Proceedings of the Jangjeon Mathematical Society
27 (2024), No. 4, pp. 871 – 879

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2024.27.4.871

A RECURSIVE FORMULA FOR WEIGHT DISTRIBUTION OF HAMMING CODES

DAE SAN KIM

ABSTRACT. We derive a recursive formula determining the weight distribution of the $[n=(q^m-1)/(q-1),\ n-m,\ 3]$ Hamming code $H(m,\ q)$. Here q is a prime power. The proof is based on Moisio's idea of using Pless power moment identity together with exponential sum techniques. We first prove the recursive formula under the restriction $(m,q-1)=1$. Then we remove the restriction so that the formula actually holds for any positive integer m and any prime power q.

Dedicated to Professor Taekyun Kim on the Occasion of His Sixtieth Birthday

1. INTRODUCTION

This paper is a combined and enlarged version of the papers ([3], [4]), which have never been published elsewhere.

The Hamming code is probably the first one that someone encounters when he is taking a beginning course in coding theory. The q-ary Hamming code $H(m,\ q)$ is an $[n=(q^m-1)/(q-1),\ n-m,\ 3]$ code which is a single-error-correcting perfect code. From now on, q will indicate a prime power unless otherwise stated. Also, we assume $m>1$.

In [6], Moisio discovered a handful of new power moments of Kloosterman sums over $\mathbb{F}_q$, with $q=2^r$. This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and frequencies of weights in the binary Zetterberg code of length $q+1$, which were known by the work of Schoof and van der Vlugt in [10]. Some new moments of Kloosterman sums were also found over $\mathbb{F}_q$, with $q=3^r$, by connecting those in the ternary Melas code of length $q-1$ ([7],[11]).

In this paper, we adopt Moisio's idea of utilizing Pless power moment identity and exponential sum techniques and prove the recursive formula in the following theorem giving the weight distribution of $H(m,q)$. We first show this under the restriction $(m,q-1)=1$. Then we remove this restriction so that it actually holds for any positive integer m and any prime power q.

2010 *Mathematics Subject Classification.* 94B05; 94B15; 11T23.

Key words and phrases. Hamming code; weight distribution; Pless power moment identity; exponential sum.

Theorem 1.1. *Let* $\{C_h\}_{h=0}^{n}(n=(q^m-1)/(q-1))$ *denote the weight distribution of the q-ary Hamming code* $H(m,\ q)$. *Then, for h with* $1 \le h \le n$,

$$\begin{aligned} h!C_h =&(-1)^h q^{m(h-1)}(q^m-1)\\ &+\sum_{i=0}^{h-1}(-1)^{h+i-1}C_i\sum_{t=i}^{h}t!S(h,t)q^{h-t}(q-1)^{t-i}\tbinom{n-i}{n-t}, \end{aligned}$$

where $S(h,t)$ *denotes the Stirling number of the second kind defined by*

$$S(h,t)=\frac{1}{t!}\sum_{j=0}^{t}(-1)^{t-j}\tbinom{t}{j}j^h. \tag{1}$$

$C_0=1$, and it is easy to check that $C_1=C_2=0$, as it should be. A few next values of C_h's were obtained, with the help of *Mathematica*, from the above formula.

Corollary 1.2. *Let* $\{C_h\}_{h=0}^{n}(n=(q^m-1)/(q-1))$ *denote the weight distribution of the q-ary Hamming code* $H(m,q)$. *Then*

$$\begin{aligned} C_3 =&\frac{1}{3!}(q^m-1)(-q+q^m),\\ C_4 =&\frac{1}{4!}(q^m-1)(-6q+5q^2+6q^m+q^{2m}-6q^{1+m}),\\ C_5 =&\frac{1}{5!}(q^m-1)(-36q+54q^2-26q^3+36q^m+6q^{2m}\\ &+q^{3m}-60q^{1+m}+35q^{2+m}-10q^{1+2m}),\\ C_6 =&\frac{1}{6!}(q^m-1)(-240q+500q^2-450q^3+154q^4\\ &+240q^m+20q^{2m}+10q^{3m}+q^{4m}-520q^{1+m}\\ &+85q^{2(1+m)}+550q^{2+m}-225q^{3+m}-110q^{1+2m}\\ &-15q^{1+3m}),\\ C_7 =&\frac{1}{7!}(q^m-1)(-1800q+4710q^2-6035q^3+3940q^4\\ &-1044q^5+1800q^m-90q^{2m}+85q^{3m}+15q^{4m}\\ &+q^{5m}-4620q^{1+m}+1505q^{2(1+m)}+6755q^{2+m}\\ &-5215q^{3+m}+1624q^{4+m}-805q^{1+2m}-735q^{3+2m}\\ &-245q^{1+3m}+175q^{2+3m}-21q^{1+4m}), \end{aligned}$$

