1 & K_1(w_1) & K_1^2(w_1) & K_1^3(w_1) \\
1 & K_1(w_2) & K_1^2(w_2) & K_1^3(w_2) \\
1 & K_1(w_3) & K_1^2(w_3) & K_1^3(w_3)
\end{bmatrix} T,$$

(5)

where $T$ is an upper triangular matrix with diagonal entries

$$T_{00} = T_{11} = 1, \quad T_{22} = \frac{1}{2\lambda_2}, \quad T_{33} = \frac{|C|}{q^3 w_1 w_2 w_3}.$$

From (5) we easily compute the determinant of $P$

$$\det P = \frac{q^3}{2\lambda_2} \prod_{i>j} (w_i - w_j) |C|.$$

If $Q$ is the dual eigenmatrix then $P Q = |C| I$ and the divisibility result is obtained by taking determinants.
A special case of theorem 2.2 is when $C^\perp$ is a 2-error-correcting code. In this case $\lambda_1 = 0$, $\lambda_2 = 1$, and Calderbank and Goethals proved as a corollary that there exists an integer $t$ such that either

(i) $w_3 - w_2 = w_2 - w_1 = p^t$ (with $q = p^m$),
(ii) $p = 3$, $w_3 - w_2 = 2.3^t$, and $w_2 - w_1 = 3^t$, or
(iii) $p = 3$, $w_3 - w_2 = 3^t$, and $w_2 - w_1 = 2.3^t$.

Note that the minimum distance $d$ of $C^\perp$ is at most equal to 7, cf. Delsarte. If $d = 7$, then $C^\perp$ is a perfect 3-error-correcting code, as MacWilliams proved that an $e$-error-correcting linear code is perfect if and only if there are exactly $e$ weights in the dual code. The only example of a perfect 3-error-correcting code is provided by the [23, 12, 7] binary Golay code whose dual has weights 8, 12 and 16. If $d = 5$ or 6, then $C^\perp$ is a uniformly packed 2-error-correcting code. Uniformly packed codes are a generalization of perfect codes and were introduced by Semakov, Zinovjev and Zaitzev. Goethals and van Tilborg proved that an $e$-error-correcting linear code is uniformly packed if and only if there are exactly $e + 1$ weights in the dual code. For example, the [21, 12, 5] and [22, 12, 6] binary codes obtained by puncturing the [23, 12, 7] Golay code are uniformly packed. Another family of examples is provided by the 2-error-correcting binary BCH codes of length $n = 2^{m+1} - 1$ $(m \geq 2)$ and dimension $2^{m+1} - 4m - 3$, for which Kasami proved that the non-zero code-words in the dual code have weight $2^{m-2} - 2^m, 2^m$ or $2^m + 2^m$. Further examples and/or possibilities are mentioned by the authors in a previous paper. We note that in all of the above cases, we have $\lambda_1 = 0$, and $\lambda_2 = 1$. In the next section we shall describe some families of examples for which $\lambda_1 \neq 0$ and $\lambda_2 > 1$.

3. Subcodes of the second-order Reed-Muller codes

In this section we shall show that all three-weight cyclic subcodes of RM$(2,m)^*$, the shortened second-order binary Reed-Muller code, satisfy the conditions of theorem 2.2. Kasami first obtained the weight distributions of these codes. Goethals described a method for analyzing these codes, based on the theory of alternating bilinear forms. From these results it follows that the only three-weight cyclic codes which are subcodes of RM$(2,m)^*$ are those described in the following lemma. For more details the reader may consult MacWilliams and Sloane, chap. 15.

**Lemma 3.1**

Let $C$ be the cyclic code of length $n = 2^m - 1$ $(m \geq 4)$ and parity-check polynomial $h(x) = m_1(x) m_2(x)$, where $s = 2^i + 1$, for some $i \leq m/2$. Then $C$ is a three-weight code if and only if either $s$ is relatively prime to $n$ or $m$ is even and $s = 2^{m/2} + 1$. 

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


148
The weight distribution of these codes can be described as follows. When \( n \) and \( s \) are relatively prime, we have \((m, 2i) = (m, i) = d\), say. Then, with \( r \) defined by \( r = \frac{1}{2}(m - d)\), the weight distribution of \( C \) is as given in the table below (table I).

