Journal of Combinatorial Theory, Series A **96**, 20–30 (2001)

Codes from Veronese and Segre Embeddings and Hamada's Formula

S. P. Inamdar and N. S. Narasimha Sastry

Stat-Math Unit, Indian Statistical Institute, 8th Mile, Mysore Road, Bangalore 560059, India
E-mail: inamdar@isibang.ac.in, nsastry@isibang.ac.in

Communicated by the Managing Editors

Received February 10, 2000; published online August 21, 2001

In this article we study the codes given by l hypersurfaces in $\mathbb{P}_q^n$ to obtain a new formula for the dimension of codes given by $(n-l)$ flats. We also obtain a new formula for the dimension of the νth order generalized Reed–Muller code and describe the code given by the hyperplane intersections of the Segre embedding of $\mathbb{P}_q^n \times \mathbb{P}_q^m$.

1. INTRODUCTION

This article grew out of our attempt to understand the methods of [6] in the context of Veronese and Segre embeddings of projective spaces over finite fields.

Let $q = p^e$, p a prime, and P denote the n dimensional projective space over the finite field $\mathbb{F}_q$. The zero set in P of a homogeneous polynomial of degree l over $\mathbb{F}_q$ is called a l *hypersurface* in P. Let k be a field of characteristic p. Let $C_k^n(l, q)$ denote the subspace of k^P spanned by the characteristic functions of l hypersurfaces in P. Our main results give a basis for $C_{\mathbb{F}_q}^n(l, q)$ consisting of monomial functions (Theorem 2.5), its cardinality (Theorem 2.13) and therefore the dimension of $C_k^n(l, q)$.

Let $\tilde{C}_k^n(l, q)$ denote the subspace of k^P spanned by the characteristic functions of l flats in P. Clearly, $C_k^n(l, q) = \tilde{C}_k^n(n-l, q)$ for $l = 0, 1$. We prove this equality for all $l \leqslant n$ (Theorem 3.3). Therefore, Theorem 2.13 provides an alternative to the well-known Hamada's formula [4, Theorem 1]. This identification also follows from recent results of M. Bardoe and P. Sin and we thank P. Sin for pointing this and sending us a copy of [2]. Apart from a conceptually different approach, our formula is also simpler. See Remarks 3.5 and 3.6. In Appendix, we use our formula to write certain explicit formulae. See [1, Corollary 5.7.5, pp. 186] for the words of minimum weights of these codes and [2] for their $PSL(n+1, q)$ module structure.

[3] discusses words of minimum weight of their duals and a reformulation of Hamada's formula.

In Secton 4, we give a new formula for the dimension of the νth order generalized Reed–Muller code (Theorem 4.1). In Section 5, we describe the code over k generated by the characteristic functions of intersections of the Segre embedding of $\mathbb{P}_q^n \times \mathbb{P}_q^m$ in $\mathbb{P}_q^{(n+1)(m+1)-1}$ with hyperplanes (Theorem 5.1).

2. THE l HYPERSURFACE CODE

Let $R = \mathbb{F}_q[X_0, ..., X_n]$. For any graded ring S, we denote by S_t its t^{th} graded piece. The zero set of an element in R_1 in P is also the zero set of its l^{th} power. Therefore $C_k^n(l, q)$ contains the code generated by the hyperplanes of P and thus the all one vector $\mathbf{1}$. Hence $C_k^n(l, q) = k\mathbf{1} \oplus D_k^n(l, q)$ where $D_k^n(l, q)$ is the k span of the characteristic functions of complements of l hypersurfaces in P. If $f \in R_l$, then f^{q-1} defines the characteristic function of the complement of the l hypersurface defined by f.

Let $T = \mathbb{F}_q[Z_m \mid m \in R_l,\ m \text{ a monomial}]$. We denote by φ_l the l^{th} Veronese homomorphism from T to R defined by $\varphi_l(Z_m) = m$ and $\varphi_l(\lambda) = \lambda$ for $\lambda \in \mathbb{F}_q$ (See [5, pp. 23]). Linear forms in T correspond to l forms in R under φ_l. Thus the characteristic function of the complement of a l hypersurface in P is given by $\varphi_l(h^{q-1})$ for some $h \in T_1$. Thus $D_k^n(l, q)$ is spanned by functions on P defined by elements of the form $\varphi_l(h^{q-1})$, $h \in T_1$. Further, the $\mathbb{F}_q$ span $T_{q-1}^{\dagger}$ of $\{h^{q-1} : h \in T_1\}$ has a basis consisting of monomials $Z_{m_0}^{a_0} \cdots Z_{m_r}^{a_r}$ of degree $(q-1)$ such that the multinomial coefficient $\binom{q-1}{a_0, a_1, ..., a_r}$ is not divisible by p. Thus,

Proposition 2.1. *$D_{\mathbb{F}_q}^n(l, q)$ consists of functions on P defined by elements of $\varphi_l(T_{q-1}^{\dagger})$. Therefore, $D_{\mathbb{F}_q}^n(l, q)$ has a monomial basis.*

A monomial in $R_{l(p-1)}$ can be written as a product of $(p-1)$ monomials in R_l. Therefore we have

Lemma 2.2. *The map φ_l induces a surjection from the vector space T_{p-1} onto $R_{l(p-1)}$.*

For an integer a_i, let $a_i = \sum a_{i,j} p^j$ denote its p-adic expression.

