REPORTS IN INFORMATICS

ISSN 0333-3590

On the second greedy weight for linear codes of dimension at least 4

Wende Chen and Torleiv Kløve

REPORT NO 252 August 2003

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL http://www.ii.uib.no/publikasjoner/texrap/ps/2003-252.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

On the second greedy weight for linear codes of dimension at least 4

Wende Chen,
Laboratory of Systems and Control, Center of Information Security,
Institute of Systems Science, Academy of Mathematics and Systems Science,
Chinese Academy of Science, Beijing 100080, China.

Torleiv Kløve,
The Selmer Center, Department of Informatics, University of Bergen,
HIB, N-5020 Bergen, Norway.

Abstract

The maximum of $g_2 - d_2$ for linear $[n, k, d; q]$ codes $\mathcal{C}$ is studied. Here d_2 is the smallest size of the support of a 2-dimensional subcode of $\mathcal{C}$ and g_2 is the smallest size of the support of a 2-dimensional subcode of $\mathcal{C}$ which contains a codeword of weight d. For codes of dimension 4 or more, upper and lower bounds on the maximum of $g_2 - d_2$ are given.

1 Introduction

Ozarow and Wyner [7] suggested one application of linear codes to cryptology, namely to the wire-tap channel of type II. For this channel, an adversary is assumed to be able to tap s bits (of his choice) of n bits transmitted. The goal for the sender is to encode k bits of information into n transmitted bits in such a way that the adversary gets as little information as possible.

One of their schemes was to use the dual of an $[n, k; q]$ binary linear code $\mathcal{C}$. The code has q^k cosets, each representing a k-tuple. If the sender wants to transmit k symbols of information to the receiver, he selects a random vector in the corresponding coset. The channel is assumed to be noiseless, so the receiver can determine the corresponding coset of the received vector. It is assumed the adversary has full knowledge of the code, but not of the random selection of a vector in a coset.

In his studies of this scheme, Wei [8] introduced a set of parameters of a linear code which he called the generalized Hamming weights. The same parameters had also been studied previously in another context [5] and has since proved important in still other contexts.

For any code $\mathcal{D}$, let $\chi(\mathcal{D})$, the *support* of $\mathcal{D}$, be the number of positions where not all the codewords of $\mathcal{D}$ are zero. For an $[n, k; q]$ code $\mathcal{C}$ and any r, where $1 \le r \le k$, Wei defined

$$d_r(\mathcal{C}) = \min\{|\chi(\mathcal{D})| \mid \mathcal{D} \text{ is an } [n, r; q] \text{ subcode of } \mathcal{C}\}.$$

In particular, the minimum distance of $\mathcal{C}$ is $d_1(\mathcal{C})$.

For the Ozarow-Wyner scheme, it was shown by Wei [8] that the adversary can obtain r symbols of information if and only if $s \ge d_r(\mathcal{C})$.

Cohen et al. [4] considered the following variation of the problem. The adversary is greedy. He first reads $d = d_1$ positions to obtain one symbol of information as soon as possible. He then reads a minimal number of further positions to get one additional symbol of information and so on. Let g_r denote the minimal number of symbols he has to read to get r symbols of information in this way. In particular, g_2 is the smallest support of a 2-dimensional subcode of $\mathcal{C}$ which contains a codeword of weight d. The cost to the adversary (in extra positions read) to get two symbols of information using this algorithm is $g_2 - d_2$. We denote the maximum of $g_2 - d_2$ over all $[n, k, d; q]$ codes without zero-positions by $\mu_q(n, k, d)$. If no $[n, k, d; q]$ code exists, we define $\mu_q(n, k, d) = 0$. We want to estimate $\mu_q(n, k, d)$.

We have considered this problem for $k = 3$ and general q in [3], and $q = 2$ and general $k \geq 4$ in [2]. In this paper we consider general $k \geq 4$ and q.

