On the Orthogonality of Geometric Codes

DAVID G. GLYNN
glynn@mac.com
3 St. Winifreds Place, Brynher, Christchurch 8005, New Zealand

Communicated by: J. Hirschfeld

Received November 2, 2000; Revised May 29, 2002; Accepted June 10, 2002

Abstract. We solve some problems concerning the orthogonality of geometric codes associated with sets of i- and j-dimensional subspaces of \( PG(n, q) \). Various applications are found, and we discuss all the interesting cases in small dimensional spaces.

Keywords: geometric code, dual code, Reed-Muller code, polynomial function

AMS Classification: 51E20, 05B25, 14G15, 94B15

1. Introduction

\( PG(n, q) \) is the finite projective geometry of dimension \( n \) over the finite field \( F = GF(q) \), where \( q = p^h \), \( p \) prime. \( [n]_i := PG^{(i)}(n, q) \) is the set of all \( i \)-dimensional subspaces of \( PG(n, q) \), where \( -1 \leq i \leq n \).

We restate the main theorem of geometric codes (due to Delsarte and in a different way, to Hamada), as given in the paper by Glynn and Hirschfeld [2]. This uses the point of view of projective geometry codes as Reed-Muller codes. For a detailed account and more references, see Assmus and Key [1, Chapter 5].

Let \( C = C(n, q) \) be the set of all functions from \( PG^{(i)}(n, q) \) to \( F \). It is a vector space of dimension \( v := q^n + \cdots + q + 1 \) over \( F \), with the usual addition of functions and multiplication of functions by a scalar in \( F \). A function \( f \in C \) can be thought of as a vector \( (a_1, \ldots, a_v) \) with \( f(P) = a_j \), for some labeling \( P_j \) of the points. A function can be called a word, and the weight of a word is the number of non-zero values that the function takes. With these assumptions any subspace of functions of \( C \) gives a linear code, of which one of the most important is the following.

The geometric code

\[
C_i(n, q) := \left\{ f \in C \mid \sum_{P \in [n]_i} f(P) = 0, \forall \sigma \in [n]_j \right\}, \quad (0 \leq i \leq n).
\]

When \( n \) and \( q \) are understood this function code is denoted by \( C_i \). It is not hard to show that \( C_i \subseteq C_j \) for all \( i \leq j \leq n \).

The characteristic function \( \chi(S) \) of any subset \( S \) of points of \( PG(n, q) \) is just the function mapping points of \( S \) to 1, and all other points to 0. So the code \( C_i^\perp \) is the
subspace of $C$ generated by the characteristic functions of the $i$-dimensional subspaces. These codes $C^+_i$ can be called the subspace codes. For example it is natural to call $C^+_1$ the line code, $C^+_2$ the plane code, and $C^+_n-1$ the hyperplane code. The codes $C_i$ and $C^+_i$ are duals, and so their dimensions satisfy $\dim(C_i) + \dim(C^+_i) = q^n + \cdots + q + 1$.

Each point of $PG(n,q)$ is represented as usual by homogeneous coordinates $(x_0, \ldots, x_n)$. Any function $f \in C$ is represented by a unique polynomial $g$ in the $n+1$ variables $x_i$, every term of which is "reduced"; that is, a general term is $t = c \prod_{i=0}^{n} x_i^{a_i}$, where $c \in GF(q)$ and $0 \leq a_i \leq q - 1$, such that $f(x) = g(x)$ for all $x \in PG(n,q)$ with $g(0) = 0$. Every term of $g$ has total degree $\sum_{i=0}^{n} a_i = e(q-1)$, where $e \in \mathbb{Z}, 1 \leq e \leq n+1$; note that $e$ need not be the same for different terms. A term has the form $x_0^{a_0} \cdots x_n^{a_n}$ while the corresponding monomial is $x_0^{e_0} \cdots x_n^{e_n}$.

The reduction mapping is the function $r : \mathbb{Z} \to \{0, \ldots, q-1\}$, such that $r(0) = 0, r(n) \equiv n \pmod{q-1}$, and $r(e(q-1)) = q - 1$, for all $e \in \mathbb{Z} \setminus \{0\}$. If $t = c \prod_{i=0}^{n} x_i^{a_i}$ is a term with $c \neq 0$, then the reduced degree of $t$ is $\deg(t) := \sum_{i=0}^{n} r(a_i)$. We use this reduction to make certain that we always have valid terms with powers between 0 and $q - 1$.