Definition 2.3. We denote by $S_{n,e}^{l,r}$ the set of monomials $X^a = X_0^{a_0} \cdots X_n^{a_n}$ of degree $(l-r)(q-1)$ such that there exist integers $1 \leqslant r_1, ..., r_{e-1} \leqslant l$ such that (i) $\sum_{i=0}^n \sum_{j \geqslant e-1} a_{i,j} p^{j-e+1} = p(l-r) - r_{e-1}$ and (ii) $\sum_{i=0}^n a_{i,j} = pr_{j+1} - r_j$ for all $0 \leqslant j \leqslant e-2$ with $r_0 = l - r$. In this case, we say that $(r_0, r_1, ..., r_{e-1})$ is the associated tuple of X^a.

LEMMA 2.4. *$X^a \in S^{l,0}_{n,e}$ if and only if there exist monomials $X^b \in R_{l(p-1)}$ and $X^c \in S^{l,0}_{n,e-1}$ such that $X^a = (X^b)^{p^{e-1}} X^c$.*

Proof. Let $X^a = X_0^{a_0} \cdots X_n^{a_n} \in S^{l,0}_{n,e}$ with associated tuple $(l, r_1, ..., r_{e-1})$. Choose integers b_i such that $lp - l = \sum_{i=0}^n b_i$ with $0 \leqslant b_i \leqslant \sum_{j \geqslant e-1} a_{i,j} p^{j-e+1}$. Let $X^c = X^a/(\prod (X_i^{b_i})^{p^{e-1}}) = X_0^{c_0} \cdots X_n^{c_n}$.

Then, $\sum_{i=0}^n \sum_{j \geqslant e-1} c_{i,j} p^{j-e+1} = l - r_{e-1}$ and $\sum_{i=0}^n \sum_{j \geqslant e-2} c_{i,j} p^{j-e+2} = lp - r_{e-2}$. Since $c_{i,j} = a_{i,j}$ for $0 \leqslant j \leqslant e-2$, we have $\sum_{i=0}^n c_{i,j} = r_{j+1} p - r_j$ for every $0 \leqslant j \leqslant e-3$. Hence $X^c \in S^{l,0}_{n,e-1}$ with associated tuple $(l, r_1, ..., r_{e-2})$.

Conversely, let $X^b = X_0^{b_0} \cdots X_n^{b_n} \in R_{l(p-1)}$, $X^c = X_0^{c_0} \cdots X_n^{c_n} \in S^{l,0}_{n,e-1}$ with associated tuple $(r_0, ..., r_{e-2})$ and $X^a = X^c (X^b)^{p^{(e-1)}} = X_0^{a_0} \cdots X_n^{a_n}$. Since $\sum_{i=0}^n \sum_{j \geqslant e-2} c_{i,j} p^{j-e+2} = lp - r_{e-2}$, $\sum_{i=0}^n \sum_{j \geqslant e-1} c_{i,j} p^{j-e+2} = rp$ and $\sum_{i=0}^n c_{i,e-2} = (l-r)\, p - r_{e-2}$ for some $0 \leqslant r \leqslant l-1$. Also, $\sum_{i=0}^n \sum_{j \geqslant e-1} a_{i,j} p^{j-e+1} = \sum_{i=0}^n \sum_{j \geqslant e-1} c_{i,j} p^{j-e+1} + \sum_{i=0}^n b_i = lp - (l-r)$. Moreover, $a_{i,j} = c_{i,j}$ for $j \leqslant e-2$. Hence $\sum_{i=0}^n a_{i,j} = r_{j+1} p - r_j$ for $0 \leqslant j \leqslant e-3$ and $\sum_{i=0}^n a_{i,e-2} = (l-r)\, p - r_{e-2}$. Thus $X^a \in S^{l,0}_{n,e}$ with associated tuple $(r_0, ..., r_{e-2}, l-r)$. ∎

THEOREM 2.5. *$C^n_{\mathbb{F}_q}(l, q)$ is the $\mathbb{F}_q$ span of $\mathbf{1}$ and the functions on P defined by elements of $S^{l,0}_{n,e}$.*