$$\begin{aligned}
C_8 =&\frac{1}{8!}(q^m-1)(-15120q+47124q^2-77196q^3+72779q^4\\
&-37240q^5+8028q^6+15120q^m-3276q^{2m}+840q^{3m}\\
&+175q^{4m}+21q^{5m}+q^{6m}-43848q^{1+m}\\
&+17934q^{2(1+m)}-1960q^{3(1+m)}+79632q^{2+m}\\
&+6769q^{2(2+m)}-87808q^{3+m}+52661q^{4+m}\\
&-13132q^{5+m}-3276q^{1+2m}-19236q^{3+2m}\\
&-3080q^{1+3m}+4270q^{2+3m}-476q^{1+4m}+322q^{2+4m}\\
&-28q^{1+5m}),\\
C_9 =&\frac{1}{9!}(q^m-1)(-141120q+507024q^2-1002736q^3\\
&+1221444q^4-910644q^5+382088q^6-69264q^7\\
&+141120q^m-57456q^{2m}+10864q^{3m}+1960q^{4m}\\
&+322q^{5m}+28q^{6m}+q^{7m}-449568q^{1+m}\\
&+165396q^{2(1+m)}-67116q^{3(1+m)}+957936q^{2+m}\\
&+246624q^{2(2+m)}-1349404q^{3+m}+1175874q^{4+m}\\
&-571116q^{5+m}+118124q^{6+m}+33936q^{1+2m}\\
&-332584q^{3+2m}-67284q^{5+2m}-39396q^{1+3m}\\
&+74844q^{2+3m}+22449q^{4+3m}-7812q^{1+4m}\\
&+10332q^{2+4m}-4536q^{3+4m}-840q^{1+5m}\\
&+546q^{2+5m}-36q^{1+6m}),\\
C_{10} =&\frac{1}{10!}(q^m-1)(-1451520q+5880384q^2-13550832q^3\\
&+20090832q^4-19485852q^5+11984244q^6\\
&-4251240q^7+663696q^8+1451520q^m-893376q^{2m}\\
&+174384q^{3m}+21504q^{4m}+4536q^{5m}+546q^{6m}\\
&+36q^{7m}+q^{8m}-4987008q^{1+m}+857520q^{2(1+m)}\\
&-1569540q^{3(1+m)}+63273q^{4(1+m)}+12035088q^{2+m}\\
&+5797770q^{2(2+m)}-20393616q^{3+m}+723680q^{2(3+m)}\\
&+23050848q^{4+m}-16423398q^{5+m}+6661236q^{6+m}\\
&-1172700q^{7+m}+1341360q^{1+2m}-4686480q^{3+2m}\\
&-3264780q^{5+2m}-576240q^{1+3m}+1233960q^{2+3m}\\
&+1030260q^{4+3m}-269325q^{5+3m}-117012q^{1+4m}\\
&+227808q^{2+4m}-196392q^{3+4m}-17430q^{1+5m}\\
&+22260q^{2+5m}-9450q^{3+5m}-1380q^{1+6m}\\
&+870q^{2+6m}-45q^{1+7m}).
\end{aligned}$$

The Hamming code was discovered by Hamming in late 1940's. So it is surprising that there are no such recursive formulas determining the weight distributions of the Hamming codes in the nonbinary cases. In the binary case, we have the following well known formula which follows from elementary combinatorial reasoning([5, p. 129]).

Theorem 1.3. *Let $\{C_h\}_{h=0}^{n}(n=(2^m-1))$ denote the weight distribution of the binary Hamming code $H(m,2)$. Then the weight distribution satisfies the following recurrence relation:*

$$C_0=1,\ C_1=0,$$
$$(i+1)C_{i+1}+C_i+(n-i+1)C_{i-1}=\tbinom{n}{i}\ (i\geq 1).$$

It is known ([9]) that, when $(m,q-1)=1$, $H(m,q)$ is a cyclic code.

