Duality and support weight distributions

Hans Georg Schaathun, *Member, IEEE*

***Abstract*— We show how to compute the support weight distribution A_i^r for $r \geq k - d_2^\perp + 3$, where $d_2^\perp$ is the second minimum support weight of the dual code, provided the weight enumerator of the dual code is known.**

***Index Terms*— support weight distribution, dual code**

I. Introduction

We have observed some recent interest in the support weight distributions, particularly those of self-dual codes [2], [7]. Possibly, these parameters may lead to non-existence proofs, finally determining the highest minimum distance of self-dual codes with certain lengths. The original motivation for introducing the support weight distribution was to compute the weight enumerator for certain infinite classes of cyclic codes [3]. The weight enumerator in turn is used for the computation of error probabilities in error-control systems.

Kløve has previously shown how to compute the support weight distribution A_i^r, provided that we know $A_i^{r'}$ for $r' \leq r$ of the dual code. This result appears first in [5] and was formulated as a generalised MacWilliams identity in [6]. A different proof of this result appeared in [9].

In [8], we explored a relation between a code and the projective multiset corresponding to the dual code. In the sequel, we will use this relation to determine support weight distributions of high orders. Whereas previous results rely on solving a large set of equations, the MacWilliams type identities, we find formulaic expressions which are faster to compute.

We hope that this will take us one step towards the complete determination of support weight distributions of some self-dual codes, for instance the $[72, 36, 16]$ Type II code. It is not known whether this code exists or not.

II. Projective multisets and duality

There is a well-studied correspondence between projective multisets and linear codes. In its easiest description, the projective multiset is obtained by taking the columns of some generator matrix of the code, counting multiplicities [4]. We will keep this description in mind, but still develop a more mathematically rigorous description, which will aid us in the study of duality. This description follows the one presented in [8].

A. Vectors, Codes, and Multisets

A multiset is a collection of elements which are not necessarily distinct. More formally, we define a multiset γ on a set S as a map $\gamma : S \to \{0, 1, 2, \ldots\}$. The number $\gamma(s)$ is the number of occurrences of s in the collection γ. The map γ is always extended to the power set of S,

$$\gamma(S') = \sum_{s \in S'} \gamma(s), \quad \forall S' \subseteq S.$$

The number $\gamma(s)$ or $\gamma(S')$ is called the value of s or S'. The size of γ is the value $\gamma(S)$. We will be concerned with multisets of vectors. We will always keep the informal view of γ as a collection in mind.

We consider a fixed finite field F_q with q elements. A message word is a k-tuple over F_q, while a codeword is an n-tuple over F_q. Let M be a vector space of dimension k (the message space), and V a vector space of dimension n (the ambient space). The generator matrix G gives a linear, injective transformation $G : \mathsf{M} \to \mathsf{V}$, and the code C is simply the image under G.

The columns of G form a multiset γ_C on M. Two codes are said to be permutation equivalent if one is obtained from the other by reordering the columns of the generator matrix, and thus γ_C defines C up to permutation equivalence. Two codes are also equivalent if one can be obtained from the other by replacing a column $\mathbf{g}$ of G by $\alpha\mathbf{g}$ for some non-zero scalar α. Hence the code C can alternatively be defined by the projective multiset γ'_C obtained by mapping γ_C into $\mathsf{PG}(k-1, q)$, the projective geometry of dimension $k-1$ over F_q.

We say that two multisets γ_0 and γ_1 on M are equivalent if $\gamma_1 = \gamma_0 \circ \phi$ for some automorphism ϕ on M. Such an automorphism is given by $\phi : \mathbf{g} \mapsto \mathbf{g}A$ where A is a square matrix of full rank. Replacing each $\mathbf{g}_i$ by $\mathbf{g}_i A$ in the encoding function is equivalent to replacing the message $\mathbf{m}$ by $A\mathbf{m}$. In other words, equivalent multisets give different encoding, but they give the same code. This is an important observation, because it implies that the coordinate system on M is not essential.

Let $\mathcal{B} := \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ be the coordinate basis of V. The vectors may be considered as linear forms on V. There is a natural endomorphism $\mu : \mathsf{V} \to \mathsf{V}/C^\perp$, where $\mu(\mathbf{v}) = \mathbf{v} + C^\perp$. The elements of $\mathsf{V}/C^\perp$ are linear forms on C, and $\mu(\mathbf{e}_i)(\mathbf{c}) = \mathbf{g}_i\mathbf{m}$ whenever $\mathbf{c} = \mathbf{m}G$. So when C is identified with M, $\mathbf{g}_i$ will correspond to $\mu(\mathbf{e}_i)$, establishing an isomorphism between $\mathsf{V}/C^\perp$ and M and proving the following lemma.