Proof. Let $M \in T^{\dagger}_{q-1}$ be a monomial. Then there exist monomials $M_0, ..., M_{e-1}$ in T_{p-1} such that $M = \prod_{j=0}^{e-1} (M_j)^{p^j}$ (See [6, p. 357].) Therefore, $\varphi_l(M) = \prod_{j=0}^{e-1} (\varphi_l(M_j))^{p^j}$. Now Lemmas 2.2 and 2.4 imply

$$S^{l,0}_{n,e} = \{\varphi_l(M) \mid M \in T^{\dagger}_{q-1},\ M \text{ a monomial}\}.$$

Proposition 2.1 now proves the theorem. ∎

We now determine distinct functions on P given by elements of $S^{l,0}_{n,e}$. Let I be the ideal in R generated by $X_i^q - X_i$ for $0 \leqslant i \leqslant n$ and $\prod_{i=0}^n (1 - X_i^{q-1})$. Then R/I is the ring of functions on P.

LEMMA 2.6 [6, Lemma 4]. *Let $f \in \mathbb{F}_q[Y_0, ..., Y_N]$ be a polynomial having degree at most $q-1$ in each of the variables. If f vanishes on $\mathbb{F}_q^{N+1}$ then f is the zero polynomial.*

DEFINITION 2.7. Let $S^{l,r}_{n,e}(q-1)$ denote the subset of $S^{l,r}_{n,e}$ consisting of elements all of whose exponents are at most $q-1$.

PROPOSITION 2.8. *For $1 \leqslant l \leqslant n$, $S^{l,r}_{n,e}$ and $S^{l,r+1}_{n,e} \cup S^{l,r}_{n,e}(q-1)$ define the same set of functions on P.*

Proof. Since $S^{l,l-1}_{n,e} = S^{l,l-1}_{n,e}(q-1)$, we assume that $r \leqslant l-2$. Let $X^a = X_0^{a_0} \cdots X_n^{a_n}$ be an element of $S^{l,r}_{n,e} \setminus S^{l,r}_{n,e}(q-1)$ with associated tuple $(r_0, ..., r_{e-1})$.

Without loss of generality, we may assume that $a_0 \geqslant q$. Then the monomials $X^b = X^a/X_0^{q-1}$ and X^a define the same function on P. We prove that $X^b \in S_{n,e}^{l,r+1}$.

Case 1. $a_{0,j} = p-1$ for $0 \leqslant j \leqslant e-1$. In this case, $r_1 \geqslant 2$ as $\sum_{i=0}^{n} a_{i,0} = pr_1 - (l-r) \geqslant p-1$ and $(l-r) \geqslant 2$. Similarly, $r_j \geqslant 2$ for all $1 \leqslant j \leqslant e-1$. Thus $X^b \in S_{n,e}^{l,r+1}$ with associated tuple $(r_0 - 1, ..., r_{e-1} - 1)$.

Case 2. $a_{0,j} < p-1$ for some $j \leqslant e-1$. Let $0 \leqslant t \leqslant e-1$ be the smallest integer such that $a_{0,t} < p-1$. As before, $r_j \geqslant 2$ for all $j \leqslant t$ and $b_{0,j} = 0$ for all $j \leqslant t-1$, $b_{0,t} = a_{0,t} + 1$, $b_{0,j} = a_{0,j}$ for all $t < j \leqslant e-1$. Also, $\sum_{j \geqslant e} b_{0,j} p^{j-e+1} = (\sum_{j \geqslant e} a_{0,j} p^{j-e+1}) - p$. Thus $X^b \in S_{n,e}^{l,r+1}$ with associated tuple $(r_0 - 1, ..., r_t - 1, r_{t+1}, ..., r_{e-1})$.

We now produce for every X^b in $S_{n,e}^{l,r+1}$ an element of $S_{n,e}^{l,r}$ which defines the same function as X^b on P. Let $(s_0, ..., s_{e-1})$ be the associated tuple of X^b and t be the smallest integer such that $p^t \nmid b_i$ for some i. We assume without loss of generality that b_0 is not divisible by p^t. We prove that $X^b X_0^{q-1} \in S_{n,e}^{l,r}$. Let $X^a = X^b X_0^{q-1}$. For $1 \leqslant j \leqslant \min\{t, e-1\}$, we have $s_j < (l-1)$ since $ps_{j+1} - s_j = 0$ and $s_0 \leqslant l$.

Case 1. $t \geqslant e-1$. In this case $\sum_{i=0}^{n} a_{i,j} = a_{0,j} = p-1$ for all $j < e-1$. Thus $X^a \in S_{n,e}^{l,r}$ with associated tuple $(s_0 + 1, ..., s_{e-1} + 1)$.