Theorem 1.4. *Let $n=(q^m-1)/(q-1)$, where $(m,q-1)=1$. Let γ be a primitive element of $\mathbb{F}_{q^m}$. Then the cyclic code of length n with the defining zero γ^{q-1} is equivalent to the q-ary Hamming code $H(m,q)$.*

2. Preliminaries

Let $q=p^r$ be a prime power. Then we will use the following notations throughout this paper.

$$\begin{aligned}
tr(x) =& x+x^p+\cdots+x^{p^{r-1}}\\
&\quad the\ trace\ function\ \mathbb{F}_q\to\mathbb{F}_p,\\
Tr(x) =& x+x^q+\cdots+x^{q^{m-1}}\\
&\quad the\ trace\ function\ \mathbb{F}_{q^m}\to\mathbb{F}_q,\\
\lambda(x) =& e^{\frac{2\pi i}{p}tr(x)}\\
&\quad the\ canonical\ additive\ character\ of\ \mathbb{F}_q,\\
\lambda_m(x) =& \lambda(Tr(x))\\
&\quad the\ canonical\ additive\ character\ of\ \mathbb{F}_{q^m}.
\end{aligned}$$

The following lemma is well known.

Lemma 2.1. *For any $\alpha\in\mathbb{F}_q$,*

$$\sum_{x\in\mathbb{F}_q}\lambda(\alpha x)=\begin{cases} q, & \alpha=0,\\ 0, & \alpha\neq 0.\end{cases}$$

For a positive integer s, the multiple Kloosterman sum $K_s(\alpha)$ $(\alpha\in\mathbb{F}_q^*)$, is defined by

$$K_s(\alpha)=\sum_{x_1,\cdots,x_s\in\mathbb{F}_q^*}\lambda(x_1+\cdots+x_s+\alpha x_1^{-1}\cdots x_s^{-1}).$$

The following result follows immediately from Lemma 2.1.

Lemma 2.2. *For an integer $s>1$,*

$$\sum_{\alpha\in\mathbb{F}_q^*}K_{s-1}(\alpha)=(-1)^s.$$

Proof. $\sum_{\alpha\in\mathbb{F}_q^*} K_{s-1}(\alpha) = (\sum_{x\in\mathbb{F}_q^*}\lambda(x))^s$. □

The following lemma is immediate.

Lemma 2.3. *Let $(m,q-1)=1$. Then the following map is a bijection.*

$$\alpha \mapsto \alpha^m : \mathbb{F}_q^* \to \mathbb{F}_q^*.$$

Theorem 2.4 (Thm. 3 of [8])**.** *For any $\alpha\in\mathbb{F}_{q^m}^*$,*

$$\sum_{x\in\mathbb{F}_{q^m}^*} \lambda_m(\alpha x^{q-1}) = (-1)^{m-1}(q-1)K_{m-1}(N(\alpha)),$$

where N denotes the norm map $N:\mathbb{F}_{q^m}^*\to\mathbb{F}_q^*$, defined by $N(\alpha)=\alpha^n$, with $n=(q^m-1)/(q-1)$.

The following theorem is due to Delsarte([5, P. 208]).

Theorem 2.5 (Delsarte)**.** *Let B be a linear code of length n over $\mathbb{F}_{q^m}$. Then*

$$(B|_{\mathbb{F}_q})^\perp = Tr(B^\perp).$$

The following is a special case of the result stated in [1, Thm. 4.2], although only the binary case is mentioned there. In fact, using Theorem 2.5 above, this can be proved in exactly the same manner as described immediately after the proof of Theorem 4.2 in [1].

Theorem 2.6. *The dual $H(m,q)^\perp$ of $H(m,q)$ is given by*

$$\begin{aligned} &H(m,q)^\perp \\ &= \{c(a) = (Tr(a), Tr(a\gamma^{(q-1)}), \cdots, Tr(a\gamma^{(n-1)(q-1)})) \\ &\qquad |a\in\mathbb{F}_{q^m}\}. \end{aligned}$$

Lemma 2.7. *The map $a\mapsto c(a):\mathbb{F}_{q^m}\to H(m,q)^\perp$ is an isomorphism of $\mathbb{F}_q$-vector spaces.*

Proof. The map is $\mathbb{F}_q$-linear, surjective and $dim_{\mathbb{F}_q}\mathbb{F}_{q^m} = dim_{\mathbb{F}_q}H(m,q)^\perp$. □

Our recursive formula in Theorem 1.1 will be a consequence of the application of Pless power moment identity([9]), which is equivalent to MacWilliams identity.