Lemma 1: A code $C \subseteq \mathsf{V}$ is given by the vector multiset $\gamma_C := \mu(\mathcal{B})$ on $\mathsf{V}/C^\perp \cong \mathsf{M}$.

Given a collection $\{s_1, s_2, \ldots, s_m\}$ of vectors and/or subsets of a vector space V, we write $\langle s_1, s_2, \ldots, s_m \rangle$ for its span. In other words $\langle s_1, s_2, \ldots, s_m \rangle$ is the intersection of all subspaces containing $s_1, s_2, \ldots, s_m$.

B. Weights

We define the support $\chi(\mathbf{c})$ of $\mathbf{c} \in C$ to be the set of coordinate positions not equal to zero, that is

$$\chi(\mathbf{c}) := \{i \mid c_i \neq 0\}, \quad \text{where } \mathbf{c} = (c_1, c_2, \ldots, c_n).$$

The support of a subset $S \subseteq C$ is

$$\chi(S) = \bigcup_{\mathbf{c} \in S} \chi(\mathbf{c}).$$

The author is with Dept. Informatics, University of Bergen, Norway. Email: ⟨georg@ii.uib.no⟩. The work has been partially supported by the Research Council of Norway.

The weight (or support size) $w(S)$ is the cardinality of $\chi(S)$. The ith minimum support weight $d_i(C)$ is the smallest weight of an i-dimensional subcode $D_i \subseteq C$. The subcode D_i will be called a minimum i-subcode. The weight hierarchy of C is $(d_1(C), d_2(C), \ldots, d_k(C))$.

The support weight distribution of C is the set of parameters $\{A_i^r(C) : i = 1, \ldots, n; r = 0, \ldots, k\}$, where $A_i^r(C)$ is the number of r-dimensional subcodes of weight i.

The following lemma was proved in [4], and the remark is a simple consequence of the proof.

Lemma 2: There is a one-to-one correspondence between subcodes $D \subseteq C$ of dimension r and subspaces $U \subseteq \mathsf{M}$ of codimension r, such that $\gamma_C(U) = n - w(D)$.

Remark 1: Consider two subcodes D_1 and D_2, and the corresponding subspaces U_1 and U_2. We have that $D_1 \subset D_2$ is equivalent to $U_2 \subset U_1$.

We define $d_{k-r}(\gamma_C)$ such that $n - d_{k-r}(\gamma_C)$ is the largest value of an r-space $V_r \subseteq \mathsf{M}$. From Lemma 2 we get this corollary.

Corrollary 1: If C is a linear code and γ_C is the corresponding multiset, then $d_i(\gamma_C) = d_i(C)$.

C. Projective spaces and multisets

A submultiset $\gamma' \subseteq \gamma$ is a multiset with the property that $\gamma'(x) \le \gamma(x)$ for all x. If γ is a multiset on some vector space V, we define a cross-section of γ to be the restriction $\gamma|_U$ to some subspace $U \subseteq \mathsf{V}$. Cross-sections of projective multisets are defined in the same way.

In some cases it is easier to deal with cross-sections and their sizes, than with subspaces and their values. In particular, we have that $n - d_{k-r}(\gamma_C)$ is the size of the largest r-dimensional cross-section of γ_C.

Let

$$\begin{bmatrix} k \\ r \end{bmatrix} = \prod_{i=0}^{r-1} \frac{q^{k-i} - 1}{q^{r-i} - 1}$$

denote the number of distinct linear r-spaces containing the origin. The number of r-spaces containing a given m-space is given by $\begin{bmatrix} k-m \\ r-m \end{bmatrix}$.

The r-th generalised Singleton bound states that $d_r \le d_k - k + r$. The code is r-MDS if it meets this bound with equality.

Consider an m-space $\Pi_m \subseteq \mathsf{PG}(k-1, q)$. Let

$$\pi_{\Pi_m} : \mathsf{PG}(k-1, q) \backslash \Pi_m \to \mathsf{PG}(k-2-m, q)$$

be the projection map through Π_m. Let C' be the code corresponding to $\gamma_{C'} := \gamma_C \circ \pi^{-1}$. Note that C' has parameters $[n - \gamma_C(\Pi_m), k-1-m]$. Every r-space in $\mathsf{PG}(k-2-m, q)$ is the image of an $(r+m+1)$-space containing Π_m in $\mathsf{PG}(k-1, q)$. Hence

$$\Delta_r(C') \le \Delta_{r+m+1}(C) - \gamma_C(\Pi_m).$$

Hence, if Π_m has maximum value, then C' is $(k-1-m_1+m-2)$-MDS. Note that C' can be viewed as a subcode of C [1].

