ON THE DUALS OF BINARY HYPER-KLOOSTERMAN CODES

MARKO MOISIO*

Abstract. Binary hyper-Kloosterman codes $C(r,m)$ of length $(2^r-1)^{m-1}$ are a quasi-cyclic generalization of the dual of the Melas code of length 2^r-1. In this note the duals $C^{\perp}(r,m)$ i.e. a generalization of the Melas code $C^{\perp}(r,2)$ itself are studied. In particular, the minimum distance of $C^{\perp}(r,m)$ for all $r,m \geq 2$, the weight distribution of $C(2,m)$ and $C^{\perp}(2,m)$ for all $m \geq 2$, and the weight distribution of $C(r,3)$ and $C^{\perp}(r,3)$ for all $r \geq 2$ is obtained.

Key words. Exponential sum, Fermat curve, hyper-Kloosterman code, Kloosterman sum, Melas code, Pless power moments, Weight distribution

AMS subject classifications. 11T23, 11T71

1. Introduction. Let $r,m \geq 2$ be integers and let $q=2^r$. Let $\mathbb{F} := \mathbb{F}_q$ denote the finite field of q elements and let $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$. For $\mathbf{a} := (a_1,\ldots,a_m) \in \mathbb{F}^m$ we define a rational function in $m-1$ variables:

$$f_{\mathbf{a}}(\mathbf{X}) := a_1X_1 + \cdots + a_{m-1}X_{m-1} + \frac{a_m}{X_1\cdots X_{m-1}}.$$

Let $\mathbf{x}_1,\ldots,\mathbf{x}_n$ be a fixed ordering of the elements of $(\mathbb{F}^*)^{m-1}$.

In [3] the following linear code $C(r,m)$ was introduced and it was called a *hyper-Kloosterman code*:

$$C(r,m) = \Big\{c(\mathbf{a}) := \big(\mathrm{t}r(f_{\mathbf{a}}(\mathbf{x}_1)),\ldots,\mathrm{t}r(f_{\mathbf{a}}(\mathbf{x}_n))\big) \mid \mathbf{a} \in \mathbb{F}^m\Big\},$$

here $\mathrm{t}r$ is the trace function from $\mathbb{F}$ onto $\mathbb{F}_2$. These codes are a quasi-cyclic generalization of the Kloosterman code, i.e. the dual of the Melas code, of length 2^r-1. For the proof of the quasi-cyclicity we refer to [4, Theorem 4.2].

In this note we are interested in the duals $C^{\perp}(r,m)$ which are a generalization of the Melas code $C^{\perp}(r,2)$ $(r>2)$. We shall show that the minimum distance of $C^{\perp}(r,m)$ is three if $m>2$, and give the weight distribution of $C(2,m)$ and $C^{\perp}(2,m)$ for all $m \geq 2$, and the weight distribution of $C(r,3)$ and $C^{\perp}(r,3)$ for all $r \geq 2$. We remark that the weight distributions of $C(r,2)$ and $C^{\perp}(r,2)$ $(r>2)$ were obtained in [5] and in [14], respectively.

The rest of this paper is organized as follows. In Section 2 we first consider some simple basic properties of hyper-Kloosterman codes. Next, the weight distribution of $C(r,m)$ is given in terms of certain monomial exponential sums (Theorem 2.5), and then, a recursion formula for the weight distribution of $C^{\perp}(r,m)$ involving the moments M_j of those exponential sums is obtained by using the Pless power moment identity (Theorem 2.8).

In Section 3 we first connect the moments M_j to a Fermat curve $\mathcal{X}$, and then obtain the number of weight three codewords in $C^{\perp}(r,m)$ in terms of the number of rational points on $\mathcal{X}$ (Theorem 3.2). Finally, we determine the minimum distance of $C^{\perp}(r,m)$ by either using our explicit knowledge of the number of rational points on $\mathcal{X}$ or by estimating that number by either the Hasse-Weil bound or a bound which we shall derive by using Deligne's bound on hyper-Kloosterman sums (Theorem 3.7).

*Department of Mathematics and Statistics, Faculty of Technology, University of Vaasa, PO. Box 700, FIN-65101, Finland(`mamo@uwasa.fi`).

In a few cases we are forced to calculate the number of rational points numerically since neither of those bounds is then strong enough.

In Sections 4 and 5 we determine the weight distribution of the codes $C(r,m)$ and $C^{\perp}(r,m)$ in the special cases $r=2$, $m>2$, and $r>2$, $m=3$, respectively. In the latter case a relation between one and two dimensional Kloosterman sums from [1] is used, and then, the weight distribution of $C(r,3)$ is obtained by using results on the distribution of values of Kloosterman sums obtained in [5] (Theorem 5.3). Finally, the weight distribution of $C^{\perp}(r,3)$ is obtained in terms of even moments of Kloosterman sums calculated in [10] by using result from [14]. Especially, explicit formulae for the number of codewords of weights from three to five is given (Theorem 5.5).

2. On the weight distribution of $C(r,m)$ and $C^{\perp}(r,m)$. Let χ be the canonical additive character of $\mathbb{F}$. Let

$$k_{m-1}(\mathbf{a}) = \sum_{x_1,\ldots,x_{m-1}\in\mathbb{F}^*} \chi(a_1x_1+\ldots+a_{m-1}x_{m-1}+a_m(x_1\cdots x_{m-1})^{-1}),$$

be an $(m-1)$-dimensional Kloosterman sum. If $\mathbf{a}=(1,1,\ldots,1,a)$ with $a\neq 0$ we use the notation

$$k_{m-1}(a) := k_{m-1}(\mathbf{a}).$$

Let v be the number of zero-components of $\mathbf{a}$. Assume $v>0$. If $a_m=0$ then, by the orthogonality of characters, we get

$$k_{m-1}(\mathbf{a}) = \sum_{x_1,\ldots,x_{m-1}\in\mathbb{F}^*} \chi(a_1x_1+\cdots+a_{m-1}x_{m-1}) = (-1)^{m-v}(q-1)^{v-1}.$$