Theorem 2.8 (Pless power moment identity)**.** *Let C be an q-ary $[n,k]$ code, and let C_i (resp. $C_i^\perp$) denote the number of codewords of weight i in C (resp. in $C^\perp$). Then, for $h=0,1,2,\cdots$,*

$$\sum_{i=0}^{n} i^h C_i = \sum_{i=0}^{min\{n,h\}} (-1)^i C_i^\perp \sum_{t=i}^{h} t!S(h,t)q^{k-t}(q-1)^{t-i}\tbinom{n-i}{n-t}, \tag{2}$$

where $S(h,t)$ denotes the Stirling number of the second kind defined by (1).

3. Proof of Theorem 1.1 when $(m,q-1)=1$

In our discussion below, we will assume that $(m,q-1)=1$, so that $H(m,q)$ is a cyclic code with the defining zero γ^{q-1}, where γ is a primitive element of $\mathbb{F}_{q^m}$.

Let h be an integer with $1\le h\le n$. Observe that the weight of the codeword $c(a)$, $(a\in\mathbb{F}_{q^m}^*)$, in Theorem 2.6 can be expressed as

$$
\begin{aligned}
w(c(a)) =& \sum_{i=0}^{n-1}(1-q^{-1}\sum_{\alpha\in\mathbb{F}_q}\lambda(\alpha Tr(a\gamma^{i(q-1)})))\\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Lemma 2.1)}\\
=&n-q^{-1}\sum_{\alpha\in\mathbb{F}_q}\sum_{i=0}^{n-1}\lambda_m(\alpha a\gamma^{i(q-1)})\\
=&n-q^{-1}(q-1)^{-1}\sum_{\alpha\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^m}^*}\lambda_m(\alpha a x^{q-1})\\
=&n-q^{-1}(q-1)^{-1}(q^m-1)-q^{-1}(q-1)^{-1}\\
&\times\sum_{\alpha\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^m}^*}\lambda_m(\alpha a x^{q-1})\\
=&n-q^{-1}(q-1)^{-1}(q^m-1)+(-1)^m q^{-1}\\
&\times\sum_{\alpha\in\mathbb{F}_q^*}K_{m-1}(\alpha^m N(a)) \qquad \text{(by Theorem 2.4)}\\
=&n-q^{-1}(q-1)^{-1}(q^m-1)+(-1)^m q^{-1}\\
&\times\sum_{\alpha\in\mathbb{F}_q^*}K_{m-1}(\alpha N(a)). \qquad \text{(by Lemma 2.3)}
\end{aligned}
\tag{3}
$$

We now apply Pless power moment identity in Theorem 2.8 with $C = H(m,q)^{\perp}$. On the one hand, the left hand side of (2) is

$$
\begin{aligned}
&\sum_{a\in\mathbb{F}_{q^m}^*} w(c(a))^h \qquad\qquad\qquad\qquad \text{(by Lemma 2.7)}\\
=&\sum_{a\in\mathbb{F}_{q^m}^*}(n-q^{-1}(q-1)^{-1}(q^m-1)+(-1)^m q^{-1}\\
&\times\sum_{\alpha\in\mathbb{F}_q^*}K_{m-1}(\alpha N(a)))^h \qquad\qquad \text{(by (3))}\\
=&\frac{q^m-1}{q-1}\sum_{a\in\mathbb{F}_q^*}(n-q^{-1}(q-1)^{-1}(q^m-1)+(-1)^m q^{-1}\\
&\times\sum_{\alpha\in\mathbb{F}_q^*}K_{m-1}(\alpha a))^h\\
=&(q^m-1)(n-q^{-1}(q-1)^{-1}(q^m-1)+(-1)^m q^{-1}\\
&\times\sum_{\alpha\in\mathbb{F}_q^*}K_{m-1}(\alpha))^h\\
=&(q^m-1)(n-q^{-1}(q-1)^{-1}(q^m-1)+q^{-1})^h\\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Lemma 2.2)}\\
=&q^{(m-1)h}(q^m-1)\ (as\ n=\frac{q^m-1}{q-1}).
\end{aligned}
$$