Case 2. $t \leqslant e-2$. We have $a_{0,j} = p-1$ for all $j \leqslant t-1$, $a_{0,t} = b_{0,t} - 1$ and $a_{0,j} = b_{0,j}$ for $t < j < e$. Thus $X^a \in S_{n,e}^{l,r}$ with associated tuple $(s_0 + 1, ..., s_t + 1, s_{t+1}, ..., s_{e-1})$. ∎

Lemma 2.6 and Proposition 2.8 imply

COROLLARY 2.9. *$\bigcup_{r=0}^{l-1} S_{n,e}^{l,r}(q-1)$ is a basis for $D_{\mathbb{F}_q}^n(l, q)$.*

DEFINITION 2.10. Let α and j be positive integers and let $N_{i\alpha-j,n}$ denote the number of monomials of degree $i\alpha - j$ in $(n+1)$ variables with all exponents less than α.

PROPOSITION 2.11. *For positive integers α and j,*

$$N_{i\alpha-j,n} = \sum_{r=0}^{i-1} (-1)^r \binom{n+1}{r} \binom{n+i\alpha-j-r\alpha}{n}.$$

Proof. If $a_i = k_i \alpha + r_i$ with $k_i \geqslant 0$, $0 \leqslant r_i \leqslant \alpha - 1$, then $X_0^{a_0} \cdots X_n^{a_n} = (X_0^{k_0} \cdots X_n^{k_n})^\alpha X_0^{r_0} \cdots X_n^{r_n}$. Thus, a degree $(s\alpha - j)$ monomial is uniquely a product of the α^{th} power of a monomial of degree $(s-r)$ and a monomial of degree $(r\alpha - j)$ whose exponents are less than α. Further $\binom{n+r}{r}$ is the number of monomials of degree r in $(n+1)$ variables. Hence for $1 \leqslant s \leqslant i$, we have

$$\binom{n+s\alpha-j}{n} = \sum_{r=1}^{s} \binom{n+s-r}{n} N_{r\alpha-j,n}.$$

Solution to this set of equations in variables $N_{r\alpha-j,n}$ is unique due to the invertibility of the matrix A whose (s,r)th entry is $\binom{n+s-r}{n}$ for $s \geqslant r$ and 0 otherwise. Thus to check the formula, we need to prove that

$$\sum_{r=0}^{i-1} (-1)^r \binom{n+1}{r} \binom{n+i\alpha-j-r\alpha}{n}$$
$$= \binom{n+i\alpha-j}{n} - \sum_{r=1}^{i-1} \binom{n+i-r}{n} \sum_{t=0}^{r-1} (-1)^t \binom{n+1}{t} \binom{n+r\alpha-j-t\alpha}{n}.$$

We compare the coefficients of $\binom{n-j+m\alpha}{n}$ for every $1 \leqslant m \leqslant i$. For $m=i$, the coefficient on both sides is 1. For $1 \leqslant m \leqslant i-1$, the coefficient of $\binom{n-j+m\alpha}{n}$ on the left side is $(-1)^{i-m} \binom{n+1}{i-m}$. The coefficient on the right side of the equation is $-\sum_{t=0}^{i-1-m} (-1)^t \binom{n+1}{t} \binom{n+i-t-m}{n}$. So we need to prove that $\sum_{t=0}^{i-m} (-1)^t \binom{n+1}{t} \binom{n+i-t-m}{n} = \frac{1}{n!} \sum_{t=0}^{i-m} (-1)^t \binom{n+1}{t} \prod_{r=1}^{n} (r+i-t-m) = 0$. That is, $u=i-m$ is a root of

$$\sum_{t=0}^{u} (-1)^t \binom{n+1}{t} \prod_{r=1}^{n} (X+r-t).$$

We can assume that $u \leqslant n+1$, since $\binom{n+1}{t}=0$ for all $t>n+1$. Also, for $u+1 \leqslant t \leqslant n+1$, $u+r=t$ for $1 \leqslant r \leqslant n$. Thus, u is a root of $\sum_{t=u+1}^{n+1} (-1)^t \binom{n+1}{t} \prod_{r=1}^{n} (X+r-t)$. Therefore, it is enough to show that u is a root of

$$P_n(X) = \sum_{t=0}^{n+1} (-1)^t \binom{n+1}{t} \prod_{r=1}^{n} (X+r-t).$$

However, $P_n(X)$ is the zero polynomial since the coefficient of X^{n-h} in $P_n(X)$ is a linear combination of sums $\sum_{t=0}^{n+1} t^g (-1)^t \binom{n+1}{t}$ for $0 \leqslant g \leqslant h$ and each of these sums is zero (by induction on g). ∎

COROLLARY 2.12. *The cardinality of* $S_{n,e}^{l,r}(q-1)$ *is*

$$\sum_{\substack{1 \leqslant r_1, \ldots, r_{e-1} \leqslant l \\ r_0 = r_e = l-r}} \prod_{j=0}^{e-1} \sum_{t=0}^{r_{j+1}-1} (-1)^t \binom{n+1}{t} \binom{n+pr_{j+1}-r_j-tp}{n}.$$