D. Duality

Write $(d_1, \ldots, d_k)$ for the weight hierarchy of C, and $(d_1^\perp, \ldots, d_{n-k}^\perp)$ for the weight hierarchy of $C^\perp$. Let $B \subseteq \mathcal{B}$. Then $\mu(B)$ is a submultiset of γ_C. Every submultiset of γ_C is obtained this way. Obviously $\dim\langle B\rangle = \#B$. Let $D := \langle B\rangle \cap C^\perp$ be the largest subcode of $C^\perp$ contained in $\langle B\rangle$. Then D is the kernel of $\mu|_{\langle B\rangle}$, the restriction of μ to $\langle B\rangle$. Hence

$$\dim\langle\mu(B)\rangle = \dim\langle B\rangle - \dim D. \tag{1}$$

Clearly $\#B \ge w(D)$.

We are particularly interested in the case when when $\mu(B)$ is a cross-section of $\mu(\mathcal{B})$. This is of course the case if and only if $\mu(B)$ equals the cross-section $\mu(\mathcal{B})|_{\langle\mu(B)\rangle}$.

Let $U \subseteq \mathsf{V}/C^\perp$ be a subspace. We have $\mu(\mathcal{B})|_U = \mu(B)$, where $B = \{\mathbf{e} \in \mathcal{B} \mid \mu(\mathbf{e}) \in U\}$. Hence we have $\mu(B) = \mu(\mathcal{B})|_{\langle\mu(B)\rangle}$ if and only if there exists no point $\mathbf{e} \in \mathcal{B}\backslash B$ such that $\mu(\mathbf{e}) \in \langle\mu(B)\rangle$.

It follows from (1) that a large cross-section $\mu(B)$ of a given dimension, must be such that $\langle B\rangle$ contains a large subcode of $C^\perp$ of sufficiently small weight.

Define for any subcode $D \subseteq C^\perp$,

$$\beta(D) := \{\mathbf{e}_x \mid x \in \chi(D)\} \subseteq \mathcal{B}.$$

Obviously $\beta(D)$ is the smallest subset of $\mathcal{B}$ such that D is contained in its span. It follows from the above argument that if D is a minimum subcode and $\mu(\beta(D))$ is a cross-section, then $\mu(\beta(D))$ is a maximum cross-section for C. Thus we are lead to the following two lemmata.

Lemma 3: If $n - d_r = d_i^\perp$, $B \subseteq \mathcal{B}$, and $\#B = n - d_r$, then $\mu(B)$ is a cross-section of maximum size and codimension r if and only $B = \beta(D_i)$ for some minimum i-subcode $D_i \subseteq C^\perp$.

Lemma 4: Let r be an arbitrary number, $0 < r \le n - k$. Let i be such that $d_i^\perp \le n - d_r < d_{i+1}^\perp$, and let $D_i \subseteq C^\perp$ be a minimum i-subcode. Then $\mu(\langle B\rangle)$ is a maximum r-subspace for any $B \subseteq \mathcal{B}$ such that $D_i \subseteq \langle B\rangle$ and $\#B = n - d_r$.

E. Support weight distributions

Let $\mathfrak{V}_i^r(C)$ be the set of all r-spaces of value i, i.e.

$$\mathfrak{V}_i^r(C) := \{\Pi \subseteq \mathsf{PG}(k-1, q) \mid \gamma_C(\Pi) = i, \dim\Pi = r\}.$$

We define the *value distribution* of γ_C to be

$$V_i^r(\gamma_C) = V_i^r(C) := \#\mathfrak{V}_i^r(C). \tag{2}$$

By Lemma 2, each element of $\mathfrak{V}_i^r(C)$ corresponds to a $k-1-r$-dimensional subcode of weight $n-i$. Hence $V_i^r(C) = A_{n-i}^{k-1-r}(C)$.

We will mostly abbreviate and write $V_i^r = V_i^r(C)$, $A_i^r = A_i^r(C)$, $\tilde{A}_i^r = A_i^r(C^\perp)$, and $\tilde{V}_i^r = V_i^r(C^\perp)$. Define

$$m_i = m_i(C) := d_i(C^\perp) - i - 1.$$

Obviously $m_0 = -1$ and $m_{n-k} = k - 1$. We will determine V_i^r for $m_j \le r < m_{j+1}$ for $j = 0$ and $j = 1$. We start with a relatively simple result.