On the other hand, by separating the term corresponding to h and noting $S(h,h)=1$, the right hand side of (2) is

$$\begin{aligned}&(-1)^h C_h h! q^{m-h}\\&+\sum_{i=0}^{h-1}(-1)^i C_i \sum_{t=i}^{h} t! S(h,t) q^{m-t}(q-1)^{t-i}\tbinom{n-i}{n-t}.\end{aligned}$$

So

$$\begin{aligned}&q^{(m-1)h}(q^m-1)\\&\quad=(-1)^h C_h h! q^{m-h}\\&\qquad+\sum_{i=0}^{h-1}(-1)^i C_i \sum_{t=i}^{h} t! S(h,t) q^{m-t}(q-1)^{t-i}\tbinom{n-i}{n-t}.\end{aligned}\tag{4}$$

Multiplying both sides of (4) by $(-1)^h q^{h-m}$, we get the desired result. ■

4. Proof of Theorem 1.1 without the restriction $(m,q-1)=1$

We know that the formula in Theorem 1.1 holds for $(m,q-1)=1$. By the recursive formula in Theorem 1.1, we see that all C_i $(i=0,1,2,\cdots,\ n=(q^m-1)/(q-1))$ are formally polynomials in q with rational coefficients, which depend on m (cf. Corollary 1.2 for the explicit expressions of C_i for $i\le 10$). Put $C_i=P_i(q;m)$, for $i=0,1,2,\cdots,\ n=(q^m-1)/(q-1)$. Then (1.1) can be rewritten as

$$\begin{aligned}&h!P_h(q;m)=(-1)^h q^{m(h-1)}(q^m-1)+\\&\sum_{i=0}^{h-1}(-1)^{h+i+1}P_i(q;m)\sum_{t=i}^{h} t! S(h,t) q^{h-t}(q-1)^{t-i}\begin{pmatrix}\frac{q^m-1}{q-1}-i\\ t-i\end{pmatrix},\end{aligned}\tag{5}$$

$(1\le h\le n=(q^m-1)/(q-1))$.

Let m, h be fixed positive integers. Then the left hand side and the right hand side of (5) are formally polynomials in q and (5) is valid whenever q is replaced by prime powers p^r satisfying $(m,p^r-1)=1$ and $h\le(p^{rm}-1)/(p^r-1)$.

So it is enough to show that there are infinitely many prime powers p^r such that $(m,p^r-1)=1$, since then (5) is really a polynomial identity in q, so that the restriction of our concern can be removed. There are three cases to be considered.

Case 1) 2 does not divide m.
Let $m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, where $p_1,p_2,\cdots,p_r$ are distinct odd primes and e_j's are positive integers. Then, by Dirichlet's theorem on arithmetic progressions, there are infinitely many prime numbers p such that $p\equiv 2 \pmod m$. For each such an p, $p\equiv 2 \pmod{p_j}$, for $j=1,\cdots,r$. Then p_j does not divide $p-1$, for all j, so that all p_j is relatively prime to $p-1$. So $(m,p-1)=1$, for all such primes p.

Case 2) 2 is the only prime divisor of m.
In this case, $2^l-1(l=1,2,\cdots)$ are all relatively prime to m.

Case 3) 2 and some odd prime divide m.
Let $m=2^e m_1$, $m_1=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, where $e,e_1,\cdots,e_r,r$ are positive integers and $p_1,p_2,\cdots,p_r$ are distinct odd primes. Noting that $(2,m_1)=1$, we let $f=ord_{m_1}2$ be the order of 2 modulo m_1. Then $2^{lf}\equiv 1 \pmod{m_1}$, for all positive integers l. So $2^{lf}\equiv 1 \pmod{p_j}$, for all $j=1,\cdots,r$. Thus $2^{lf+1}\equiv 2 \pmod{p_j}$, for all j, and

hence p_j does not divide $2^{lf+1}-1$, for all j. This implies that $(m, 2^{lf+1}-1)=1$, for all positive integers l. ■