Proof. For X^a in $S^{l,r}_{n,e}(q-1)$ with associated tuple $(r_0, ..., r_{e-1})$, we have $\sum_{i=o}^n a_{i,j} = pr_{j+1} - r_j$ for $0 \leqslant j \leqslant e-1$ with $1 \leqslant r_1, ..., r_{e-1} \leqslant l$ and $r_0 = r_e = l - r$. The corollary now follows from the uniqueness of the p-adic expression of a_i and Proposition 2.11 with $\alpha = p$. ∎

Corollaries 2.9 and 2.12 imply:

THEOREM 2.13. *The dimension of $C^n_k(l, q)$ is*

$$1 + \sum_{i=1}^{l} \sum_{\substack{1 \leqslant r_1, ..., r_{e-1} \leqslant l \\ r_0 = r_e = i}} \prod_{j=0}^{e-1} \sum_{t=0}^{r_{j+1}-1} (-1)^t \binom{n+1}{t} \binom{n + pr_{j+1} - r_j - pt}{n}.$$

Remark 2.14. If $l = 1$, the dimension is $1 + \binom{p-1+n}{n}^e$. Since $C^n_k(1, q)$ is the hyperplane code, above formula thus agrees with the known formula.

3. THE IDENTIFICATION

In this section, we identify the code given by l hypersurfaces with the one given by $(n-l)$ flats in P. This identification generalizes Remark 2.14 and provides an alternative to Hamada's formula.

For an integer $a = \sum_{i=0}^{e-1} a_i p^i$, with $0 \leqslant a_i \leqslant p-1$ we define $[a] = a$, $[pa] = pa - a_{e-1}(q-1) = a_{e-1} + a_0 p + \cdots + a_{e-2} p^{e-1}$, and $[p^j a] = [p[p^{j-1}a]]$ for $2 \leqslant j \leqslant e-1$. Note that the coefficient of p^i in the p-adic expression of $[p^j a]$ is a_l where $l + j = i \bmod(e)$. For $X^a = X_0^{a_0} \cdots X_n^{a_n}$, we write $X^{[p^j a]}$ for $X_0^{[p^j a_0]} \cdots X_n^{[p^j a_n]}$. If $X^a \in S^{l.r}_{n,e}(q-1)$ with associated tuple $(r_0 = l - r, r_1, ..., r_{e-1})$ then, $X^{[pa]} \in S^{l, l-r_{e-1}}_{n,e}$ with associated tuple $(r_{e-1}, r_0, ..., r_{e-2})$. For $\alpha \in \mathbb{F}_q$, we have $\alpha^{[p^j a]} = \alpha^{p^j a}$, thus $X^{[p^j a]}$ and $X^{p^j a}$ define the same function on $\mathbb{F}_q^{n+1}$.

By Proposition 2.8, $S = \bigcup_{r=0}^{l-1} S^{l,r}_{n,e}(q-1)$ is a basis for $D^n_{\mathbb{F}_q}(l, q)$. Let B denote the subset of $D^n_{\mathbf{F}_q}(l, q)$ consisting of polynomials $\sum_{j=0}^{e-1} \alpha^{p^j} X^{[p^j a]}$, $\alpha \in \mathbb{F}_q$ and $X^a \in S$. Note that every element of B takes values in $\mathbb{F}_p$.

PROPOSITION 3.1. *B spans $D^n_{\mathbb{F}_p}(l, q)$.*

Proof. Let V denote the $\mathbf{F}_p$ span of B. We check that for $X^a \in S$, the dimension of the $\mathbf{F}_p$-span of $\{\sum_{j=0}^{e-1} \alpha^{p^j} X^{[p^j a]} \mid \alpha \in \mathbb{F}_q\}$ is the cardinality t of $\{X^{[p^j a]} \mid 0 \leqslant j \leqslant e-1\}$. Therefore, $\dim_{\mathbf{F}_p}(V) = \dim_{\mathbf{F}_q}(D^n_{\mathbb{F}_q}(l, q))$ and $D^n_{\mathbb{F}_p}(l, q) = V$.

Since the function X^a on $\mathbf{F}_q^{n+1}$ is same as $X^{[p^t a]} = X^{p^t a}$, it takes values in $\mathbf{F}_{p^t}$. Let $\alpha_1, ..., \alpha_t$ be a basis of $\mathbf{F}_{p^t}$ over $\mathbf{F}_p$ and $\beta_i \in \mathbb{F}_q$ be a preimage of α_i under the trace map from $\mathbb{F}_q$ to $\mathbb{F}_{p^t}$. Since the $\mathbf{F}_p$ linear map $\alpha \mapsto (\alpha, \alpha^p, ..., \alpha^{p^{t-1}})$ from $\mathbb{F}_{p^t} \to (\mathbb{F}_{p^t})^t$ is injective, it takes a $\mathbb{F}_p$ basis of

$\mathbb{F}_{p^t}$ to a linearly independent set. Therefore the set $\{\sum_{j=0}^{e-1} \beta_i^{p^j} X^{[p^j a]} = \sum_{j=0}^{t-1} \alpha_i^{p^j} X^{[p^j a]} \mid 1 \leqslant i \leqslant t\}$ is linearly independent. ∎

For convenience, we state a theorem of Delsarte; see for example [1, Theorem 5.7.3, Example 5.7.2, pp. 187–188].