Note that we do not allow a constant in $F$ to be a valid term of a homogeneous function: this is at variance with Assmus and Key [1, Section 5.6], where this does occur sometimes. We believe that our approach, and that of Glynn and Hirschfeld [2], is more consistent. For one thing, our polynomials satisfy the natural condition $g(0) = 0$, and for another, we have no problems constructing unique basis elements this way.

Indeed every function in $C$ can be written in the form (see Glynn and Hirschfeld [2])

$$f(x) = \sum_{\substack{0 \leq a_0, a_1, \ldots, a_n \leq q-1 \\ a_0 \neq 0 \ \ a_i \neq 0 \ \ for \ i = 1, \ldots, n}} k_{a_0} x_0^{a_0} \cdots x_n^{a_n},$$

for unique $k_{a_0} \cdots a_n \in F$. $k_{0_0, 0} = 0$ and so $f$ has no constant term. Each term of $f(x)$ must have degree that is divisible by $q-1$ and is non-zero. The coefficients $k_{a_0} \cdots a_n$ of the terms are uniquely determined by the function.

We say that a polynomial function $f$ in $C$ has a term $t$ if the coefficient in $GF(q)$ of $t$ in the unique representation of $f$, as a sum of terms, is non-zero.

Consider a monomial $t = x_0^{a_0} \cdots x_n^{a_n}$, where the exponents $a_i$ satisfy $0 \leq a_i \leq q - 1, (a_i \in \mathbb{Z})$. Also, the degree of $t$ should satisfy $\deg(t) := \sum_{i=0}^{n} a_i = j(q - 1)$, for some $1 \leq j \leq n+1$. Thus $t$ is a "valid monomial" of $C(n, q)$.

The degree sequence $S(t)$ of $t$ is the "cycle" of integers $(s_0, s_1, \ldots, s_{k-1})$, where $s_k = \deg(p^k)/(q - 1)$, and the subscripts $k$ are considered to be in the cyclic group modulo $h$.

Any degree sequence must satisfy a certain set of inequalities and conversely, any such sequence corresponds to at least one valid monomial.
ON THE ORTHOGONALITY OF GEOMETRIC CODES

LEMMA 1.1. A sequence $S$ is the degree sequence of a monomial in $C(n,q)$, $q = p^h$, $p$ prime, if and only if $0 \leq p \cdot s_{k+1} - s_k \leq (n+1)(p-1)$, $0 \leq k \leq h-1$, and $p \cdot s_{k+1} - s_k > 0$ for some $0 \leq k \leq h-1$.

Proof. See Glynn and Hirschfeld [2].

Definition 1.2. The minimum value taken by a degree sequence $S$ is denoted by $\min(S)$. Its maximum value is denoted by $\max(S)$. If $t$ is any valid monomial of $C$, and if $t$ has degree sequence $S(t)$ then $\mindeg(t) := \min(S(t))$, while $\maxdeg(t) := \max(S(t))$.

THE MAIN THEOREM OF GEOMETRIC CODES $C_i$. 1.3. A basis for the vector space of polynomials corresponding to the functions of $C_i$ consists of the monomials of $C$ of $\mindeg \leq i$.

Now let us consider the implications for the dual code $C_i^\perp$.

THE MAIN THEOREM OF SUBSPACE CODES $C_i^\perp$. 1.4. A basis for the vector space of polynomials corresponding to the functions of $C_i^\perp$ consists of:

1. The monomials of $C$ of $\maxdeg \leq n - j$.
2. The function

$$f_j := \sum_{|A| \leq j, A \subseteq \{0, \ldots, n\}} (-1)^{|A|} \prod_{i \notin A} x_i^{q-1}.$$  