If $a_m\neq 0$ and e.g. $a_1=0$ then, by the substitution $y=x_1^{-1}$, we obtain

$$\begin{aligned} k_{m-1}(\mathbf{a}) &= \sum_{x_2,\ldots,x_{m-1}\in\mathbb{F}^*} \chi(a_2x_2+\cdots+a_{m-1}x_{m-1}) \sum_{y\in\mathbb{F}^*}\chi\Big(\frac{a_m}{x_2\cdots x_{m-1}}y\Big) \\ &= -\sum_{x_2,\ldots,x_{m-1}\in\mathbb{F}^*} \chi(a_2x_2+\cdots+a_{m-1}x_{m-1}) \\ &= -(-1)^{m-2-(v-1)}(q-1)^{v-1}. \end{aligned}$$

Hence we have

Lemma 2.1. *If exactly $v>0$ of the components of $\mathbf{a}\in\mathbb{F}^m$ are zeros, then*

$$k_{m-1}(\mathbf{a}) = (-1)^{m-v}(q-1)^{v-1}.$$

If $v=0$, then we have the following well known bound by Deligne:

$$|k_{m-1}(\mathbf{a})| \le mq^{\frac{m-1}{2}}.$$

Lemma 2.2. *The dimension k of $C(r,m)$ over $\mathbb{F}_2$ is rm if $rm>4$. If $r=m=2$, then $k=2$.*

Proof. Consider group homomorphism

$$\Psi : (\mathbb{F}^m,+) \longrightarrow C(r,m), \mathbf{a} \mapsto \big(\mathrm{tr}(f_{\mathbf{a}}(\mathbf{x}_1)),\ldots,\mathrm{tr}(f_{\mathbf{a}}(\mathbf{x}_n))\big). \tag{2.1}$$

If $\mathbf{a}$ belongs to $\mathrm{K}er(\Psi)$ then $k_{m-1}(\mathbf{a}) = (q-1)^{m-1}$. If $rm > 4$, this can happen if and only if $\mathbf{a} = \mathbf{0}$, by Deligne's bound and by Lemma 2.1, and therefore ψ is an isomorphism.

If $r = m = 2$ and $a, b \in \mathbb{F}_4^*$, then $k_{m-1}((a,b)) = k_{m-1}(ab)$. If $ab = 1$, then $k_{m-1}(ab) = 3$ and otherwise $k_{m-1}(ab) = -1$. Hence, in this case, $|\mathrm{K}er(\Psi)| = 4$ and consequently $|C(r,m)| = 16/4 = 4$. □

Remark. A different proof for this result is given in [4, Theorem 3.1]

The Hamming weight $w(c(\mathbf{a}))$ of codeword $c(\mathbf{a})$ is given by

$$w(c(\mathbf{a})) = \sum_{\mathbf{x}\in(\mathbb{F}^*)^{m-1}} \frac{1}{2}\Big(1-(-1)^{tr(f_{\mathbf{a}}(\mathbf{x}))}\Big) = \frac{1}{2}\big((q-1)^{m-1} - k_{m-1}(\mathbf{a})\big). \tag{2.2}$$

Next we express $w(c(\mathbf{a}))$ by means of a monomial exponential sum over $\mathbb{F}_{q^m}$. Let e denote the canonical additive character of $\mathbb{F}_{q^m}$. Let $t = (q^m-1)/(q-1)$ and let $\mathrm{N}(\alpha) := \alpha^t$ denote the norm of α from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Let γ be a primitive element of $\mathbb{F}_{q^m}$, and let

$$s(\alpha) = \sum_{i=0}^{t-1} e\big(\alpha\gamma^{(q-1)i}\big).$$

We have the following result from [9, Theorem 3]:

THEOREM 2.3. *Let $\alpha \in \mathbb{F}_{q^m}^*$ and let $a = \mathrm{N}(\alpha)$. Then*

$$\sum_{x\in\mathbb{F}_{q^m}^*} e(\alpha x^{q-1}) = (-1)^{m-1}(q-1)k_{m-1}(a),$$

or, equivalently,

$$k_{m-1}(a) = (-1)^{m-1}s(\alpha).$$

LEMMA 2.4. *Let $\mathbf{a} \in (\mathbb{F}^*)^m$ and let $b = a_1\cdots a_m$. Let $g := \mathrm{N}(\gamma)$ be a primitive element of $\mathbb{F}$, $i = \mathrm{ind}_g(b)$, and $\beta = \gamma^i$. Then*

$$\begin{aligned} w(c(\mathbf{a})) &= \frac{1}{2}\big((q-1)^{m-1} - k_{m-1}(b)\big) \\ &= \frac{1}{2}\big((q-1)^{m-1} + (-1)^m s(\beta)\big). \end{aligned}$$

Proof. The first equality follows easily by equation (2.2), and the second one then by Theorem 2.3. □

Let S denote the range of $s(\gamma^i)$ as i varies over the set $I := \{0,\dots,q-2\}$, and, for $j \in S$, let N_j denote the number of elements i in I such that $s(\gamma^i) = j$, i.e.

$$S = \big\{s(\gamma^i) \mid i \in I\big\},$$

and

$$N_j = \big|\{i \in I \mid s(\gamma^i) = j\}\big|.$$

THEOREM 2.5. *Assume $rm > 4$. For $\mathbf{a} \in \mathbb{F}^m$ let v be the number of zero components of $\mathbf{a}$. If $v > 0$, there are*

$$\binom{m}{v}(q-1)^{m-v} \text{ codewords } c(\mathbf{a}) \text{ of weight } ((q-1)^{m-1} - (-1)^{m-v}(q-1)^{v-1})/2,$$

and otherwise, for each $j \in S$, there are

$$N_j(q-1)^{m-1} \text{ codewords } c(\mathbf{a}) \text{ of weight } ((q-1)^{m-1} + (-1)^m j)/2$$

in $C(r, m)$. Moreover, these are the only weights in $C(r, m)$.

Proof. First, for each $\mathbf{a} \in \mathbb{F}^m$, there exists exactly one codeword $c(\mathbf{a}) \in C(r, m)$, by isomorphism (2.1). If $v > 0$ the claim follows now by Lemmas 2.1 and 2.4.