PROPOSITION 3.2. *The $\mathbb{F}_p$-span of the incidence matrix of the design of points versus $(n-l)$ flats of P consists of functions on P defined by the polynomials $p(X_0, ..., X_n) = \sum_{l_0, l_1, ..., l_n} d(l_0, ..., l_n) X_0^{l_0} \cdots X_n^{l_n}$ in $\bigoplus_{l=1}^{\infty} R_{l(q-1)}$ such that $0 \leqslant l_i \leqslant q-1$, and for every $0 \leqslant j \leqslant e-1$*

1. $\sum_{i=0}^{n} [p^j l_i] \leqslant l(q-1)$.
2. $d([p^j l_0], ..., [p^j l_n]) = (d(l_0, ..., l_n))^{p^j}$.

THEOREM 3.3. $C_k^n(l, q) = \tilde{C}_k^n(n-l, q)$.

Proof. (A) We prove that $C_k^n(l, q) \subseteq \tilde{C}_k^n(n-l, q)$. See also [1, Theorem 5.7.7, Exercise 5.7.2, pp. 190–192] for $l=2$. It is enough to prove that $D_{\mathbb{F}_p}^n(l, q) \subseteq \tilde{C}_{\mathbb{F}_p}^n(n-l, q)$. The set B spans $D_{\mathbb{F}_p}^n(l, q)$ by Proposition 3.1. Since each element of B satisfies conditions of Proposition 3.2, inclusion follows.

(B) We show $C_{\mathbb{F}_p}^n(l, q) \supseteq \tilde{C}_{\mathbb{F}_p}^n(n-l, q)$ by induction on l. An l hypersurface which is a union of hyperplanes is called a *monomial l hypersurface*. For $1 \leqslant r \leqslant l-1$, the zero set of a monomial of degree r is also the zero set of a monomial of degree l. Thus a monomial l hypersurface under a change of variables is the zero set of a monomial of degree at most l.

We claim that the characteristic function χ_L of any $(n-l)$ flat L in P can be written as a $\mathbb{F}_p$ linear combination of characteristic functions of monomial l hypersurfaces all of whose irreducible components contain L.

For $l=1$, the statement is obvious. We now assume by way of induction that the statement is true for $(n-r)$ flats with $r \leqslant l-1$. Thus the characteristic function of any $(n-r)$ flat is a $\mathbb{F}_p$ linear combination of characteristic functions of monomial l hypersurfaces all of whose irreducible components contain L.

Any $(n-l)$ flat L can be written as an intersection of a hyperplane H and a $(n-l+1)$ flat L' such that $L' \nsubseteq H$. Thus, $\chi_L = \chi_{L'} + \chi_H - \chi_{L' \cup H}$. If $\chi_{L'} = \sum a_i \chi_{P_i}$, with each P_i a monomial $(l-1)$ hypersurface and $a_i \in \mathbb{F}_p$ then $P_i \cup H$ is a monomial l hypersurface and $\chi_{L' \cup H} = \sum a_i \chi_{P_i \cup H}$. Thus the claim.

Now Theorems 2.5 and 3.3 yield

COROLLARY 3.4. *If $k \supseteq \mathbb{F}_q$, $\tilde{C}_k^n(n-l, q)$ is generated by monomial functions.*

Remark 3.5. Theorem 3.3 and Corollary 3.4 are some of the consequences of much stronger results of Bardoe and Sin which describe all $GL(n+1)$

submodules of k^P using representation theory (see [2, Lemma 5.2 and Sect. 8]). However, our methods are different and elementary.

Remark 3.6. We note that unlike Hamada's formula, for fixed l and e, the number of terms in the formula of Theorem 2.13 is independent of n. Thus, asymptotically for fixed values of l and e, our formula is a simpler alternative to Hamada's formula.