Proof. This has an easy proof that follows quickly from Theorem 1.3. It also follows from a theorem of Delsarte (see Assmus and Key [1]) with perhaps the polynomial $f_j$ being replaced by 1. Firstly, each monomial of type (1) above is the “complement” of a monomial that is not in $C_j$, where the complement of $x_0^{\alpha_0} \ldots x_n^{\alpha_n}$ is $x_0^{n+1-\alpha_0} \ldots x_n^{n+1-\alpha_n}$. Note that $t$ has degree sequence $S(t)$ if and only if its complement $t$ has degree sequence $n+1 - S(t)$. Now there is just one valid monomial in $C$, the complement of which is not a valid monomial in $C$. This is the monomial $x_0^{q-1} \ldots x_n^{q-1}$, which is also the only monomial with degree sequence $(n+1 \ldots n+1)$. However, we can associate the function of type (2) with this monomial. This gives us a bijection between the set of functions of types (1) and (2) above, and the valid monomials not in $C_j$. Hence, by the dimension formula for the dual code, the number of functions for our presumed basis is correct. In addition, the above functions are clearly linearly independent over $GF(q)$, since they have no terms in common. And finally, we have to check that each monomial of (1) is in $C_j^\perp$, and so is $f_j$. But this is quite easy, using the fact that a function, summed over all points of $PG(n,q)$, is zero if and only if the function has no term $cx_0^{q-1} \ldots x_n^{q-1}$, $c \neq 0$. (Use the main theorem of geometric codes in the case $i = n$.) Now two functions are “orthogonal” if and only if their product has a zero sum over all points of $PG(n,q)$ if
and only if there is no term $x_0^{q-1} \ldots x_n^{q-1}$ in their product (when viewed as a reduced algebraic function). Hence we see immediately that a monomial of mindeg at most $j$ and a monomial of maxdeg at most $n - j$ are orthogonal. Then we can check that $f_j$ is also orthogonal to every monomial of $C_j$. Thus if $|A| \leq j$, and $A \subseteq \{0, \ldots, n\}$, then $\prod_{x \in A} x_0^{q-1} \cdot t$ has a sum over all points that is zero unless all the exponents of $t$ are 0 or $q - 1$. However in the latter case $f_j \cdot t$ turns out to be the zero function.

Note that the function of type (2) in Theorem 1.4 does not have any terms of type (1), and so it is easy to tell from the terms of a function if it is in a certain subspace code. Perhaps we could change the complicated function of type (2) to the unit function $1$, but this would be a false saving, since 1 in fact has a more complicated algebraic formula when we use valid terms.

The above result makes it natural for us to consider the following code.

**Definition 1.5.** $\tilde{C}_j^\perp :=$ the subspace of $C_j^\perp$ generated by the monomials of maxdeg $\leq n - j$. Equivalently, this is the subspace of functions of $C_j^\perp$ that have a sum of zero over all points of $PG(n, q)$. Another way to generate this subspace is to take sums of the characteristic functions of $j$-dimensional subspaces, the coefficients of which sum to zero.

This gives us enough knowledge to characterize the orthogonality of these codes.

2. **The Orthogonality of Geometric Codes**

Let $0 \leq i \leq n$, and $0 \leq j \leq n$. We say that $C_i$ is orthogonal to $C_j$, writing $C_i \perp C_j$, if the product of a function from $C_i$ and a function from $C_j$ always has a zero sum over all points of $PG(n, q)$. Thus $C_i \perp C_j$ if and only if $C_i \subseteq \tilde{C}_j^\perp$, and this happens when every function from $C_i$ is a sum of the characteristic functions of $j$-dimensional subspaces with various coefficients. Similarly, $C_j^\perp \perp C_j^\perp$ if and only if $C_j^\perp \subseteq C_j$. But clearly this cannot happen, because there is always the generator $f_j \in C_j^\perp$, which has the term $f_n = x_0^{q-1} \ldots x_n^{q-1}$, which is never in $C_j$. Hence, Definition 1.5 gives us a more satisfactory answer.

**Theorem 2.1.** $\tilde{C}_j^\perp \subseteq C_i$ if and only if $\tilde{C}_i^\perp \subseteq C_j$ if and only if $i + j \geq n$. If $i + j \geq n$ then $C_j^\perp \cap C_i = C_j^\perp$.