Assume $v = 0$. For each $b \in \mathbb{F}^*$ there are exactly $(q-1)^{m-1}$ vectors $\mathbf{a} \in (\mathbb{F}^*)^m$ such that the product of the components of $\mathbf{a}$ equals b. The second claim follows now by Lemma 2.4 since there is exactly one i in I such that $\mathrm{N}(\gamma^i) = b$. The last claim is now obvious. □

COROLLARY 2.6. *The weights in $C(r, m)$ are divisible by $2^{\ell-1}$, where $\ell = \min\{r, m\}$.*

Proof. Let $\alpha \in \mathbb{F}_{q^m}$. By [12, Theorem 2], the exponential sum

$$\sum_{x \in \mathbb{F}_{q^m}} e(\alpha x^{q-1})$$

is divisible by $2^{\lceil rm/s \rceil}$ where s is the binary weight of $q-1$. Now $s = r$, and therefore $\sum_{x \in \mathbb{F}_{q^m}} e(\alpha x^{q-1}) = 2^m z$ for some $z \in \mathbb{Z}$.

Let $\mathbf{a} \in (\mathbb{F}^*)^m$, and let $\beta \in \mathbb{F}^*_{q^m}$ such that $\mathrm{N}(\beta) = a_1 \cdots a_m$. Now

$$\begin{aligned}
(q-1)w(c(\mathbf{a})) &= \frac{1}{2}\big((q-1)^m + (-1)^m(q-1)s(\beta)\big) \\
&= \frac{1}{2}\big((q-1)^m + (-1)^m \sum_{x \in \mathbb{F}^*_{q^m}} e(\alpha x^{q-1})\big) \\
&= \frac{1}{2}\big((q-1)^m + (-1)^m \sum_{x \in \mathbb{F}_{q^m}} e(\alpha x^{q-1}) - (-1)^m\big) \\
&= \frac{1}{2}(q^m - mq^{m-1} + \cdots + (-1)^{m-1}mq + (-1)^m 2^m z),
\end{aligned}$$

and, as $q = 2^r$, the claim follows in this case. If some of the components of $\mathbf{a}$ is zero, then it is easily seen that 2^{r-1} is a factor of $w(c(\mathbf{a}))$. □

Remark. A different proof for this result is given in [3, Corollary 4.3].

To obtain the weight distribution of $C^\perp(r, m)$ we use the Pless power moment identity proved in [13] (see also e.g. [6, p. 131]):

THEOREM 2.7 (Power moment identity). *Let B be a binary linear $[n, k]$ code, and let B_i (resp. $B_i^\perp$) denote the number of codewords of weight i in B (resp. in $B^\perp$). Then, for $h = 0, 1, \ldots$, we have:*

$$\sum_{i=0}^{n} i^h B_i = \sum_{i=0}^{n} (-1)^i B_i^\perp \sum_{t=0}^{h} t! S(h, t) 2^{k-t} \binom{n-i}{n-t},$$

where

$$S(h,t) := \frac{1}{t!}\sum_{j=0}^{t}(-1)^{t-j}\binom{t}{j}j^h \qquad \text{(a Stirling number of the second kind)},$$

and the binomial coefficient $\binom{u}{v}$ *is defined to be zero whenever* $v > u$ *or* $v < 0$.

For a non-negative integer j we denote by M_j the jth moment of the period $s(\gamma^l)$, or

$$M_j := \sum_{l=0}^{q-2} s(\gamma^l)^j.$$

THEOREM 2.8. *Assume* $rm > 4$, *and let* $w = 1-q$. *The number* $C_h^\perp$ *of codewords of weight* h *in* $C^\perp(r,m)$ *is given by*

$$q^m h! C_h^\perp = f(C_0^\perp, \dots, C_{h-1}^\perp) + g(M_0,\dots,M_h) + (-1)^{(m+1)(h+1)} w^{-h}\Big(w^m(1-w^m)^h - \sum_{j=0}^{h}\binom{h}{j}(-1)^j(w^{j+1}-w^h)^m\Big),$$

where

$$f(C_0^\perp,\dots,C_{h-1}^\perp) = q^m \sum_{i=0}^{h-1}(-1)^{h+i+1}C_i^\perp \sum_{t=i}^{h} t!S(h,t)2^{h-t}\binom{n-i}{n-t},$$

$$g(M_0,\dots,M_h) = \sum_{j=0}^{h}\binom{h}{j}(-1)^{mj+h}(q-1)^{(m-1)(h-j+1)}M_j.$$

Moreover, if $m = 3$, *the formula simplifies to*

$$q^3 h! C_h^\perp = f(C_0^\perp,\dots,C_{h-1}^\perp) + g(M_0,\dots,M_h) + 3(q-1)^2(-q)^h((q-2)^h + (q-1)^{h-1}).$$

Proof. We choose $B = C(r,m)$ in the power moment identity. Then, by Theorem 2.5,

$$\sum_{i=0}^{n} i^h C_i = \sum_{v=1}^{m}\binom{m}{v}(q-1)^{m-v}2^{-h}((q-1)^{m-1} - (-1)^{m-v}(q-1)^{v-1})^h + \sum_{l=0}^{q-2} 2^{-h}(q-1)^{m-1}((q-1)^{m-1} + (-1)^m s(\gamma^l))^h =: S_1 + S_2,$$

where

$$2^h S_1 = \sum_{v=1}^{m}\binom{m}{v}(q-1)^{m-v}((q-1)^{m-1} - (-1)^{m-v}(q-1)^{v-1})^h$$

and

$$2^h S_2 = (q-1)^{m-1}\sum_{l=0}^{q-2}((q-1)^{m-1} + (-1)^m s(\gamma^l))^h.$$

First, we manipulate S_2 somewhat:

$$\begin{aligned}
2^h S_2 &= (q-1)^{m-1} \sum_{l=0}^{q-2} \sum_{j=0}^{h} \binom{h}{j} (-1)^{mj} s(\gamma^l)^j (q-1)^{(m-1)(h-j)} \\
&= \sum_{j=0}^{h} \binom{h}{j} (-1)^{mj} (q-1)^{(m-1)(h-j+1)} \sum_{l=0}^{q-2} s(\gamma^l)^j \\
&= \sum_{j=0}^{h} \binom{h}{j} (-1)^{mj} (q-1)^{(m-1)(h-j+1)} M_j.
\end{aligned}$$