When $q = p$, Theorems 2.13 and 3.3 imply

THEOREM 3.7. *The dimension of $\tilde{C}_k^n(n-l, p)$ is*

$$1 + \sum_{i=1}^{l} \sum_{t=0}^{i-1} (-1)^t \binom{n+1}{t} \binom{n+ip-i-tp}{n}.$$

Remark 3.8. When $q = p$, the only $GL(n+1, p)$ submodules of k^P are $\tilde{C}_k^n(l, p)$ for $0 \leqslant l \leqslant n$ together with the complement of $k.\mathbf{1}$ in them; see for example [2, Theorem A]. Thus taking orthogonal complements with respect to Hamming metric on k^P induces an isomorphism between $\tilde{C}_k^n(l, p)/\tilde{C}_k^n(l+1, p)$ and $\tilde{C}_k^n(n-l, p)/\tilde{C}_k^n(n-l+1, p)$. Therefore,

$$\tilde{C}_k^n(n-l, p) \simeq k\mathbf{1} \oplus \sum_{i=1}^{l} \tilde{C}_k^n(l-i, p)/\tilde{C}_k^n(l-i+1, p).$$

Thus Theorem 3.7 can also be obtained using above isomorphism and Hamada's formula for $\tilde{C}_k^n(l-i, p)/\tilde{C}_k^n(l-i+1, p)$.

4. GENERALIZED REED–MULLER CODES

In this section we use Proposition 2.11 to obtain a formula for the dimension of the v^{th} order generalized Reed–Muller code $R_{\mathbb{F}_q}(v, n+1)$. Recall that $R_{\mathbb{F}_q}(v, n+1)$ is the subspace of the space of functions from $\mathbb{F}_q^{n+1}$ to $\mathbb{F}_q$ defined by elements of $\bigoplus_{m=0}^{v} R_m$.

THEOREM 4.1. *Let $v = i_0 q - j_0$ with $0 \leqslant j_0 \leqslant q-1$, then*

$$\dim(R_{\mathbb{F}_q}(v, n+1)) = 1 + \sum_{r=1}^{i_0} \sum_{j=j_r}^{q-1} \sum_{t=0}^{r-1} (-1)^t \binom{n+1}{t} \binom{n+rq-j-tq}{n},$$

where $j_r = 0$ if $r < i_0$ and $j_{i_0} = j_0$.

Proof. The factor 1 corresponds to degree zero functions. For $1 \leqslant m \leqslant v$, we write $m = rq - j$ with $1 \leqslant r \leqslant i_0, j_r \leqslant j \leqslant q-1$ and use Proposition 2.11 with $\alpha = q$ to compute the number of monomials of degree m all of whose exponents are at most $q-1$. ∎

Remark 4.2. Note that for fixed q and v, number of terms in the above formula is independent of n unlike in [1, Theorem 5.4.1, p. 154].

5. SEGRE EMBEDDINGS

Let $R = \mathbb{F}_q[X_0, ..., X_n]$, $T = \mathbb{F}_q[Y_0, ..., Y_m]$ and $S = \mathbb{F}_q[Z_{ij} \mid 0 \leqslant i \leqslant n, 0 \leqslant j \leqslant m]$. The Segre embedding of $\mathbb{P}^n \times \mathbb{P}^m$ in $\mathbb{P}^{(n+1)(m+1)-1}$ is defined by the map

$$(a_0, ..., a_n, b_0, ..., b_m) \mapsto (a_i b_j),$$

where $a_i b_j$ occur in the lexicographic order on (i, j) (See [5, pp. 25]).

Let $S_k^{n,m}(q)$ (resp. $\tilde{S}_k^{n,m}(q)$) denote the k span of characteristic functions of the intersections of Segre embedding of $\mathbb{P}_q^n \times \mathbb{P}_q^m$ in $\mathbb{P}_q^{(n+1)(m+1)-1}$ with the hyperplanes (resp. complements of hyperplanes). The all one vector $\mathbf{1}$ on the Segre embedding is in $S_k^{n,m}(q)$. Therefore, $S_k^{n,m}(q) = k\mathbf{1} \oplus \tilde{S}_k^{n,m}(q)$. Let $\tilde{D}_k^n(n-1, q)$ denote the k span of the characteristic functions of the complement of hyperplanes in $\mathbb{P}_q^n$.

PROPOSITION 5.1. $\tilde{S}_k^{n,m}(q) = \tilde{D}_k^n(n-1, q) \otimes \tilde{D}_k^m(m-1, q)$ *and so has dimension* $(\binom{n+p-1}{p-1}\binom{m+p-1}{p-1})^e$.