Lemma 5: If $m_{j+1} > m_j$, then

$$V^{m_j}_{m_j+j+1} = \tilde{A}^j_{m_j+j+1},$$
$$V^{m_j}_i = 0, \quad i > m_j + j + 1.$$

Proof: Consider an m_j-space Π for some j where $m_{j+1} > m_j$. From Lemma 3 we know that Π has value $d^\perp_j = m_j + j + 1$ if and only if it contains $\mathbf{x}_i$ for all $i \in \chi(D)$ where $D \subseteq C^\perp$ is a j-dimensional subcode of weight $d^\perp_j$. This gives the first equation. The second equation is obvious. ∎

The difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ is defined by $\delta_i = d_{k-i} - d_{k-1-i}$, and is occasionally more convenient than the weight hierarchy. The maximum value of an r-dimensional, projective subspace is $\Delta_r = \delta_0 + \ldots + \delta_r = n - d_{k-1-r}$.

III. The new results

The following theorem was proved in [5].

Theorem 1: For $-1 \le r < m_1$, and any code C, we have that $V^r_i(C) = \mathcal{V}^r_j(n,k)$ where

$$\mathcal{V}^r_j(n,k) = \binom{n}{j} \sum_{i=0}^{r-j+1} (-1)^i \begin{bmatrix} k-j-i \\ r-j+1-i \end{bmatrix} \binom{n-j}{i},$$

for any code C.

Our result is the determination of $V^i_r(C)$ when $m_1 \le r < m_2$. We know that $V^r_i = 0$ for all $i > r+2$.

Consider an r-space Π of value $r+2$. The cross-section $\gamma_C|_\Pi$ defines an $[r+2, r+1]$ code C'. Let $s := m_1(C')$. We say that Π has Type s. Clearly $m_1 \le s \le r$. The set of r-spaces of Type s is denoted by $\mathfrak{S}(r,s)$.

Given an r-space Π' of value $i \le r+1$, we say that Π' is Type I if it contains a $(i-2)$-space Π'' of value i. This $(i-2)$-space is unique when it exists. Clearly Π'' has Type s for some s, and then we say that Π' is Type I(s).

If Π' is not Type I, we say that it is Type II, and then it contains a unique $(i-1)$-space of value i. Let $\mathfrak{U}^r_i(X)$ be the set of r-spaces of value i and Type X, where X is I, II, or I(s) for some s. Write $U^r_i(X) := \#\mathfrak{U}^r_i(X)$.

A. Subspaces of Maximum Value

If C is an $[n, n-1]$ code, there is a unique s such that $\delta_s(C) = 2$, and $\delta_i(C) = 1$ for $i \ne s$. Clearly $m_1(C) = s$. In this case, we call C an $[n, n-1]$ code of Type s.

Lemma 6: Let γ_C be a projective multiset defining an $[n, n-1]$ code C of Type s. Then there is a unique s-space Π_s of value $s+2$.

Proof: There exists at least one such s-space since $s = m_1 = \Delta_s(C) - 2$. Suppose there are two distinct s-spaces Θ_1 and Θ_2 of value $s+2$. Let i be the dimension of $\Theta := \Theta_1 \cap \Theta_2$. Clearly $i < s$ and thus $\gamma_C(\Theta) \le i+1$. We get

$$\gamma(\langle \Theta_1, \Theta_2 \rangle) \ge 2(s+2) - (i+1) = 2s - i + 3,$$

but

$$\dim \langle \Theta_1, \Theta_2 \rangle = 2s - i = 2s - i,$$

so

$$\gamma(\langle \Theta_1, \Theta_2 \rangle) \le \Delta_{2s-i}(C) = 2s - i + 2.$$

The lemma follows by contradiction. ∎

There is only one $[n, n-1]$ code of Type s up to equivalence. The corresponding projective multiset is obtained by taking a frame for a projective s-space and then adding projectively independent points to obtain an $(n-2)$-space.

Lemma 7: For any code C, if $m_1 \le s \le r < m_2$, we have

$$\#\mathfrak{S}(r,s) = \tilde{A}^1_{s+2} \binom{n-s-2}{r-s}.$$

Proof: The number of maximum r-spaces of Type $r = s$ is

$$\#\mathfrak{S}(s,s) = \tilde{A}^1_{s+2}, \tag{3}$$

by Lemma 5.