2 Upper bounds

Let $\mathcal{G}$ be a generator matrix for an $[n, k; q]$ code $\mathcal{C}$. For any $\mathbf{x} \in GF(q)^k$, $m(\mathbf{x})$, the *multiplicity* of $\mathbf{x}$, will denote the number of occurrences of $\mathbf{x}$ as a column in $\mathcal{G}$. In [1], [6] it was shown that there is a one-one correspondence between the subspaces $\mathcal{D}$ of dimension r and the subspaces of $GF(q)^k$ of dimension $(k - r)$ such that if $\mathcal{D}$ corresponds to U, then

$$|\chi(\mathcal{D})| + \sum_{\mathbf{x} \in U} m(\mathbf{x}) = d_k. \tag{1}$$

Assuming that $\mathcal{G}$ contains no all-zero columns, we may view the columns of $\mathcal{G}$ as points in the projective space $PG(k-1, q)$, and $\mathcal{G}$ determines a projective multiset, that is a function

$$m : PG(k-1, q) \to N = \{0, 1, 2, \ldots\}.$$

For $p \in PG(k-1, q)$ we call $m(p)$ the *multiplicity* of p. Conversely, a projective multiset defines a generator matrix and a code (up to equivalence). We define the multiplicity of a subset $S \subset PG(k-1, q)$ by $m(S) = \sum_{p \in S} m(p)$.

Suppose that a projective multiset m corresponding to an $[n, k, d; q]$ code is given. Let $\mathcal{S}_r$ denote the set of subspaces of $PG(k-1, q)$ of (projective) dimension r. Further let $\mathcal{P}_{k-3}$ denote the set of $P \in \mathcal{S}_{k-3}$ for which there exist an $H \in \mathcal{S}_{k-2}$ such that $P \subset H$ and $m(H) = n - d$.

Let

$$\begin{aligned}
\alpha &= \max\{m(P) \mid P \in \mathcal{S}_{k-3}\}, \\
\beta &= \max\{m(P) \mid P \in \mathcal{P}_{k-3}\}, \\
\Delta(m) &= \alpha - \beta.
\end{aligned}$$

By (1), we have

$$n - d = \max\{m(H) \mid H \in \mathcal{S}_{k-2}\}.$$

$$\alpha = n - d_2, \quad \beta = n - g_2.$$

In particular, $g_2 - d_2 = \alpha - \beta = \Delta(m)$.

We will now give a couple of upper bounds on $\mu_q(n, k, d)$. Let

$$\begin{aligned}
U_1(q, n, k, d) &= d - \left\lceil \frac{d+1}{q} \right\rceil, \\
U_2(q, n, k, d) &= \left\lfloor \frac{q^{k-1} - q^{k-2}}{q^{k-1} - 1} \cdot (n - d) \right\rfloor - \left\lceil \frac{d+1}{q} \right\rceil.
\end{aligned}$$

Theorem 1 *For all n, $k \geq 4$, and d we have*

$$\begin{aligned}
\mu_q(n, k, d) &\leq U_1(q, n, k, d), \\
\mu_q(n, k, d) &\leq \max\{0, U_2(q, n, k, d)\}.
\end{aligned}$$

Proof: If $\mu_q(n,k,d) = 0$, there is nothing to prove. Therefore, let m be a projective multiset over $PG(k-1,q)$ such that $\Delta(m) = \mu_q(n,k,d) > 0$. Let $Q \in \mathcal{S}_{k-3}$ such $m(Q) = \alpha$, and let $H \in \mathcal{S}_{k-2}$ and $R \in \mathcal{P}_{k-3}$ such that $m(H) = n-d$, $R \subset H$, and $m(R) = \beta$.

There are $q+1$ spaces $P \in \mathcal{S}_{k-2}$ which contain Q. By definition, these spaces have multiplicity at most $n-d-1$. Hence

$$n + q\alpha = \sum_{Q \subset P \in \mathcal{S}_{k-2}} m(P) \leq (q+1)(n-d-1)$$

and so

$$\alpha \leq \left\lfloor \frac{qn-(q+1)(d+1)}{q} \right\rfloor = n-d-\left\lceil \frac{d+1}{q} \right\rceil. \tag{2}$$