Secondly we consider S_1. If $m = 3$, then

$$2^h S_1 = 3(q-1)^2 q^h ((q-2)^h + (q-1)^{h-1}).$$

Next we write S_1 in the form from which we can derive explicit formulae for the number of low-weight codewords in the duals $C^{\perp}(r, m)$ for an arbitrary integer $m \geq 2$:

$$\begin{aligned}
2^h S_1 &= (q-1)^{m-1} \sum_{v=1}^{m} \binom{m}{v} (q-1)^{(v-1)(h-1)} ((q-1)^{m-v} + (-1)^{m-v-1})^h \\
&= (q-1)^{m-1} \sum_{v=1}^{m} \binom{m}{v} (q-1)^{(v-1)(h-1)} (-1)^{(m-v-1)h} (1-(1-q)^{m-v})^h \\
&= (-1)^{(m-1)h} (-w)^{m-1} \sum_{j=0}^{h} \binom{h}{j} (-1)^j \sum_{v=1}^{m} \binom{m}{v} (-1)^{vh} (-w)^{(v-1)(h-1)} w^{(m-v)j} \\
&= (-1)^{(m-1)h} (-w)^{-h} \sum_{j=0}^{h} \binom{h}{j} (-1)^j \sum_{v=1}^{m} \binom{m}{v} w^{vh} (-w)^{m-v} w^{(m-v)j} \\
&= (-1)^{(m-1)h+m} (-w)^{-h} \sum_{j=0}^{h} \binom{h}{j} (-1)^j \sum_{v=1}^{m} \binom{m}{v} (-1)^v w^{vh} w^{(m-v)(j+1)} \\
&= (-1)^{m(h+1)} w^{-h} \sum_{j=0}^{h} \binom{h}{j} (-1)^j \Big(\big(w^{j+1} - w^h\big)^m - w^{m(j+1)} \Big).
\end{aligned}$$

Since

$$\begin{aligned}
\sum_{j=0}^{h} \binom{h}{j} (-1)^j w^{m(j+1)} &= (1-q)^m \sum_{j=0}^{h} \binom{h}{j} (-1)^j (1-q)^{mj} \\
&= w^m (1-w^m)^h,
\end{aligned}$$

we have

$$\begin{aligned}
2^h S_1 = (-1)^{m(h+1)} w^{-h} &\sum_{j=0}^{h} \binom{h}{j} (-1)^j \big(w^{j+1} - w^h\big)^m \\
&-(-1)^{m(h+1)} w^{m-h} (1-w^m)^h.
\end{aligned}$$

As the left hand side of the power moment identity equals $S_1 + S_2$, and the right hand side equals

$$\begin{aligned} &\sum_{i=0}^{n}(-1)^i C_i^{\perp}\sum_{t=0}^{h} t!S(h,t)2^{rm-t}\binom{n-i}{n-t} \\ &= \sum_{i=0}^{h}(-1)^i C_i^{\perp}\sum_{t=i}^{h} t!S(h,t)2^{rm-t}\binom{n-i}{n-t} \\ &= \frac{q^m}{2^h}\sum_{i=0}^{h}(-1)^i C_i^{\perp}\sum_{t=i}^{h} t!S(h,t)2^{h-t}\binom{n-i}{n-t}, \end{aligned}$$

the claims follow now easily. □

3. The minimum distance of $C^{\perp}(r,m)$. To determine the minimum distance of $C^{\perp}(r,m)$ we need some auxiliary results. We recall that $t = (q^m - 1)/(q - 1)$ and $\mathbb{F}_{q^m}^* = \langle\gamma\rangle$.

LEMMA 3.1. *The first four moments M_j in Theorem 2.8 are given by*

$$\begin{aligned} M_0 &= q-1,\ M_1 = -1,\ M_2 = q^m - t, \\ M_3 &= \frac{|\mathcal{X}(\mathbb{F}_{q^m})| - 3(q-1)}{(q-1)^2} q^m - t^2, \end{aligned}$$

where $|\mathcal{X}(\mathbb{F}_{q^m})|$ is the number of rational points on the projective curve $\mathcal{X}$ over $\mathbb{F}_{q^m}$ defined by the equation

$$\mathcal{X} : x^{q-1} + y^{q-1} + z^{q-1} = 0.$$

Proof. Obviously $M_0 = q - 1$, and

$$M_1 = \sum_{l=0}^{q-2} s(\gamma^l) = \frac{q-1}{q^m-1}\sum_{l=0}^{q^m-2} s(\gamma^l) = \frac{1}{t}\sum_{i=0}^{t-1}\sum_{l=0}^{q^m-2} e(\gamma^{(q-1)i}\gamma^l) = -\frac{t}{t},$$

where the last equality follows by the orthogonality of characters. To prove the formula for M_2 we count the number N of solutions of the equation $x + y = 0$ in the group H of $(q-1)$th powers in $\mathbb{F}_{q^m}^*$. On the one hand $N = t$, and on the other hand, by the orthogonality of characters

$$\begin{aligned} q^m t &= \sum_{x,y\in H}\sum_{u\in\mathbb{F}_{q^m}} e(u(x+y)) = t^2 + \sum_{u\in\mathbb{F}_{q^m}^*}\left(\sum_{x\in H} e(ux)\right)^2 = t^2 + t\sum_{l=0}^{q-2} s(\gamma^l)^2 \\ &= t^2 + tM_2, \end{aligned}$$

from which the formula for M_2 follows.

Let N denote the number of solutions of equation

$$x^{q-1} + y^{q-1} + z^{q-1} = 0 \tag{3.1}$$

in $\mathbb{F}_{q^m}^3$. It is easy to see ([9, Section 3]) that $N = N'_m + N_m$, where

$$N'_m = 3(q-1)(q^m-1) + 1$$

and

$$\begin{aligned}
q^m N_m &= \sum_{u\in\mathbb{F}_{q^m}^*}\Big(\sum_{x\in\mathbb{F}_{q^m}^*} e(ux^{q-1})\Big)^3 + (q^m-1)^3\\
&= (q-1)^3\sum_{u\in\mathbb{F}_{q^m}^*} s(u)^3 + (q^m-1)^3\\
&= (q-1)^3 tM_3 + (q^m-1)^3,
\end{aligned}$$

and consequently,

$$q^m N = 3(q-1)(q^m-1)q^m + q^m + (q-1)^3 tM_3 + (q^m-1)^3.$$

Since $\big|\mathcal{X}(\mathbb{F}_{q^m})\big| = (N-1)/(q^m-1)$, we obtain

$$(q-1)^3\frac{q^m-1}{q-1}M_3 = q^m(q^m-1)\big|\mathcal{X}(\mathbb{F}_{q^m})\big| - 3(q-1)(q^m-1)q^m - (q^m-1)^3,$$

which simplifies to

$$(q-1)^2 M_3 = q^m\big|\mathcal{X}(\mathbb{F}_{q^m})\big| - 3(q-1)q^m - (q^m-1)^2.$$