An r-space Π_r of Type s contains a unique s-space Π_s of value $s+2$ by Lemma 6. Hence there is a one-to-one correspondence between r-spaces of Type s and pairs (Π_s, S) where $\Pi_s \in \mathfrak{S}(s,s)$ and $S \subset \gamma_C \backslash \Pi_s$ is a set of $r-s$ points. There are $\tilde{A}^1_{s+2}$ ways to choose Π_s by (3) and $\binom{n-s-2}{r-s}$ ways to choose S. Hence we get the result. ∎

Lemma 8: If $m_1 \le r < m_2$, then

$$V^r_{r+2} = \sum_{s=m_1}^{r} \tilde{A}^1_{s+2} \binom{n-s-2}{r-s},$$
$$V^r_i = 0, \quad i > r+2.$$

Proof: An r-space of value $r+2$ has Type s for some s where $m_1 \le s \le r$. Thus we can take the sum of the equation in Lemma 7. Hence the result. ∎

B. When $n = k+1$

In this section we study an $[n, n-1]$ code C of Type s. We will need the number $\mathcal{F}(j,n,s) := U^{n-3}_j(\mathrm{II})$ for C in the later sections.

We obviously have that $\mathcal{F}(j,n,s) = 0$ if $j \ge n-1$. When $n = s+2$, C is MDS, so

$$\mathcal{F}(j, s+2, s) = \mathcal{V}^{s-1}_j(s+2, s+1). \tag{4}$$

Lemma 9: For any $[n, n-1]$ code of Type s, if $j \le n-2$, then $U^{n-3}_j(\mathrm{II})$ is given by

$$\mathcal{F}(i,n,s) = \sum_{j=0}^{i} \mathcal{V}^{s-1}_j(s+2, s+1) \binom{m}{i-j} (q-1)^{m-i+j},$$

where $m = n-s-2$.

Proof: Note that if $n = s+2$, the lemma reduces to (4).

We consider the projective space $\mathsf{PG}(n-2, q)$. We want to find the number $\mathcal{F}(i,n,s)$ of hyperplanes of value i and Type II. Consider an arbitrary such hyperplane Π. There is a unique s-space $\Theta \subseteq \mathsf{PG}(n-2,q)$ of value $s+2$. Every hyperplane must meet Θ in a subspace of dimension $s-1$ or more. Since Π has Type II, $\Theta' := \Theta \cap \Pi$ is exactly an $(s-1)$-space. Let $j = \gamma_C(\Theta')$.

Given j ($0 \le j \le s$), there are $\mathcal{F}(j, s+2, s)$ ways to choose Θ'. Let $\Pi' \subseteq \Pi$ be the smallest subspace of value i and containing Θ'. Given Θ', we find Π' by choosing $i-j$ points among the $n-s-2$ points of positive value not contained in Θ. Given j, there are thus

$$\mathcal{F}(j, s+2, s) \binom{n-s-2}{i-j} = \mathcal{V}^{s-1}_j(s+2, s+1) \binom{n-s-2}{i-j}$$

ways to choose Π'.

Consider now the projection $\pi_{\Pi'}$. The multiset $\gamma'' := \gamma_C \circ \pi_{\Pi'}^{-1}$ defines an $[n-i, n-1-s-i+j]$ code. There is but one point x of value $\gamma''(x) = s+2-j$, namely $x = \pi_{\Pi'}(\Theta)$. The remaining points have value 0 or 1. We define a new projective multiset γ' by $\gamma'(x) = 1$ and $\gamma'(y) = \gamma''(y)$ for $y \neq x$. The corresponding code is a projective $[n', n']$ code where $n' = n-i-s-1+j$.

Finding $\Pi \geqq \Pi'$ of value i is the same as finding a hyperplane of zero value for γ', which is the same as counting one-dimensional subcodes of weight n' for the $[n', n']$ code. This number is $(q-1)^{n'-1}$. The lemma follows by summing over all j. ■

C. Other subspaces

Now we return to the general $[n,k]$ code C, in order to determine V_j^r for $j \leq r+1$.

Proposition 1: For $m_1 \leq r < m_2$ and $r \geq i-2$, we have

$$U_i^r(\mathrm{I}(s)) = \mathcal{V}_0^{r+1-i}(n-i, k+1-i)\tilde{A}_{s+2}^1 \binom{n-s-2}{i-s-2},$$
$$U_i^r(\mathrm{I}) = \mathcal{V}_0^{r+1-i}(n-i, k+1-i) V_i^{i-2}.$$

For $r < i-2$, we have $U_i^r(\mathrm{I}) = U_i^r(\mathrm{I}(s)) = 0$.

Proof: We have from Lemma 7, that

$$U_i^{i-2}(\mathrm{I}(s)) = \tilde{A}_{s+2}^1 \binom{n-s-2}{i-2-s}.$$

An r-space of value i and Type s contains a unique $(i-2)$-space Π' of value i and Type s. There are $U_i^{i-2}(\mathrm{I}(s))$ ways to choose Π'.