Since $\alpha > \beta$ we have $Q \not\subset H$. Let $C = Q \cap H$. We have

$$\alpha = m(Q) = m(C) + m(Q \setminus C) \leq m(C) + d,$$

and so

$$m(C) \geq \alpha - d. \tag{3}$$

The $q+1$ spaces P in H which contain C all have multiplicities at most β. Hence, by (3)

$$(q+1)\beta \geq \sum_{C \subset P \subset H} m(P) = n-d+qm(C) \geq n-d+q(\alpha-d),$$

and so

$$\beta \geq \left\lceil \frac{n-d+q(\alpha-d)}{q+1} \right\rceil. \tag{4}$$

Combining (2) and (4) we get

$$\begin{aligned}
\Delta(m) &\leq \alpha - \left\lceil \frac{n-d+q(\alpha-d)}{q+1} \right\rceil \\
&= \left\lfloor \frac{\alpha - n + (q+1)d}{q+1} \right\rfloor \\
&\leq \left\lfloor \frac{\left\lfloor \frac{qn-(q+1)(d+1)}{q} \right\rfloor - n + (q+1)d}{q+1} \right\rfloor \\
&= d - \left\lceil \frac{d+1}{q} \right\rceil = U_1.
\end{aligned}$$

Next, the $(q^{k-1}-1)/(q-1)$ subspaces of H of dimension $k-3$ have value at most β. Since each point in H belongs to $(q^{k-2}-1)/(q-1)$ of these spaces, we get

$$\frac{q^{k-2}-1}{q-1} \cdot (n-d) = \frac{q^{k-2}-1}{q-1} \cdot m(H) \leq \frac{q^{k-1}-1}{q-1} \cdot \beta$$

and so

$$\beta \geq \left\lceil \frac{(q^{k-2}-1)(n-d)}{q^{k-1}-1} \right\rceil. \tag{5}$$

Combining (2) and (5) we get

$$\begin{aligned}
\Delta(m) &\leq n-d-\left\lceil \frac{d+1}{q} \right\rceil - \left\lceil \frac{(q^{k-2}-1)(n-d)}{q^{k-1}-1} \right\rceil \\
&= \left\lfloor \frac{(q^{k-1}-q^{k-2})(n-d)}{q^{k-1}-1} \right\rfloor - \left\lceil \frac{d+1}{q} \right\rceil = U_2.
\end{aligned}$$

Corollary 1 *If*

$$n \leq \frac{q^k - 1}{q^k - q^{k-1}} d, \tag{6}$$

then $\mu_q(n,k,d) = 0$.

Proof: If (6) is true, then in particular

$$n < \frac{(q^k - 1)d + (q^{k-1} - 1)}{q^k - q^{k-1}},$$

that is

$$\frac{q^{k-1} - q^{k-2}}{q^{k-1} - 1} \cdot (n - d) < \frac{d+1}{q}$$

and so $U_2(q,n,k,d) < 0$.

3 Constructions

To describe the constructions, we fix four subspaces

$$H \in \mathcal{S}_{k-2} \quad \text{and} \quad X, Q, R \in \mathcal{S}_{k-3}$$

such that

$$X \subset H, \quad R \subset H, \quad X \neq R, \quad Q \not\subset H, \quad (Q \cap R) \not\subset X, \quad \text{and} \quad Q \cap R \in \mathcal{S}_{k-4}.$$

Further, let $Y = H \setminus X$, and let a and b be points such that

$$a \in (Q \cap R) \setminus X \quad \text{and} \quad b \in Q \setminus H.$$

We will construct multisets m such that

$$\begin{aligned}
m(p) &\geq 0 \text{ for all } p \in PG(k-1,q), && (7)\\
m(H) &= n - d, && (8)\\
m(P) &\leq m(R) \text{ for all } P \in \mathcal{S}_{k-3} \text{ such that } P \subset H, && (9)\\
m(P) &\leq m(Q) \text{ for all } P \in \mathcal{S}_{k-3}, && (10)\\
m(G) &< n - d \text{ for all } G \in \mathcal{S}_{k-2} \setminus \{H\}. && (11)
\end{aligned}$$

This will imply that $d_2 = n - m(Q)$ and $g_2 = n - m(R)$ and so $\Delta(m) = m(Q) - m(R)$.