**Proof.** The monomials in $C_j^\perp$ have maxdeg $\leq n - j$, and those in $C_i$ have mindeg $\leq i$. Thus every monomial of $C_j^\perp$ is a monomial of $C_i$ if and only if $n - j \leq i$. Note that at least one monomial with constant degree sequence $(k, \ldots, k)$ for $1 \leq k \leq n + 1$ always exists, indeed because this sequence satisfies the inequalities of Lemma 1.2, or more directly, because the monomial $x_0^{q-1} \ldots x_{k-1}^{q-1}$ is an example. Such a monomial has mindeg = maxdeg = $k$. Putting $k = n - j$ shows that the condition $i + j \geq n$ of the theorem is necessary.
Geometrically, the above theorem says that a sum of the characteristic functions of $j$-dimensional subspaces, with coefficients adding to zero, is always orthogonal to the characteristic function of any $i$-dimensional subspace if and only if $i + j \geq n$. In fact, there is an easy geometrical proof of this fact using the property that $i$-dimensional and $j$-dimensional subspaces intersect in 1 modulo $q$ points if $i + j \geq n$, but can also be skew if $i + j < n$, for the number of points of a $k$-dimensional subspace that is the intersection of two subspaces is $q^k + \cdots + q + 1$.

The next observation follows directly from Theorems 1.3 and 1.4.

**Lemma 2.2.** \(C_i \perp C_j\) in \(PG(n, q)\) if and only if, for any valid degree sequence \(S\) of \(PG(n, q)\), if it has \(\min(S) \leq i\) then it has \(\max(S) \leq n - j\).

**Proof.** For \(C_i \perp C_j\) in \(PG(n, q)\) if and only if \(C_i \subseteq C_j^\perp\), and it follows immediately from the bases of \(C_i\) and \(C_j^\perp\) that the vector space of functions \(C_i \cap C_j^\perp\) is generated by monomials that have both \(\mindeg \leq i\) and \(\maxdeg \leq n - j\). \(\square\)

However, the next theorem does not seem to have an easy geometrical proof such as the one above.

**Theorem 2.3.** \(C_i \perp C_j\) in \(PG(n, q)\) implies \(C_i \perp C_j\) in \(PG(n + 1, q)\), and so in \(PG(m, q), \forall m \geq n\).

**Proof.** We use Lemma 2.2. The problem to characterize \(C_i \perp C_j\) then reduces to a purely integer programming one, since a valid monomial exists if and only if certain linear inequalities on its degree sequence are satisfied. Thus, all we need to show for this theorem is that given a valid degree sequence \(S\) of \(PG(n + 1, q)\) with \(\min(S) \leq i\) and \(\max(S) \geq n + 2 - j\) then we can construct a valid sequence \(S'\) for \(PG(n, q)\) that satisfies \(\min(S') \leq i\) and \(\max(S') \geq n + 1 - j\). The way to do this is to subtract 1 from \(S\) at appropriate places \(s_{k+1}\) where \(p \cdot s_{k+1} - s_k \leq (n + 1)(p - 1)\). Other values of \(S\) can stay the same. Thus, from a monomial of \(C(n + 1, q)\) that is in \(C_i\) but not in \(C_j^\perp\) we obtain at least one monomial of \(C(n, q)\) that does the same. We should assume that the monomial of \(C(n + 1, q)\) does not have constant degree sequence, which we can. Then we can check that the appropriate inequalities are satisfied for the new sequence \(S'\). Also, \(\min(S') = \min(S)\) and \(\max(S') = \max(S) - 1\). \(\square\)

Certainly, the following shows that there is a minimal value of \(n\) such that \(C_i \perp C_j\) in \(PG(n, q)\).

**Theorem 2.4.** Suppose that \(i \leq j\). Then \(C_i \perp C_j\) in \(PG(n, q)\), where \(q = p^h, p\) prime, if \(n \geq ip^{h-1} + j\).

**Proof.** Suppose \(n \geq ip^{h-1} + j\). Suppose we have a valid degree sequence \(S\) for a monomial of \(C(n, q)\) such that \(\min(S) \leq i\). Using an automorphism (or a cycle) of the degree sequence we can assume that \(s_{h-1} \leq j\). Now, using the inequalities \(0 \leq p \cdot s_{k+1} - s_k\) of Lemma 1.1, we see that \(s_{h-2} \leq p \cdot s_{h-1} \leq p^1, s_{h-3} \leq p \cdot s_{h-2} \leq p^2, \text{ and} \)
in fact $s_0 \leq p^{h-1}i$. Thus $\max(S) \leq p^{h-1}i \leq n-j$. Hence using Lemma 2.2, we see that $C_i \perp C_j$ in $PG(n, q)$.