Consider then the multiset $\gamma' := \gamma_C \circ \pi_{\Pi'}^{-1}$ obtained by projection through Π'. We know that γ' defines an $[n-i, k+1-i]$ code C'. Finding an r-space $\Pi \geqq \Pi'$ of value i corresponds to finding an $(r+1-i)$-space of value 0 for γ'. Furthermore γ' defines a code with

$$\Delta_{m_2-i}(C') \leq \Delta_{m_2-1}(C) - i = m_2 + 1 - i.$$

Hence C' is $(k-1-m_2+i)$-MDS, and since $r+1-i \leq m_2 - i$, there are $\mathcal{V}_0^{r+1-i}(n-i, k+1-i)$ ways to choose $\Pi \geqq \Pi'$. This proves the first equation, and the second one follows by summing over all s. ■

Proposition 2: If $m_1 < j \leq m_2$, we have

$$U_j^{j-1}(\mathrm{II}) = \binom{n}{j} - U_j^{j-2}(\mathrm{I}) - \sum_{s=m_1}^{j-1} (s+2) U_{j+1}^{j-1}(\mathrm{I}(s)).$$

For $i > j$, we have $U_i^{j-1}(\mathrm{II}) = 0$.

Proof: We consider all the $\binom{n}{j}$ possible ways to chose a set S of j points of positive value. To find $U_j^{j-1}(\mathrm{II})$, we must subtract the number of cases where these j points generate a subspace of Type I.

Since $j-1 < m_2$, we have three cases:

1) $\dim\langle S\rangle = j-1$ and $\gamma_C(\langle S\rangle) = j$. (Type II)
2) $\dim\langle S\rangle = j-2$ and $\gamma_C(\langle S\rangle) = j$. (Type I)
3) $\dim\langle S\rangle = j-1$ and $\gamma_C(\langle S\rangle) = j+1$. (Type I)

The number of sets S giving the first case is $U_j^{j-1}(\mathrm{II})$, while for the second case, it is $U_j^{j-2}(\mathrm{I})$. The third case is more difficult, because S does not contain all points of positive value in $\langle S\rangle$. Suppose $\langle S\rangle$ has Type s. Then $\langle S\rangle$ can be chosen in $U_{j+1}^{j-1}(\mathrm{I}(s))$ different ways. There is one point $x \notin S$ of positive value in $\langle S\rangle$, and x must be contained in the unique s-space $\Pi_s \subseteq \langle S\rangle$ of value $s+2$. Moreover x can be any point of positive value in Π_s, hence there are $s+2$ different choices for S giving the same $\langle S\rangle$ of the third case. This gives the lemma. ■

Let

$$\begin{aligned}&\mathfrak{U}(r_1, v_1, X_1; r_2, v_2, X_2)\\ =&\{(\Pi_1, \Pi_2) \mid \Pi_1 \subseteq \Pi_2, \Pi_j \in \mathfrak{U}_{v_j}^{r_j}(X_j), j = 1, 2\}.\end{aligned}$$

We will write $v_j = *$ resp. $X_j = *$, when we allow any value of v_j resp. X_j.

Lemma 10: If $m_1 \leq r < m_2$ and $0 \leq j \leq r$, then

$$U_j^r(\mathrm{II}) = \frac{q-1}{q^{r+1-j}-1}\left(U_j^{r-1}(\mathrm{II})\frac{q^{k-r}-1}{q-1} - \sum_{v=j+1}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *)\right).$$

Proof: We will count the number of elements of $\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II})$ in two different ways. Consider a pair

$$(\Pi', \Pi) \in \mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II}).$$

There are $U_j^r(\mathrm{II})$ ways to choose Π. For Π', we can choose any $(r-1)$-space containing the unique $(j-1)$-space of value j in Π. Hence

$$\begin{aligned}\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II}) &= U_j^r(\mathrm{II}) \begin{bmatrix} r+1-j \\ r-j \end{bmatrix} \\ &= U_j^r(\mathrm{II}) \frac{q^{r+1-j}-1}{q-1}.\end{aligned} \tag{5}$$

This gives the first of the two expressions we seek.