Construction 1

Theorem 2 *For* $k \geq 4$, $d \geq 1$, *and*

$$n \geq d + q^{k-2}\omega, \tag{12}$$

we have

$$\mu_q(n,k,d) \geq d - (q-1)q^{k-4}\omega, \tag{13}$$

where

$$\omega = \left\lceil \frac{d+1}{q^{k-3}(q-1)} \right\rceil.$$

Proof: First we note that if $d < (q-1)q^{k-4}\omega$, then the lower bound is negative and there is nothing to prove. Hence, assume that

$$d \geq (q-1)q^{k-4}\omega. \tag{14}$$

We assign the following multiplicities:

$$\begin{aligned} m(a) &= n - d - (q^{k-2}-1)\omega, \\ m(b) &= d, \\ m(p) &= \omega \text{ for } p \in Y,\ p \neq a, \\ m(p) &= 0 \text{ otherwise.} \end{aligned}$$

We will show that (7-11) are satisfied.

By (12), $m(a) \geq \omega \geq 1$. For $p \neq a$, it follows directly from the definition of m that $m(p) \geq 0$. This proves (7).

We note that $(Q \cap R) \not\subset X$ inplies that $Q \cap X \in \mathcal{S}_{k-5}$ and so

$$|Y| = q^{k-2}, |Q \cap Y| = q^{k-4}, |R \cap Y| = q^{k-3}.$$

Hence

$$\begin{aligned} m(H) &= m(a) + (q^{k-2}-1)\omega = n - d, \\ m(Q) &= m(a) + m(b) + (q^{k-4}-1)\omega = n - (q^2-1)q^{k-4}\omega, \\ m(R) &= m(a) + (q^{k-3}-1)\omega = n - d - (q-1)q^{k-3}\omega. \end{aligned}$$

In particular, (8) is satisfied. Let $P \in \mathcal{S}_{k-3}$. If $P \subset H$ and $P \neq X$, then $|P \cap Y| = q^{k-3}$ and so

$$m(P) \leq m(a) + (q^{k-3}-1)\omega = m(R).$$

Since $m(X) = 0$, this proves (9). If $P \not\subset H$, then $|P \cap Y| = q^{k-4}$ if $P \cap H \not\subset X$ and $|P \cap Y| = 0$ if $P \cap H \subset X$. Hence

$$m(P) \leq m(a) + m(b) + (q^{k-4}-1)\omega = m(Q).$$

This proves (10).

Finally, let $G \in \mathcal{S}_{k-2} \setminus \{H\}$. Then $|G \cap Y| = q^{k-3}$ if $G \cap H \neq X$ and $|G \cap Y| = 0$ if $G \cap H = X$ and Hence

$$\begin{aligned} m(G) &\leq m(b) + m(G \cap Y) \\ &\leq m(b) + m(a) + (q^{k-3}-1)\omega \\ &= m(H) + d - (q-1)q^{k-3}\omega \\ &\leq m(H) + d - (d+1) < m(H), \end{aligned}$$

and this proves (11).

Remark. We note that if $d \equiv r \pmod{(q-1)q^{k-3}}$ where $-q \leq r \leq -1$, then the upper bound U_1 and the lower bound (13) coincide. In general, there is a gap between these two bounds which is at most $(q-1)q^{k-4} - 1$.

Construction 2

We will now show how to find multisets m for which $\Delta(m)$ is close to U_2. We first describe the underlying idea. We note that if m_1 is a constant multiset, that is $m_1(p) = \theta$ for all $p \in PG(k-1, q)$, then $n = \theta(q^k-1)/(q-1)$, $d = q^{k-1}\theta$ and $\Delta(m_1) = 0$. Also,

$$U_2\Big(q, \frac{q^k-1}{q-1}\theta, k, q^{k-1}\theta\Big) = -1.$$

Next, $U_2 \leq U_1$ if and only if

$$d \geq \frac{q^{k-1} - q^{k-2}}{q^{k-1} - 1} \cdot (n - d),$$

that is

$$d \geq \frac{n(q^{k-1} - q^{k-2})}{2q^{k-1} - q^{q-2} - 1} \approx \frac{n(q-1)}{2q-1}.$$

Let m_2 denote the multiset obtained from Construction 1 for $d = \frac{n(q-1)}{2q-1}$ (disregarding for the moment that the multiplicities may be non-integers). Both m_1 and m_2 are multisets close to U_2. Choosing (convex) linear combinations of m_1 and m_2 we get a multiset (possibly with non-integral multiplicities) close to U_2 for $\frac{n(q-1)}{2q-1} \leq d \leq \frac{n(q^{k-1}-1)}{q^k-1}$. To avoid the non-integral multiplicities, we round the values to one of the nearest integers in a careful way.