Since $(q^m-1)^2 = (q-1)^2 t^2$, we see that the claim is true also for M_3. ☐

THEOREM 3.2. *The minimum distance of $C^\perp(r,m)$ is at least three. Moreover, if $rm > 4$, the number $C_3^\perp$ of weight three codewords in $C^\perp(r,m)$ is given by*

$$C_3^\perp = \frac{(q-1)^{m-3}\big((q-2)^m + (-1)^m(q^m+3q-|\mathcal{X}(\mathbb{F}_{q^m})|-5)\big)}{6}$$

Proof. Let $n=(q-1)^{m-1}$, and let $\mathbf{c}\in C^\perp(r,m)$. If $w(\mathbf{c})=2$ then

$$tr(f_{\mathbf{a}}(\mathbf{x}_i)+f_{\mathbf{a}}(\mathbf{x}_j)) = tr(f_{\mathbf{a}}(\mathbf{x}_i)) + tr(f_{\mathbf{a}}(\mathbf{x}_j)) = 0$$

for some $1\le i<j\le n$, say $i=1, j=2$, and for all $\mathbf{a}\in\mathbb{F}_q^m$. Let $1\le l\le m-1$ be the index of the coordinate place where $\mathbf{x}_1$ and $\mathbf{x}_2$ differ, say $l=1$. By choosing $\mathbf{a}=(a,0,\dots,0)$ we have $tr(a(x+y))=0$ for all $a\in\mathbb{F}_q$, and for some $x,y\in\mathbb{F}_q^*$ with $x\neq y$. (Here x and y are the first components of $\mathbf{x}_1$ and $\mathbf{x}_2$.) This contradicts the surjectivity of tr. A similar argument also proves that $w(\mathbf{c})\neq 1$.

Next we use Theorem 2.8 and Lemma 3.1 to prove the claimed formula for $C_3^\perp$. First,

$$\begin{aligned}
f(C_0^\perp, C_1^\perp, C_2^\perp) = f(1,0,0) &= q^m\sum_{t=0}^{3} t!S(3,t)2^{3-t}\binom{n}{n-t}\\
&= q^m(4n+6n(n-1)+(n-2)(n-1)n)\\
&= (q-1)^{2m-2}((q-1)^{m-1}+3)q^m,
\end{aligned}$$

and second,

$$\begin{aligned}
&g(M_0,M_1,M_2,M_3) = \sum_{j=0}^{3}\binom{3}{j}(-1)^{mj+h}(q-1)^{(m-1)(h-j+1)}M_j\\
&= -(q-1)^{4m-3} + 3(-1)^m(q-1)^{3(m-1)} - 3(q-1)^{2(m-1)}\left(q^m - \frac{q^m-1}{q-1}\right)\\
&\quad -(-1)^m(q-1)^{m-1}\left(\frac{|\mathcal{X}(\mathbb{F}_{q^m})|-3(q-1)}{(q-1)^2}q^m - \frac{(q^m-1)^2}{(q-1)^2}\right),
\end{aligned}$$

or, equivalently,

$$(q-1)^{3-m} g(M_0, M_1, M_2, M_3) = (-1)^m - 3(q-1)^m + 3(-1)^m (q-1)^{2m}$$
$$- (q-1)^{3m} + \big((-1)^m (q^m + 3q - |\mathcal{X}(\mathbb{F}_{q^m})| - 5) - 3(q-2)(q-1)^m\big) q^m.$$

Finally, since

$$(q-1)^{3-m} w^{-3} \Big(w^m (1-w^m)^3 - \sum_{j=0}^{3} \binom{3}{j} (w^{j+1} - w^3)^m \Big) =$$
$$- (-1)^m + 3(q-1)^m - 3(-1)^m (q-1)^{2m} + (q-1)^{3m}$$
$$- ((q-1)^m + 3)(q-1)^m q^m + (q-2)^m q^m,$$

we obtain

$$6C_3^{\perp} = (q-1)^{m-3}((q-2)^m + (-1)^m (q^m + 3q - |\mathcal{X}(\mathbb{F}_{q^m})| - 5)),$$

by Theorem 2.8. □

Example 3.3. If $r = m = 2$ then $n = 3$, and therefore the minimum distance of $C^{\perp}(2,2)$ is three. Hence, $C^{\perp}(2,2)$ is a repetition code.

Example 3.4. Consider the Melas code $C^{\perp}(r,2)$. By [9, Theorem 1]

$$\big|\mathcal{X}(\mathbb{F}_{q^2})\big| = (1 - (-1)^r)(q-1)^2 + 3(q-1),$$

and consequently

$$C_3^{\perp} = (1 + (-1)^r)(q-1)/6,$$

which is in accordance with [14, Table 6.1].

Example 3.5. Consider code $C^{\perp}(r,3)$. By [9, Theorem 2]

$$\big|\mathcal{X}(\mathbb{F}_{q^3})\big| = (2q + 1 - (-1)^r)(q-1)^2 + 3(q-1),$$

and therefore

$$C_3^{\perp} = (2q - 5 - (-1)^r)(q-1)^2/6.$$

Remark. By generalizing the argument used in the proof of Theorem 3.2 to prove the non-existence of weight two codewords, it is easy to see that a check matrix for $C^{\perp}(r,m)$ is $(\mathbf{y}_1^T\ \mathbf{y}_2^T \dots \mathbf{y}_n^T)$ where $\mathbf{y}_i = (\mathbf{x}_i\ z_i)$ and z_i is the product of the inverses of the components of $\mathbf{x}_i$.