Now we observe that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, *, *) = \sum_{v=j}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *). \tag{6}$$

This number can equivalently be obtained by counting the number of $(r-1)$-spaces of value j and Type II, and the number of r-spaces containing each such space. This gives

$$\begin{aligned}\#\mathfrak{U}(r-1, j, \mathrm{II}; r, *, *) &= U_j^{r-1}(\mathrm{II}) \begin{bmatrix} k-r \\ 1 \end{bmatrix} \\ &= U_j^{r-1}(\mathrm{II}) \frac{q^{k-r}-1}{q-1}.\end{aligned} \tag{7}$$

Clearly we have that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{I}) = 0,$$

and if we combine this with with (6) and (7), we get

$$\begin{aligned}\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II}) = U_j^{r-1}(\mathrm{II}) &\frac{q^{k-r}-1}{q-1} \\ &- \sum_{v=j+1}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *),\end{aligned}$$

which is our second expression for $\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j, \mathrm{II})$. Combining this with (5), we get the lemma. ■

Lemma 11: If $j < v - 1$, then

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{I}(s)) = U_v^r(\mathrm{I}(s))\mathcal{F}(j, v, s)q^{r+2-v}.$$

Proof: Consider a pair

$$(\Pi', \Pi) \in \mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{I}(s)).$$

There are $U_v^r(\mathrm{I}(s))$ ways to choose Π. There is a unique $(v-2)$-space $\Theta \subseteq \Pi$ of value v and Type s. The intersection $\Theta' := \Pi' \cap \Theta$ is a $(v-3)$-space of value j. There are $\mathcal{F}(j, v, s)$ ways to choose Θ'.

Consider the projection $\pi_{\Theta'}$. Finding Π' is the same as finding a hyperplane in $\operatorname{im} \pi_{\Theta'}$ not meeting $\pi_{\Theta'}(\Theta)$, which is a point. There are $(q^{r+3-v} - 1)/(q-1)$ hyperplanes in $\operatorname{im} \pi_{\Theta'}$, of which $(q^{r+2-v} - 1)/(q-1)$ meet $\pi_{\Theta'}(\Theta)$. Hence there are q^{r+2-v} hyperplanes not meeting $\pi_{\Theta'}(\Theta)$. ■

Lemma 12: If $j < v$, then

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{II}) = U_v^r(\mathrm{II})\mathcal{V}_j^{v-2}(v, v)q^{r+1-v}.$$

Proof: Consider a pair

$$(\Pi', \Pi) \in \mathfrak{U}(r-1, j, \mathrm{II}; r, v, \mathrm{II}).$$

There are $U_v^r(\mathrm{II})$ ways to choose Π. There is a unique $(v-1)$-space $\Theta \subseteq \Pi$ of value v, and $\gamma_C|_\Theta$ defines a $[v, v]$ code. The intersection $\Theta' := \Pi' \cap \Theta$ is a $(v-2)$-space of value j. There are $\mathcal{V}_j^{v-2}(v, v)$ ways to choose Θ'.

Consider the projection $\pi_{\Theta'}$. Finding Π' is the same as finding a hyperplane in $\operatorname{im} \pi_{\Theta'}$ not meeting $\pi_{\Theta'}(\Theta)$, which is a point. There are q^{r+1-v} such hyperplanes. ■

We define for brevity:

$$\mathfrak{F}(r, j) := \sum_{v=j+1}^{r+2} \#\mathfrak{U}(r-1, j, \mathrm{II}; r, v, *).$$

Proposition 3: We have

$$\mathfrak{F}(r, j) = \sum_{v=j+2}^{r+2} q^{r+2-v}\Bigg[U_{v-1}^r(\mathrm{II})\mathcal{V}_j^{v-3}(v-1, v-1) + \sum_{s=m_1}^{r} U_v^r(\mathrm{I}(s))\mathcal{F}(j, v, s)\Bigg].$$

Proof: First note that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, r+2, \mathrm{II}) = 0,$$

because $U_{r+2}^r(\mathrm{II}) = 0$, and that

$$\#\mathfrak{U}(r-1, j, \mathrm{II}; r, j+1, \mathrm{I}) = 0,$$

because there is no subspace of value j in a subspace of value $j+1$ and Type I. Now the result follows from Lemmata 11 and 12. ■

Proposition 4: If $m_1 \le r < m_2$ and $0 \le j \le r$, then

$$U_j^r(\mathrm{II}) = \frac{q^{k-r} - 1}{q^{r+1-j} - 1}U_j^{r-1}(\mathrm{II}) - \frac{q-1}{q^{r+1-j} - 1}\mathfrak{F}(r, j),$$

where $\mathfrak{F}(r, j)$ is given by Proposition 3.

Proof: This is simply a rephrase of Lemma 10. ■

If we combine all the results of this paper, we get the following theorem as a conclusion.