We now describe the construction in detail. Let δ be a positive real number (this will correspond to d for m_2). Let

$$\theta = \frac{2q-1}{q^k-1}\delta \quad \text{and} \quad \omega = \frac{\delta}{q^{k-3}(q-1)}.$$

Let $0 < \gamma < 1$, and let

$$\begin{array}{ll} m(p) = \lceil \gamma\theta \rceil & \text{for } p \in X, \\ m(p) = \lceil (1-\gamma)\omega + \gamma\theta \rceil & \text{for } p \in Y, \\ m(b) = \lfloor (1-\gamma)\delta + \gamma\theta \rfloor, & \\ m(p) = \lfloor \gamma\theta \rfloor & \text{for } p \in Q \setminus H,\ p \neq b, \\ m(p) = \lfloor \gamma\theta \rfloor - 1 & \text{for } p \notin H \cup Q. \end{array}$$

We will show that (7-11) are satisfied under certain conditions. First, (7) is satisfied if and only if $\gamma\theta \geq 1$, that is,

$$\gamma\delta \geq \frac{q^k - 1}{2q - 1}. \tag{15}$$

We *define* n and d by

$$n = m(PG(k-1, q)), \quad n - d = m(H).$$

In particular, (8) is then satisfied by definition. Next, we see that

$$\begin{aligned} m(Q) &= \lfloor (1-\gamma)\delta + \gamma\theta \rfloor + (q^{k-3} - 1)\lfloor \gamma\theta \rfloor \\ &\quad + q^{k-4}\lceil (1-\gamma)\omega + \gamma\theta \rceil + \frac{q^{k-4} - 1}{q-1}\lceil \gamma\theta \rceil, \\ m(R) &= q^{k-3}\lceil (1-\gamma)\omega + \gamma\theta \rceil + \frac{q^{k-3} - 1}{q-1}\lceil \gamma\theta \rceil. \end{aligned}$$

Hence

$$\begin{aligned} m(Q) - m(R) &= \lfloor (1-\gamma)\delta + \gamma\theta \rfloor + (q^{k-3} - 1)\lfloor \gamma\theta \rfloor \\ &\quad - (q^{k-3} - q^{k-4})\lceil (1-\gamma)\omega + \gamma\theta \rceil - q^{k-4}\lceil \gamma\theta \rceil \\ &> (1-\gamma)\delta - (q^{k-3} - q^{k-4})(1-\gamma)\omega - 2q^{k-3} \\ &= (1-\gamma)\delta\frac{(q-1)}{q} - 2q^{k-3}. \end{aligned} \tag{16}$$

Hence, if

$$(1-\gamma)\delta \geq \frac{2q^{k-2}}{q-1}, \tag{17}$$

then $m(Q) > m(R)$.

Let $P \in \mathcal{S}_{k-3}$. If $P \subset H$ and $P \neq X$, then $m(P) = m(R)$. Clearly $m(X) \leq m(R)$. This proves (9). Consider $P \not\subset H$. From the definition of m it is easy to see that $m(P) \leq m(Q)$, that is, (10) is satisfied.

Finally, let $G \in \mathcal{S}_{k-2} \setminus \{H\}$. Let $Z = (G \setminus H) \cap Q$. Then $|Z| \leq q^{k-3}$ (with equality if $Q \subset G$) and so

$$\begin{aligned} m(G \setminus H) &= m(Z) + m((G \setminus H) \setminus Z) \\ &\leq m(b) + (q^{k-2} - 1)\lfloor \gamma\theta \rfloor - (q^{k-2} - |Z|) \\ &\leq m(b) + (q^{k-2} - 1)\lfloor \gamma\theta \rfloor - (q^{k-2} - q^{k-3}) \\ &\leq (1-\gamma)\delta + q^{k-2}\gamma\theta - (q^{k-2} - q^{k-3}). \end{aligned}$$