We shall see soon that the minimum distance of $C^{\perp}(r,m)$ is always three if $m > 2$. It will turn out that Theorem 3.2 together with the Hasse-Weil bound prove most of the cases. On the other hand, in case $m = 4$ it is too weak, and we shall use the following upper bound:

LEMMA 3.6.

$$\big|\mathcal{X}(\mathbb{F}_{q^m})\big| < q^m + 3q + (q-1)^3 m^3 q^{\frac{m-3}{2}} - 4.$$

Proof. As we pointed out in the proof of Lemma 3.1, the number of solutions N of (3.1) satisfies

$$q^m N = (q-1)^3\Big(\sum_{u\in\mathbb{F}_{q^m}^*} e(ux^{q-1})\Big) + (q^m-1)^3 + 3(q-1)(q^m-1)q^m + q^m,$$

and then it is easily seen (see [9, Section 3]) that

$$q^m N = (-1)^{m-1}t(q-1)^3\sum_{u\in\mathbb{F}_q^*} k_{m-1}(u)^3 + (q^m-1)^3 + 3(q-1)(q^m-1)q^m + q^m.$$

Since $|\mathcal{X}(\mathbb{F}_{q^m})| = (N-1)/(q^m-1)$ we obtain

$$q^m|\mathcal{X}(\mathbb{F}_{q^m})| = (-1)^{m-1}(q-1)^2\sum_{u\in\mathbb{F}_q^*} k_{m-1}(u)^3 + (q^m-1)^2 + 3(q-1)q^m. \tag{3.2}$$

Now Deligne's bound gives the inequality

$$\Big|\sum_{u\in\mathbb{F}_q^*} k_{m-1}(u)^3\Big| \le (q-1)m^3 q^{\frac{3(m-1)}{2}}, \tag{3.3}$$

and therefore

$$|\mathcal{X}(\mathbb{F}_{q^m})| \le (q-1)^3 m^3 q^{\frac{m-3}{2}} + q^m - 2 + 3(q-1) + q^{-m}.$$

□

THEOREM 3.7. *The minimum distance of $C^\perp(r,m)$ is three unless r is odd and $m=2$, in which case it is at least five.*

Proof. Assume $m=2$. If $r=2$ the minimum distance $d=3$ by Example 3.3, and if $r>2$, then it is well known that $d=3$ or $d\ge 5$ according as r is even or odd (see e.g. [14]).

CLAIM. *If $m>2$ then $d=3$.*

If $m=3$ the Claim is true by Example 3.5. Assume $m>3$. To prove the Claim it is enough, by Theorem 3.2, to show that

$$\epsilon := (q-2)^m + (-1)^m(q^m + 3q - |\mathcal{X}(\mathbb{F}_{q^m})| - 5)$$

is positive. By separating the cases according to the parity of m, and by using the Hasse-Weil bounds

$$q^m + 1 - (q-2)(q-3)q^{\frac{m}{2}} \le \big|\mathcal{X}(\mathbb{F}_{q^m})\big| \le q^m + 1 + (q-2)(q-3)q^{\frac{m}{2}},$$

we obtain

$$\epsilon > (q-2)^m - (q-2)(q-3)q^{\frac{m}{2}} - 3q - 6,$$

which is obviously positive if $m\ge 5$ and $r\ge 3$ (i.e. $q\ge 8$).

Assume $m=4$ and $\epsilon=0$. Then, by Lemma 3.6, we must have

$$\begin{aligned}
(q-2)^4 &< 64\sqrt{q}(q-1)^3 + 1 \;\Leftrightarrow\\
(q-1)^4 &< 64\sqrt{q}(q-1)^3 + 4(q-1)^3 - 6(q-1)^2 + 4(q-1) \Leftrightarrow\\
q-1 &< 64\sqrt{q} + 4 - \frac{6}{q-1} + \frac{4}{(q-1)^2} < 64\sqrt{q} + 5.
\end{aligned}$$

Table 3.1

r	ϵ
3	$2^3 \cdot 3 \cdot 7^2$
4	$2 \cdot 3^3 \cdot 5^2 \cdot 37$
5	$2^4 \cdot 3^2 \cdot 5 \cdot 31^2$
6	$2 \cdot 3^5 \cdot 7^2 \cdot 641$
7	$2^3 \cdot 3^2 \cdot 7 \cdot 31 \cdot 127^2$
8	$2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 17^2 \cdot 1531$
9	$2^8 \cdot 3 \cdot 5 \cdot 7^2 \cdot 67 \cdot 73^2$
10	$2 \cdot 3^3 \cdot 11^5 \cdot 31^2 \cdot 131$
11	$2^3 \cdot 3^3 \cdot 11 \cdot 23^2 \cdot 89^2 \cdot 1759$
12	$2 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 113 \cdot 24709$

The inequality $q - 6 < 64\sqrt{q}$ implies that we must have $q \leq 2^{12}$ i.e. $r \leq 12$. Hence, if $m = 4$ and $r > 12$ the minimum distance is three. In the cases $m = 4$, $3 \leq r \leq 12$, we have verified this by calculating $\left|\mathcal{X}(\mathbb{F}_{q^4})\right|$ numerically (see Table 3.1).

In the remaining cases $r = 2$, $m \geq 4$, the Claim follows by Theorem 4.3 below, by which $C_3^{\perp} = 3^{m-3}(2^{m-1} \pm 1)$. □

We computed $\left|\mathcal{X}(\mathbb{F}_{q^4})\right|$ by using (3.2). In the calculation of the three dimensional Kloosterman sums $k_3(a)$ over $\mathbb{F}_q$, $q = 2^r$ with $3 \leq r \leq 12$, we took advantage of the following result by Carlitz from [1] which related two and one dimensional Kloosterman sums:

Theorem 3.8. *For any $a \in \mathbb{F}_q^*$, we have*

$$k_2(a) = k(a)^2 - q,$$

where $k(a) := k_1(a)$.

By Theorem 3.8 we have

$$\begin{aligned} k_3(a) &= \sum_{x,y,z \in \mathbb{F}_q^*} \chi(x + y + z + a(xyz)^{-1}) = \sum_{x \in \mathbb{F}_q^*} \chi(x) k_2(ax^{-1}) \\ &= \sum_{x \in \mathbb{F}_q^*} \chi(x) k(ax^{-1})^2 - q \sum_{x \in \mathbb{F}_q^*} \chi(x) \\ &= \sum_{x \in \mathbb{F}_q^*} \chi(x) k(ax^{-1})^2 + q, \end{aligned}$$

and now it is easy to see that

$$\begin{aligned} k_3(a) &= 2 \sum_{\substack{x \in \mathbb{F}_q^* \\ tr(x) = 0}} k(ax^{-1})^2 - \sum_{x \in \mathbb{F}_q^*} k(ax^{-1})^2 + q \\ &= 2 \sum_{\substack{x \in \mathbb{F}_q^* \\ tr(x) = 0}} k(ax^{-1})^2 - (q^2 - q - 1) + q. \end{aligned}$$

By tabulating the traces of elements of $\mathbb{F}_q^*$, the indices of those elements of $\mathbb{F}_q^*$ having the trace equal to zero, and then, the range of $k(u)$ as u varies over $\mathbb{F}_q^*$, before using the formula above, the data of Table 3.1 can quickly be verified.