Theorem 2: For $k \ge r > k + 2 - d_2(C^\perp)$, it is possible to compute $A_i^r(C)$ for all i provided we know the (first) weight enumerator of $C^\perp$. We have for $k + 1 - d_1(C^\perp) < r \le k$, that

$$A_i^r(C) = \binom{n}{n-i} \sum_{j=0}^{k+i-r-n} (-1)^j \begin{bmatrix} k-n+i-j \\ k-r-n+i-j \end{bmatrix} \binom{i}{j},$$

and for $k + 2 - d_2(C^\perp) < r \le k + 1 - d_1(C^\perp)$, that

$$A_i^r(C) = U_{n-i}^{k-1-r}(\mathrm{II}) + U_{n-i}^{k-1-r}(\mathrm{I}),$$

where $U_{n-i}^{k-1-r}(\mathrm{II})$ and $U_{n-i}^{k-1-r}(\mathrm{I})$ are given by Propositions 1, 2 and 4.

IV. Discussion of future works

We have found formulæ for computing some high order support weight distributions. The formulæ are good for electronic computation of the parameters, and for instance computing the third through the 24th support weight distribution of the $[24, 12]$ Golay code is a matter of seconds. On the other hand, simplified formulæ more comprehensible to human readers would definitely be an improvement.

It will not be too difficult to continue and compute $A_i^r(C)$ for

$$k - d_2^\perp + 2 \ge r > k + 3 - \min\{d_3^\perp, 2d_1^\perp\},$$

provided the second support weight distribution of $C^\perp$ is known. We have omitted these results, because they would be too tedious, without adding significantly to the understanding of the subject.

To go below $k + 3 - 2d_1^\perp$ is more difficult, because if $i \ge 2d_1^\perp$, we may have a codeword $\mathbf{c} \in C^\perp$ and a subcode $D \subseteq C^\perp$ of dimension more than one, such that $\chi(\mathbf{c}) = \chi(D)$. This codeword $\mathbf{c}$ will be counted in $\tilde{A}_i^1$, but for computing A_j^r, only D should be counted. It is a long way to making a general statement for $r \le k + r - 2d_1^\perp$, but in special cases there may be possibilities.

We have tried to compute support weight distributions of the tentative $[72, 36]$ Type II self-dual code. By combining Theorems 1 and 2 with the MacWilliams-Kløve identities, we are left with about 100 unknowns. There is a chance that this system may be solved completely by extending the techniques presented here, and combining it with all the techniques found in the literature. That will be extensive labour in itself, so we leave it to future works.

Acknowledgement

This work was inspired by Steven Dougherty's talk at WCC in Paris January 2001. Private correspondence with Aaron Gulliver, coauthor of the mentioned talk, has been very valuable during the research. Finally, Torleiv Kløve is thanked for his continuous advice as a supervisor, concerning presentation and publication, and also for his help in finding and understanding [5].

REFERENCES

[1] S. Dodunekov and J. Simonis, "Codes and projective multisets," *Electron. J. Combin.*, vol. 5, no. 1, 1998, research Paper 37.

[2] S. Dougherty, A. Gulliver, and M. Oura, "Higher weights and graded rings for binary self-dual codes," *Discrete Applied Mathematics*, vol. 128, pp. 251–261, 2003, special issue for WCC 2001.

[3] T. Helleseth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/n)$," *Discrete Math.*, vol. 18, pp. 179–211, 1977.

[4] T. Helleseth, T. Kløve, and Ø. Ytrehus, "Generalized Hamming weights of linear codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 1133–1140, 1992.

[5] T. Kløve, "The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$," *Discrete Math.*, vol. 23, pp. 159–168, 1978.

[6] ——, "Support weight distribution of linear codes," *Discrete Math.*, vol. 106/107, pp. 311–316, 1992.

[7] O. Milenkovic, "On the generalized Hamming weight enumerators and coset weight distributions of even isodual codes," in *Proc. IEEE Intern. Symp. Inform. Theory*, June 2001, p. 62.

[8] H. G. Schaathun, "Duality and greedy weights for linear codes and projective multisets," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Springer Lecture Notes in Computer Science, vol. 2227. Springer-Verlag, Nov. 2001, pp. 92–101.

[9] J. Simonis, "The effective length of subcodes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 5, no. 6, pp. 371–377, 1994.

BIOGRAPHY, HANS GEORG SCHAATHUN

Hans Georg Schaathun was born in Bergen, Norway, in 1975. He received a Cand.Mag. degree with mathematics from the University of Bergen in 1996. He is Cand.Scient. 1999 and Dr.Scient 2002 from the Department of Informatics at the University of Bergen. During 2002 he was a lecturer, and from 2003 he is a post-doctoral researcher at this university. He has been at research stays at ENST in Paris 2000/2001 and at the Royal Holloway, University of London 2003/2004.

His research interest include codes for digital fingerprinting and higher weights of linear codes.