Proof. We note that restriction of functions on $\mathbb{P}_q^{(n+1)(m+1)-1}$ to the Segre embedding is given by the graded ring homomorphism $s: S \to R \otimes T$ defined by $Z_{ij} \mapsto X_i Y_j$. Thus, $S_{\mathbb{F}_q}^{n,m}(q)$ consists of functions in $\mathbb{F}_q[X_0, ..., X_n, Y_0, ..., Y_m]$ which arise as restrictions of elements of $S_{q-1}^{\dagger}$. For a monomial M in S, we write $s(M) = s(M)_X s(M)_Y$ where $s(M)_X \in R$ and $s(M)_Y \in T$. Then, $M \in S_{q-1}^{\dagger}$ if and only if $s(M)_X \in R_{q-1}^{\dagger}$ and $s(M)_Y \in T_{q-1}^{\dagger}$. This proves that $\tilde{S}_k^{n,m}(q) = \tilde{D}_k^n(n-1, q) \otimes \tilde{D}_k^m(m-1, q)$. The dimension follows from Remark 2.14. ∎

Remark 5.2. When $n = m = 1$, the embedding of $\mathbb{P}_q^1 \times \mathbb{P}_q^1$ in $\mathbb{P}_q^3$ is the non-degenerate quadric given by $Z_{00}Z_{11} - Z_{01}Z_{10}$. In this case our formula (which gives the dimension to be $p^{2e} + 1$) agrees with the known formula. See [6, Example 1.2, p. 355].

APPENDIX

In this section we use Theorem 2.13 and Maple to compute the dimension $c_k^n(l, q)$ of $C_k^n(l, q)$, the code given by $(n-l)$ flats in $\mathbb{P}_q^n$.

$$c_k^n(1, p^e) = 1 + \binom{n+p-1}{n}^e$$

$$c_k^4(2, p^2) = 1 + \frac{1}{36}\, p^2(p+1)^2\,(9p^4 - 4p^3 + 8p^2 - 4p + 9)$$

$$c_k^n(2, 4) = 1 + \frac{1}{12}\,(n+2)(n+1)(3n^2 + n + 6)$$

$$c_k^n(3, 4) = \frac{(n+2)}{36}\,(n^5 + n^4 + 2n^3 + 17n^2 + 15n + 36)$$

$$c_k^n(4, 4) = 1 + \frac{(n+1)(n+2)}{2880}\,(5n^6 - 11n^5 + 25n^4 + 155n^3 + 210n^2 + 576n + 1440)$$

$$c_k^n(5, 4) = 1 + \frac{(n+1)}{302{,}400}\,(21n^9 - 91n^8 + 211n^7 + 1169n^6 + 4144n^5 + 4466n^4 + 65{,}464n^3 + 120{,}456n^2 + 257{,}760n + 302{,}400)$$

$$c_k^n(6, 4) = 1 + \frac{(n+2)(n+1)}{7{,}257{,}600}\,(15n^{10} - 181n^9 + 1406n^8 - 4986n^7 + 15{,}911n^6 - 183{,}549n^5 - 270{,}916n^4 - 2{,}409{,}044n^3 - 3{,}260{,}016n^2 - 1{,}146{,}240n + 3{,}628{,}800)$$

$$c_k^n(2, 9) = 1 + \frac{(n+1)^2}{2880}\,(5n^6 + 90n^5 + 473n^4 + 852n^3 + 1268n^2 + 1632n + 2880)$$

$$c_k^n(3, 9) = 1 + \frac{(n+3)(n+2)(n+1)}{3{,}628{,}800}\,(7n^9 + 252n^8 + 2508n^7 + 4998n^6 + 5313n^5 + 45{,}318n^4 + 157{,}052n^3 + 327{,}432n^2 + 364{,}320n + 604{,}800)$$

$$c_k^n(4, 9) = 1 + \frac{(n+2)(n+1)}{4{,}877{,}107{,}200}(3n^{14} + 207n^{13} + 4745n^{12} + 39{,}111n^{11} + 67{,}147n^{10} + 35{,}841n^9 + 3{,}019{,}995n^8 + 7{,}031{,}853n^7 + 57{,}976{,}822n^6 + 128{,}101{,}692n^5 + 282{,}873{,}560n^4 + 1{,}024{,}071{,}936n^3 + 1{,}891{,}398{,}528n^2 + 2{,}295{,}336{,}960n + 2{,}438{,}553{,}600).$$

REFERENCES

1. E. F. Assmus, Jr. and J. D. Key, "Designs and Their Codes," Cambridge Tracts in Mathematics, Vol. 103, Cambridge Univ. Press, Cambridge, UK, 1992.
2. M. Bardoe and P. Sin, The permutation modules for $GL(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, *J. London Math. Soc.*, to appear.
3. N. Calkin, J. D. Key, and M. J. De Resmini, Minimal weight and dimension formulas for some geometric codes, *Des. Codes Cryptogr.* **17** (1999), 105–120.
4. N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, *J. Sci. Hiroshima Univ. Ser. A-I* **32** (1968), 381–396.
5. J. Harris, "Algebraic Geometry, A First Course," Graduate Texts in Mathematics, Vol. 133, Springer-Verlag, Berlin/New York, 1992.
6. E. Moorhouse, Some p-ranks related to geometric structures, *in* "Proceedings of Conference in Honour of T. G. Ostro on Coding Theory," pp. 353–364, 1996.