This theorem is best possible in the case of $q = p$ or $p^2$. We leave the proof of that as an exercise, since we obtain a precise result for all $q$ in Theorem 2.7 below.

**Theorem 2.5.** $C_i \perp C_j$ in $PG(n, q)$, where $q = p^h$, $p$ prime, $h = 1$ or $2$, $(i \leq j)$, if and only if $n \geq ip^{h-1} + j$.

Just as Theorem 2.4 says that if $n$ is large enough $C_i$ and $C_j$ are orthogonal, the reverse happens if $q$ is large enough and the characteristic $p$ is fixed.

**Theorem 2.6.** $C_i \not\perp C_j$ in $PG(n, q)$, $q = p^h$, $p$ prime, implies that $C_i \not\perp C_j$ in $PG(n, q')$, $q' = p^{h'}$, $p$ prime, $\forall h' \geq h$.

**Proof.** If $S$ is a valid degree sequence for a monomial of $C(n, q)$, then we can create another valid degree sequence for a monomial of $C(n, q)$ merely by repeating say $s_{h-1}$ at the end of the sequence. Note that the inequalities of Lemma 1.1 only depend upon $p$ and $n$, but the number of variables is $h$. Thus, $C_i \not\perp C_j$ in $PG(n, q)$ if and only if there exists a valid degree sequence for a monomial in $C(n, q)$ that has $\min(S) \leq i$ and $\max(S) > n-j$. But there exists a monomial in $C(n, q')$ which has a degree sequence with the same min and max.

**Theorem 2.7.** $C_i \perp C_j$ in $PG(n, q)$ $(i \leq j)$, where $q = p^h$, $p$ prime, if and only if

$$h < r + s, \text{where } r := \lceil \log_p ((n + 1 - j)/i) \rceil \text{ and } s := \lceil \log_p ((n + 1 - i)/j) \rceil.$$

**Proof.** If we try to construct a valid degree sequence $S$ in $C(n, q)$ with $\min(S) = i$ and $\max(S) = n + 1 - j$ (which should exist if the two codes are not orthogonal) then we start at $i$ and go left by inserting $pi, p^2i$, for these are the largest possible given the inequality $pS_{k+1} - S_k \geq 0$. Thus we are able to reach $n + 1 - j$ from $i$ going left in at least $r$ steps. Using the same argument (and the complement $S'$ of the sequence) we can reach $i$ from $n + 1 - j$ in at least $s$ steps. Note that the inequality $pS_{k+1} - S_k \leq (n + 1)(p - 1)$ becomes $pS'_{k+1} - S'_k \geq 0$, where $S'_k := n + 1 - S_k, \forall k$. Hence the minimum value of $h$ for which there exists a valid degree sequence that has $\min(S) = i$ and $\max(S) = n + 1 - j$ is $r + s$, and if $h < r + s$ there is no such degree sequence. Note that $h = 1$ satisfies the inequality if and only if $i + j \leq n$.

We shall give examples of the above theorem in the final section. Before that let us note that these results can be extended to the so-called subfield subcodes of the geometric codes. See also Assmus and Key [1, Section 5.7] for similar arguments. Thus, given $C_j$ we can consider all the functions (or code-words) that take values in $GF(p)$. This code is called the $GF(p)$ subcode of $C_j$. Since $C_j^i$ is generated by the characteristic functions of $i$-dimensional subspaces of $PG(n, q)$, and these characteristic functions are over $GF(p)$, since $\{0, 1\} \subseteq GF(p)$, then the dimensions
of the $GF(p)$ subcode of $C_i^\perp$ and that of $C_j^\perp$ over $GF(q)$ are the same. Thus, we see that $C_i$ is also generated by its $GF(p)$ code-words, and the dimension of the $GF(p)$ subcode of $C_i$ is the same as that of $C_i$. This means that the results above (especially of Theorem 2.7) can be applied also when we replace $C_i$ and $C_j$ by their $GF(p)$ subcodes, for two codes are orthogonal if and only if their sets of generators are orthogonal.