Further $|(H \setminus G) \cap Y| = q^{k-2} - q^{k-3}$ if $X \not\subset G$ and $|(H \setminus G) \cap Y| = q^{k-2}$ if $X \subset G$, and so

$$\begin{aligned} m(H \setminus G) &\geq (q^{k-2} - q^{k-3})\lceil (1-\gamma)\omega + \gamma\theta \rceil + q^{k-3}\lceil \gamma\theta \rceil \\ &\geq (q^{k-2} - q^{k-3})(1-\gamma)\omega + q^{k-2}\gamma\theta \\ &= (1-\gamma)\delta + q^{k-2}\gamma\theta. \end{aligned}$$

Hence

$$m(H) - m(G) = m(H \setminus G) - m(G \setminus H) \geq q^{k-2} - q^{k-3} > 0.$$

Therefore, (11) is satisfied.

We summarize the result in the following theorem where we also include an upper estimate of $U_2(q,n,k,d)$ obtained using our present values of n and d in the definition of U_2.

Theorem 3 *Let $k \geq 4$ and let δ and γ be positive real numbers such that $0 < \gamma < 1$ and*

$$\gamma\delta \geq \frac{q^k - 1}{2q - 1}.$$

Define n and d by

$$\begin{aligned} d &= \lfloor (1-\gamma)\delta + \gamma\theta \rfloor + (q^{k-1} - 1)\lfloor \gamma\theta \rfloor - (q^{k-1} - q^{k-3}) \\ n &= d + q^{k-2}\lceil (1-\gamma)\omega + \gamma\theta \rceil + \frac{q^{k-2} - 1}{q - 1}\lceil \gamma\theta \rceil, \end{aligned}$$

where

$$\theta = \frac{2q-1}{q^k - 1}\delta \quad \text{and} \quad \omega = \frac{\delta}{q^{k-3}(q-1)}.$$

Then

$$\mu_q(n,k,d) > (1-\gamma)\delta\frac{(q-1)}{q} - 2q^{k-3}.$$

Further

$$U_2(q,n,k,d) < (1-\gamma)\delta\left\{\frac{(q-1)}{q} + \frac{1}{q^k - 1}\right\} + 3q^{k-2}.$$

Remark 1. The condition (17), which we used to guarantee that $m(Q) > m(R)$, is not required in the theorem. The reason is that if (17) is not satisfied, then the lower bound on $\mu_q(n,k,d)$ in the theorem is negative and is trivially true.

Remark 2. For Construction 2 the difference $|U_2(q,n,k,d) - \Delta(m) - \frac{1}{q^k-1}(1-\gamma)\delta|$ is bounded. The construction can not be easily modified to a construction where $|U_2(q,n,k,d) - \Delta(m)|$ is bounded. Whether $|U_2(q,n,k,d) - \mu_q(n,k,d)|$ is bounded or not remains an open question.

Acknowledgements. This work was supported by The National Science Foundation of China (grant no. 10271116) and The Norwegian Research Council.

References

[1] W. Chen and T. Kløve, "The weight hierarchy of q-ary codes of dimension 4", *IEEE Trans. Inform. Theory*, vol. 42, pp. 2265–2272, 1996.

[2] W. Chen and T. Kløve, "On the second greedy weight for binary linear codes", in: M. Fossorier et al. (Eds.): *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes.* Springer Lecture Notes in Computer Science, vol. 1719, pp. 131–141, 1999.

[3] W. Chen and T. Kløve, "On the second greedy weight for linear codes of dimension 3", *Discrete Math.,* vol. 241, pp.171-187, 2001.

[4] G. D. Cohen, S. B. Encheva and G. Zémor, "Antichain codes", *Designs, Codes and Cryptography*, vol. 18, pp. 71–80, 1999.

[5] T. Helleseth, T. Kløve, 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.

[6] T. Helleseth, T. Kløve, Ø. Ytrehus, "Generalized Hamming weights of linear codes", *IEEE Trans. Inform. Theory*, vol. 38, pp. 1133–1140, 1992.

[7] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II", *AT& T Bell Labs Technical Journal*, vol. 63, pp. 2135–2157, 1984.

[8] V. K. Wei, "Generalized Hamming Weights for Linear Codes", *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412–1418, 1991.