Remark. The traces were calculated by making use of [4, Theorem 5.1].

4. The weight distribution of $C(2,m)$ and $C^{\perp}(2,m)$. In this section we assume that $m > 2$. Let γ be a primitive element of $\mathbb{F}_{2^{2m}}$. To determine the weight distribution of $C(2,m)$ and $C^{\perp}(2,m)$ we need the following result which has been proved already in [2] (see e.g. [8] for a different proof).

LEMMA 4.1. *Let $\alpha \in \mathbb{F}^*_{2^{2m}}$. Then*

$$\sum_{x \in \mathbb{F}^*_{2^{2m}}} e(\alpha x^3) = \begin{cases} (-1)^m 2^m - 1 & \text{if } 3 \nmid \mathrm{ind}_\gamma \alpha, \\ (-1)^{m+1} 2^{m+1} - 1 & \text{if } 3 \mid \mathrm{ind}_\gamma \alpha. \end{cases}$$

Lemma 4.1 together with Theorem 2.5 give the weight distribution of $C(2,m)$:

THEOREM 4.2. *The weight distribution of $C(2,m)$ is given in the following table, where v runs over the integers $1,\dots,m$.*

weight	*frequency*
$\frac{3^{m-1}-(-1)^{m-v}3^{v-1}}{2}$	$\binom{m}{v}3^{m-v}$
$\frac{1}{2}\left(3^{m-1}+\frac{2^m-(-1)^m}{3}\right)$	$2\cdot 3^{m-1}$
$\frac{1}{2}\left(3^{m-1}-\frac{2^{m+1}+(-1)^m}{3}\right)$	3^{m-1}

THEOREM 4.3. *For every non-negative integer h the number $C_h^{\perp}$ of codewords of weight h in the dual $C^{\perp}(2,m)$ of $C(2,m)$ is given by the recursion of Theorem 2.8 with*

$$M_j = 2\left(\frac{(-2)^m - 1}{3}\right)^j + \left(\frac{(-2)^{m+1} - 1}{3}\right)^j \quad \forall j = 0,1,\dots$$

Especially,

$$\begin{aligned} C_0^{\perp} &= 1,\ C_1^{\perp} = C_2^{\perp} = 0,\ C_3^{\perp} = 3^{m-3}(2^{m-1} \pm 1), \\ C_4^{\perp} &= 3^{m-5}\left(\frac{7^m - 3^{m+3} + 66}{8} + 3\cdot 2^{2m-2} \pm 2^m\right), \\ C_5^{\perp} &= 3^{m-6}\left((5^{m-1} \pm 6)2^{2m-3} - 3^{m+2}2^{m-2} + 2^{3m-2} + 7\cdot 2^{m+1} \pm \frac{55 - 3^{m+1}}{2}\right), \end{aligned}$$

where $\pm = (-1)^m$.

Proof. By Lemma 4.1 the moments M_j in Theorem 2.8 are of the claimed form, the claimed formulae for the low-weight codewords can be verified e.g. by using *Mathematica*. □

Remark. In a similar manner as was done above, the weight distribution of the codes $C(r,m)$ and $C^{\perp}(r,m)$ with $r = 3$ and $r = 4$ can be calculated as well.

5. The weight distribution of $C(r,3)$ and $C^{\perp}(r,3)$. In this section we assume that $r > 2$. Let γ be a primitive element of $\mathbb{F}_{q^3}$, and let $g = \mathrm{N}(\gamma)$ be a primitive element of $\mathbb{F} = \mathbb{F}_q$.

Now, by Theorems 2.3 and 3.8, we have the following:

LEMMA 5.1. *For each integer i satisfying $0 \le i \le q-2$, we have*

$$s(\gamma^i) = k(g^i)^2 - q.$$

Hence, the question about the distribution of the values of $s(\gamma^i)$ is equivalent to the question about the distribution of the values of (one dimensional) Kloosterman sums over $\mathbb{F}^*$. This question has been answered by Lachaud and Wolfmann in [5, Theorem 3.4 and Proposition 9.1]:

Theorem 5.2. *The set of values S of $k(a)$ as a runs over $\mathbb{F}_q^*$ is*

$$S = \{ j \in \mathbb{Z} \,|\, |j| < 2\sqrt{q} \text{ and } j \equiv -1 \pmod 4 \}.$$

Moreover, each value $j \in S$ is attained exactly $H(j^2 - 4q)$ times where $H(d)$ is the Kronecker class number of d.

As a corollary we obtain, by using Theorem 2.5, the weight distribution of $C(r,3)$:

Theorem 5.3. *The weight distribution of $C(r,3)$ is given in the following table where j runs over the set $\{|j| < 2^{(r+2)/2}$ and $j \equiv -1 \pmod 4\}$:*

weight	*frequency*
0	1
$2^r(2^{r-1}-1)$	$3(2^r-1)^2$
$2^{r-1}(2^r-1)$	$3(2^r-1)$
$(2^r(2^r-1)-j^2+1)/2$	$H(j^2-2^{r+2})(2^r-1)^2$

To give the weight distribution of $C^\perp(r,3)$ we denote by K_h the hth moment of the Kloosterman sum $k(a)$ over the field $\mathbb{F}$, i.e.

$$K_h = \sum_{a \in \mathbb{F}^*} k(a)^h,$$

and use the following result from [10] which was proved by using results from [14]:

Theorem 5.4. *Let $q = 2^r$. Then*

$$\begin{aligned}
&K_0 = q-1, \quad K_1 = 1, \quad K_2 = q^2 - q - 1, \quad K_3 = \pm q^2 + 2q + 1,\\
&K_4 = 2q^3 - 2q^2 - 3q - 1,\\
&K_5 = (t_7 \pm 4)q^3 + 5q^2 + 4q + 1,\\
&K_6 = 5q^4 - (5 + (-1)^r)q^3 - 9q^2 - 5q - 1,\\
&K_7 = (t_9 + 6t_7 \pm 14 + 1)q^4 + 14q^3 + 14q^2 + 6q + 1,\\
&K_8 = 14q^5 - (15 \pm 7)q^4 - 28q^3 - 20q^2 - 7q - 1,\\
&K_9 = (t_{11} + 8t_9 + 27t_7 + 8 \pm 48)q^5 + 42q^4 + 48q^3 + 27q^2 + 8q + 1,\\
&K_{10} = 42q^6 - (51 \pm 35)q^5 - 90q^4 - 75q^3 - 35q^2 - 9q - 1 + 2048\tau(q/4) - \tau(q),
\end{aligned}$$

where $\pm$ denotes $(-1)^r$, $t_7 = \alpha_7^r + \bar{\alpha}_7^r$ with $\alpha_7 = (1+\sqrt{-15})/4$, $t_9 = \alpha_9^r + \bar{\alpha}_9^r$ with $\alpha_9 = (-5+\sqrt{-39})/8$, $t_{11} = \beta_{11}^r + \bar{\beta}_{11}^r + \eta_{11}^r + \bar{\eta}_{11}^r$, with $\beta_{11} = \big(-3+\sqrt{505}+\sqrt{-510-6\sqrt{505}}\big)/32$, $\eta_{11} = \big(-3-\sqrt{505}+\sqrt{-510+6\sqrt{505}}\big)/32$, and τ is the Ramanujan's tau-function.

Remark. It is not hard to see that

$$\tau(q) - 2048\tau(q/4) = \mu_2^r + \bar{\mu}_2^r = D_r(-24, 2048),$$

where $\mu_2 = -12 + 4\sqrt{-119}$ and $D_r(x, 2048)$ is the Dickson polynomial of the first kind of degree r with parameter 2048 (see [11, Section 2]).

Theorem 5.5. *For every non-negative integer h the number $C_h^\perp$ of codewords of weight h in the dual $C^\perp(r,3)$ of $C(r,3)$ is given by*

$$\begin{aligned}
q^3 h! C_h^\perp = f(C_0^\perp, \ldots, C_{h-1}^\perp) + g(M_0, \ldots, M_h) +\\
3(q-1)^2(-q)^h((q-2)^h + (q-1)^{h-1}),
\end{aligned}$$

where

$$f(C_0^\perp,\dots,C_{h-1}^\perp)=q^3\sum_{i=0}^{h-1}(-1)^{h+i+1}C_i^\perp\sum_{t=i}^{h}t!S(h,t)2^{h-t}\binom{n-i}{n-t},$$

$$g(M_0,\dots,M_h)=\sum_{j=0}^{h}\binom{h}{j}(-1)^{j+h}(q-1)^{2(h-j+1)}\sum_{i=0}^{j}\binom{j}{i}(-q)^{j-i}K_{2i}.$$

Especially,

$$\begin{aligned}
&C_0^\perp=1,\ C_1^\perp=C_2^\perp=0,\ C_3^\perp=(q-1)^2(2q-5\mp 1)/3!,\\
&C_4^\perp=(q-1)^2(q^3-6q^2+(17\mp 3)q-24)/4!,\\
&C_5^\perp=(q-1)^2(q^5-8q^4+14q^3+24q^2-4(7\pm 5)q-109\mp 10\\
&\qquad\qquad +(2048\tau(q/4)-\tau(q))/q^3)/5!.
\end{aligned}$$

Proof. The moments M_j in Theorem 2.8 are, by Lemma 5.1, of the form

$$\begin{aligned}
M_j&=\sum_{l=0}^{q-2}(k(g^l)^2-q)^j=\sum_{l=0}^{q-2}\sum_{i=0}^{j}\binom{j}{i}k(g^l)^{2i}(-q)^{j-i}\\
&=\sum_{i=0}^{j}\binom{j}{i}(-q)^{j-i}\sum_{l=0}^{q-2}k(g^l)^{2i}\\
&=\sum_{i=0}^{j}\binom{j}{i}(-q)^{j-i}K_{2i},
\end{aligned}$$

and the first claim follows now by Theorem 2.8. The validity of the formulae for the number of low-weight codewords can be verified by using *Mathematica*. ☐

Remark. By Theorem 5.2, moments K_h can be calculated effectively for each non-negative integer h by

$$K_h=\sum_{\substack{|j|<2\sqrt{q}\\ j\equiv -1\ (4)}}H(j^2-4q)j^h,$$

provided that r is not too large (a "$H(d)$-calculator" can be found in [7]).

6. Acknowledgments. The author would like to thank the anonymous reviewers for their detailed comments.

REFERENCES

[1] L. Carlitz, *A note on exponential sums*, Pacific J. Math., 30 (1969), pp. 35–37.
[2] L. Carlitz, *Explicit evaluation of certain exponential sums*, Math. Scand., 44 (1979), pp. 5–16.
[3] K. Chinen and T. Hiramatsu, *Hyper-Kloosterman sums and their applications to the coding theory*, Appl. Algebra Eng. Commun. Comput., 12 (2001), pp. 381–390.
[4] K. Chinen, *On some properties of the hyper-Kloosterman codes*, Tokyo J. Math., 26 (2003), pp. 55–65.
[5] G. Lachaud and J. Wolfmann, *The weights of orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory, 36 (1990), pp. 686–692.
[6] F. J. MacWilliams and N. J .A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam: North-Holland, 1977.

[7] K. Matthews, *Some BCMath/PHP number theory programs*, Available: http://www.numbertheory.org/php

[8] M. Moisio, *A note on evaluations of some exponential sums*, Acta Arith., 93 (2000), pp. 117–119.

[9] M. Moisio, *On the number of rational points on some families of Fermat curves over finite fields*, Finite Fields Appl., 13 (2007), pp. 546–562.

[10] M. Moisio, *The moments of a Kloosterman sum and the weight distribution of a Zetterberg type binary cyclic code*, IEEE Trans. Inform. Theory, 53 (2007), pp. 843–847.

[11] M. Moisio, *On the moments of Kloosterman sums and fibre products of Kloosterman curves*, Finite Fields Appl., to appear.

[12] C.J. Moreno and O. Moreno, *The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 1894–1907.

[13] V. Pless, *Power moment identities on weight distributions in error correcting codes*, Information and Control, 6 (1963), pp. 147–152.

[14] R. Schoof and M. van der Vlugt, *Hecke operators and the weight distributions of certain codes*, J. Combin. Theory Ser., A 57 (1991), pp. 163–186.