**TABLE I**

<table>
<thead>
<tr>
<th>( w = ) weight</th>
<th>( B_w = ) number of codewords</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^{m-1} - 2^{m-1-r} )</td>
<td>( (2^m - 1)(2^r + 1)2^{r-1} )</td>
</tr>
<tr>
<td>( 2^{m-1} )</td>
<td>( (2^m - 1)(2^m - 2^{2r} + 1) )</td>
</tr>
<tr>
<td>( 2^{m-1} + 2^{m-1-r} )</td>
<td>( (2^m - 1)(2^r - 1)2^{r-1} )</td>
</tr>
</tbody>
</table>

For the special case \( m = 2t, n = 2^{2t} - 1, s = 2^t + 1 \), the weight distribution is as given in the table below (table II).

**TABLE II**

<table>
<thead>
<tr>
<th>( w = ) weight</th>
<th>( B_w = ) number of codewords</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^{2t-1} - 2^{t-1} )</td>
<td>( (2^t - 1)(2^{2t-1} + 2^{t-1}) )</td>
</tr>
<tr>
<td>( 2^{2t-1} )</td>
<td>( (2^{2t} - 1) )</td>
</tr>
<tr>
<td>( 2^{2t-1} + 2^{t-1} )</td>
<td>( (2^t - 1)(2^{2t-1} - 2^{t-1}) )</td>
</tr>
</tbody>
</table>

Delsarte and Goethals\(^{12}\) showed the relation between the latter codes and multiplicative groups consisting of \( 2^t \) Hadamard matrices of order \( 2^{2t} \). Sarwate and Pursley\(^{4}\) called the periodic sequences derived from the codewords of these codes “Kasami sequences”. Many of the sequences derived from the codes described above have interesting crosscorrelation properties.

**Lemma 3.2**

Let \( C^\perp \) be the dual of the cyclic code described in lemma 3.1 and let \( C' \) be the code of length \( n + 1 \) obtained from \( C^\perp \) by adding an overall parity-check. Then \( C' \) is left invariant by the doubly transitive group of affine permutations

\[
x \rightarrow ax + b
\]

in the field \( \text{GF}(2^m) \).

**Proof**

The codewords of \( C' \) can be described by the subsets \( X \) of \( \text{GF}(2^m) \) satisfying

\[
\sum_{x \in X} x = 0, \quad \sum_{x \in X} x^{\tau+1} = 0, \quad |X| = 0 \mod 2, \tag{6}
\]

where we have written \( \tau \) for \( 2^t \). Under the affine transformation \( x \rightarrow ax + b \) the set \( X \) is transformed into the set \( Y = \{ax + b | x \in X\} \).
Clearly we have \(|Y| = |X|\), and

\[
\sum_{y \in Y} y = a \sum_{x \in X} x + b |X|,
\]

\[
\sum_{y \in Y} y^{t+1} = a^{t+1} \sum_{x \in X} x^{t+1} + a^t b \sum_{x \in X} x^t + ab^t \sum_{x \in X} x + b^{t+1} |X|.
\]

Since moreover \(\sum x^t = (\sum x)^t\), it follows that \(Y\) satisfies the conditions (6) whenever \(X\) does.

\[\square\]

**Corollary 3.3**

The dual \(C^\perp\) of the codes described in lemma 3.1 have the property that, for any \(t \geq 2\) and for any pair of coordinate places, the number of codewords of weight \(2t - 1\) or \(2t\) having a "1" in both places is a constant \(\lambda(t)\) independent of the pair of coordinate places.

**Proof**

This follows from the fact that the extended code \(C'\) is left invariant by a doubly transitive group of permutations. Hence, for any \(t \geq 2\), the codewords of weight \(2t\) in \(C'\) form a 2-design \(2-(2^t, 2t, \lambda(t))\).

\[\square\]

**Corollary 3.4**

The codes \(C\) described in lemma 3.1 satisfy the conditions of theorem 2.2.

**Proof**

The dual code \(C^\perp\) is generated by \(m_1(x) m_s(x)\), hence has minimum weight at least equal to 3. From corollary 3.3 it follows that the number of codewords at distance 2 from any vector \(x\) is

\[
\lambda_1 = \lambda(2), \text{ if } d(x, C^\perp) = 1,
\]

\[
\lambda_2 = 1 + \lambda(2), \text{ if } d(x, C^\perp) = 2,
\]

with \(\lambda(2)\) defined as in corollary 3.3.

\[\square\]

4. **Association schemes defined by three-weight subcodes of \(RM(2, m)^*\)**

In this section, we shall study in more detail the association schemes defined by the codes of sec. 3.

4.1. **The special case \(m = 2t, s = 2^t + 1\)**

In this case the code \(C\), with weight distribution as given in table II, has dimension \(3t\). Its dual \(C^\perp\) has minimum weight equal to 3 and the number of codewords of weight 3 is given by

\[
A_3 = \frac{(2^{t-1} - 1) (2^{2t} - 1)}{3}.
\]
The constant $\lambda(2)$ is then given by

$$\lambda(2) = \frac{3A_3}{2^{2r} - 1} = 2^{r-1} - 1,$$

and $\lambda_1 = \lambda(2)$, $\lambda_2 = 1 + \lambda(2)$, cf. corollary 3.3.