3. Examples

We consider all projective spaces $PG(n, q)$ of small dimensions $n$ and calculate, using Theorem 2.7, the values of $i, j, p$ and $h$ for which $C_i \perp C_j$. First, note that the case $h = 1$ appears if and only if $i + j \leq n$. This is not so interesting and we omit all mention of this from now on, and concentrate on the cases $h \geq 2$. Also, we can assume that $1 \leq i \leq j$ and $i + j \leq n$, and it is also easy to see that $i + j = n$ only if $h = 1$, which is not so interesting.

$n = 2$.

$$2 \leq h < \left\lceil \log_p \left( \frac{3-j}{i} \right) \right\rceil + \left\lceil \log_p \left( \frac{3-i}{j} \right) \right\rceil,$$
gives no interesting cases (other than $h = 1$).

$n = 3$.

$$2 \leq h < \left\lceil \log_p \left( \frac{4-j}{i} \right) \right\rceil + \left\lceil \log_p \left( \frac{4-i}{j} \right) \right\rceil,$$
gives $(i, j) = (1, 1), p = 2, h \leq 3$.

Thus, $C_1 \perp C_1$ in $PG(3, q), q = p^h, h \geq 2$ if and only if $q = 4$ or 8.

$n = 4$.

$$2 \leq h < \left\lceil \log_p \left( \frac{5-j}{i} \right) \right\rceil + \left\lceil \log_p \left( \frac{5-i}{j} \right) \right\rceil,$$
gives $(i, j) = (1, 1), p = 2$ or 3, $h \leq 3$.

Thus, $C_1 \perp C_1$ in $PG(4, q), q = p^h, h \geq 2$ if and only if $q = 4, 8, 9,$ or 27.

$(i, j) = (1, 2), p = 2, h = 2$.

Thus, $C_1 \perp C_2$ in $PG(4, q), q = p^h, h \geq 2$ if and only if $q = 4$.

$n = 5$.

$$2 \leq h < \left\lceil \log_p \left( \frac{6-j}{i} \right) \right\rceil + \left\lceil \log_p \left( \frac{6-i}{j} \right) \right\rceil,$$
gives
\[(i,j) = (1,1), p = 2, h \leq 5, \text{ or } p = 3, h \leq 3,\]
\[(i,j) = (1,2), p = 2, h \leq 3, \text{ or } p = 3, h \leq 2,\]
\[(i,j) = (1,3), p = 2, h \leq 2.\]

\[n = 6.\]

\[2 \leq h < \left\lfloor \log_p \left( \frac{7-j}{i} \right) \right\rfloor + \left\lfloor \log_p \left( \frac{7-i}{j} \right) \right\rfloor,\]

gives
\[(i,j) = (1,1), p = 2, h \leq 5, \text{ or } p = 3 \text{ or } 5, h \leq 3,\]
\[(i,j) = (1,2), p = 2, h \leq 3, \text{ or } p = 3, h \leq 2,\]
\[(i,j) = (1,3), p = 2 \text{ or } p = 3, h \leq 2,\]
\[(i,j) = (2,2), p = 2, h \leq 3.\]

Another case is to characterize when \(C_1 \perp C_1\). Thus, we have \(h < 2\left\lfloor \log_p (n) \right\rfloor\) if and only if \(p^{h/2} < p^{\left\lceil \log_p (n) \right\rceil}\) if and only if \(\sqrt{q} < \text{ the smallest power of } p \geq n\) if and only if \(q < n^2\) (\(q\) a perfect square, \(h\) even), or \(q/p < n^2\), (\(q\) not a perfect square, \(h\) odd). This gives the final result.

**Theorem 3.1.** \(C_1 \perp C_1\) if and only if \(n^2 > q\) (\(q\) a perfect square, \(h\) even), or \(n^2 > q/p\) (\(q\) not a perfect square, \(h\) odd).

**Acknowledgment**

Thanks are due to Bhaskar Bagchi of the Indian Institute of Statistics, Bangalore, who suggested the problem considered in this paper when I visited there several years ago.

**References**