5. Further remark

Here we remark that the weight distribution of $H(m,q)$ is well known, which is given in terms of Krawtchouk polynomials. Krawtchouk polynomials are discrete orthogonal polynomials associated with coding theory and binomial distribution, which was introduced by Krawtchouk in 1929. They are defined by

$$K_k^{n,q}(x)=\sum_{j=0}^{k}(-1)^j(q-1)^{k-j}\binom{x}{j}\binom{n-x}{k-j}, \quad (0\le k\le n), \tag{6}$$

which has degree k. Among other things, they satisfy the orthogonality relations:

$$\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_r^{n,q}(i)K_s^{n,q}(i)=q^n(q-1)^r\binom{n}{r}\delta_{r,s}.$$

The following formula is known to be equivalent to the Pless power moment identity in Theorem 2.8 ([2, p. 257]).

Theorem 5.1. *Let C be an q-ary $[n,k]$ code, and let C_i (resp. $C_i^{\perp}$) denote the number of codewords of weight i in C (resp. in $C^{\perp}$). Then, for $0\le k\le n$,*

$$C_k^{\perp}=\frac{1}{|C|}\sum_{i=0}^{n}C_iK_k^{n,q}(i). \tag{7}$$

Let C be the $[n=(q^m-1)/(q-1),m]$ q-ary simplex code. Then dual code $C^{\perp}$ is the Hamming code $H(m,q)$. It is known that the weight distribution of C is $C_0=1, C_{q^{m-1}}=q^m-1$, and $C_i=0$, for all other i ([2, Theorem 2.7.5]). Now, from (6) and (7), it is immediate to see that, for $0\le k\le n$,

$$\begin{aligned}C_k^{\perp}&=q^{-m}\Big(K_k^{n,q}(0)+(q^m-1)K_k^{n,q}(q^{m-1})\Big)\\&=q^{-m}\Big((q-1)^k\binom{n}{k}+(q^m-1)K_k^{n,q}(q^{m-1})\Big).\end{aligned}$$

6. Conclusion

As we remarked in Section 5, the weight distribution of the Hamming code $H(m,q)$ is well known, which can be described in terms of Krawtchouk polynomials $K_k^{n,q}(x)$. In the binary case, there has been a recursive formula, which follows from simple combinatorial reasoning, giving the weight distribution of the Hamming codes. However, it is surprising that there have been no recursive formulas giving the weight distributions of the Hamming codes in the nonbinary case. In this paper, we were able to derive the recursive formula in Theorem 1.1 by adopting Moisio's idea of using the Pless power moment idnetity and exponential sum techniques.

References

[1] I. Honkala and A. Tietäväinen, *Codes and number theory, in Handbook of Coding Theroy vol. II, V. S. Pless and W. C. Huffman, Eds.,* North-Holland, Amsterdam, 1998, 1141-1194.

[2] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[3] D. S. Kim, *Weight distributions of Hamming codes*, arXiv:0710.1467 [cs.IT].

[4] D. S. Kim, *Weight distributions of Hamming codes II*, arXiv:0710.1469 [cs.IT].

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes,* North-Holland, Amsterdam, 1998.

[6] M. Moisio, *The moments of a Kloosterman sum and the weight distribution of a Zetterberg type binary cyclic code,* IEEE Trans. Inf. Theory **IT-53** (2007), 843-847.

[7] M. Moisio, *On the moments of Kloosterman sums and fibre products of Kloosterman curves,* Finite Fields Appl. **14** (2008), no. 2, 515-531.

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

[9] V. S. Pless, W. C. Huffman, and R. A. Brualdi, *An introduction to algebraic codes, in Handbook of Coding Theroy vol. I, V. S. Pless and W. C. Huffman, Eds.,* North-Holland, Amsterdam, 1998, 3-139.

[10] R. Schoof and M. van der Vlugt, *Hecke operators and the weight distribution of certain codes,* J. Combin. Theroy Ser. A **57** (1991), 163-186.

[11] G. van der Geer, R. Schoof and M. van der Vlugt, *Weight formulas for ternary Melas codes,* Math. Comp. **58** (1992), 781-792.

Department of Mathematics, Sogang University, Seoul 121-742, Republic of Korea

Email address: dskim@sogang.ac.kr