The Krawtchouk expansion of the polynomial $F(z)$, cf (1), is easily computed from the weights in table II. It is given by

$$F(z) = \frac{1}{2^{r-1}} \left[ K_0(z) + K_1(z) + \frac{1}{(2^{2r} - 1)/3} (K_2(z) + K_3(z)) \right].$$

From these data, one can obtain the eigenmatrix (5) of the coset scheme, which is given by

$$P = \begin{bmatrix}
I & D_1 & D_2 & D_3 \\
1 & (2^{2r} - 1) & (2^r - 1)(2^{2r} - 1) & (2^r - 1) \\
1 & (2^r - 1) & -(2^r - 1) & -1 \\
1 & -1 & -(2^r - 1) & (2^r - 1) \\
1 & -(2^r + 1) & (2^r + 1) & -1 \\
\end{bmatrix}.$$ 

We observe that $D_2$ and $D_3$ are the adjacency matrices of strongly regular graphs, since apart from their valencies, they have only two distinct eigenvalues. Moreover one of these eigenvalues is actually equal to the valency for $D_3$. This means that the graph defined by the cosets of weight 3 is a disjoint union of cliques of size $2^r$. In fact it is easily verified that the association scheme is *imprimitive* in the sense defined by Cameron, Goethals and Seidel\(^\text{13}\)). The clique property means that any two cosets of weight 3 are mutually at distance 3. Hence adjoining this set of cosets to the code $C^\perp$ gives a code with minimum distance 3 which is $2^r$ times as large. It is not difficult to verify that the latter is the Hamming code.

The dual scheme which is defined by the distance relations in $C$ is also *imprimitive*. It is easily verified, for example, that the graph defined by the distance $w_2 = 2^{2r-1}$ is a disjoint union of cliques of size $2^{2r}$. The $2^{2r}$ codewords in any clique are in a one-to-one correspondence with the rows of one of Hadamard matrices described by Delsarte and Goethals\(^\text{12}\)).

4.2. *The general case* $s = 2^i + 1$, $(2^i + 1, 2^m - 1) = 1$

In this case the code $C$, with weight distribution as given in table I, has dimension $2m$. The number of codewords of weight 3 in its dual is given by

$$A_3 = \frac{(2^m - 1)(2^{m-1-2r} - 1)}{3},$$

where $r = \frac{1}{2}(m - d)$, $d = (m, 2i) = (m, i)$. 

---

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

We observe that $A_3 = 0$ if $d = 1$, which occurs if and only if $m$ is odd and $i$ is relatively prime to $m$. This is the case when $i = 1$, i.e. $s = 3$. We then have the 2–error–correcting BCH codes of length $2^m - 1$, $m$ odd, which are known to be uniformly packed, cf. Goethals and van Tilborg\(^2\)). The above result shows that uniformly packed codes with the same parameters can be obtained for all $i$ that are relatively prime to $m$. For these codes, we have indeed $A_3 = 0$, hence $\lambda(2) = 0$, $\lambda_1 = 0$, $\lambda_2 = 1$. In the remaining cases, $\lambda(2)$ is given by

$$\lambda(2) = \frac{3A_3}{(2^m - 1)} = 2^{m-1-2r} - 1.$$ 

The Krawtchouk expansion of $F(z)$, cf. (1), is given by

$$F(z) = \frac{1}{2^m - 2^{m-2r}} [(3 \cdot 2^m - 2^{m-2r} - 2)(K_0(z) + K_1(z)) + 6(K_2(z) + K_3(z))]$$

and the eigenmatrix of the coset scheme, by

$$P = \begin{bmatrix} I & D_1 & D_2 & D_3 \\ 1 & (2^m - 1) & (2^m - 1)(2^r - 1) & (2^m - 1)(2^m + 1 - 2^r) \\ 1 & (2^m - 1) & (2^m - 1)(2^r - 1) & (2^m + 1 - 2^r) \\ 1 & -1 & -(2^r - 1) & (2^r - 1) \\ 1 & -1 & -(2^m - 1 + 1 & (2^m - 1)(2^r - 2^r + 1) & (2^m + 1 - 2^r) \end{bmatrix}.$$ 

Here also we observe that the graph defined by the cosets of weight 3 is strongly regular. A similar property holds for the graph defined by the distance $w_2$ in the distance scheme.

REFERENCES