Hokkaido Mathematical Journal Vol. 9 (1980) p. 138-139

A note on symmetric codes over $GF(3)$

By Noboru ITO*

(Received September 26, 1979)

Let q be a prime power such that $q\equiv 2 \pmod 3$ and $q\equiv 1 \pmod 4$, $GF(q)$ a field of q elements and μ the quadratic character of $GF(q)^{X}$ with $\mu(0)=0$.

Let T be a matrix of degree q defined by $T(a, b)=\mu(b-a)$, where $a, b\in GF(q)$, and

$$S=\begin{pmatrix} 0 & 1\cdots 1 & 1 \\ 1 & & \\ \vdots & T & \\ 1 & & \\ 1 & & \end{pmatrix}.$$

Let $C(q)$ be the code generated by (I, S) over $GF(3)$, which is introduced by V. Pless in [3] and I denotes the identity matrix of degree $q+1$.

The purpose of this note is to show that the minimum weight of $C(q)$ is not smallet than $\sqrt{q}$.

§ 1. Let $C^{*}(q)$ be the code generated by (I, S) over $GF(3^{2})$. Let i be a primitive fourth root of unity in $GF(3^{2})$. Then we may choose

$$\begin{pmatrix} -I-iS, & iI-S \\ -I+iS, & -iI-S \end{pmatrix}$$

as generators of $C^{*}(q)$, since $(-S, I)$ is contained in $C(q)$ (See [3]). We notice that $-i(-I-iS)=iI-S$ and $i(-I+iS)=-iI-S$. Let U and L be the subcodes of $C^{*}(q)$ generated by $(-I-iS, iI-S)$ and $(-I+iS, -iI-S)$ respectively. Then any codevector of $C^{*}(q)$ has a form $(x+y, -i(x-y))$, where $(x, -ix)\in U$ and $(y, iy)\in L$.

LEMMA 1. *Let w denote the weight function. Then we have that*

$$w\Big(x+y,\ -i(x-y)\Big)\geqq w(x) \text{ and } w(y).$$

PROOF. We may label elements of $GF(3^{2})$ as follows: $a_{1}=0$, $a_{2}=1$, $a_{3}=-1$, $a_{4}=i$, $a_{5}=i+1$, $a_{6}=i-1$, $a_{7}=-i$, $a_{8}=-i+1$ and $a_{9}=-i-1$. Now let n_i be the number of a_i in x and n_{ij} the number of a_j in the portion of y which corresponds to n_i coordinates of x giving a_i $(i, j=1, \cdots, 9)$. Then we have that $w(x)=n_2+\cdots+n_9$, $w(y)=n_{12}+\cdots+n_{19}+n_{22}+\cdots+n_{29}+\cdots+n_{92}+\cdots+n_{99}$, $w(x+y)=n_{12}+\cdots+n_{19}+n_{21}+n_{22}+n_{24}+\cdots+n_{29}+\cdots+n_{91}+\cdots+n_{94}+n_{96}+\cdots+n_{99}$ and $w(x-y)=n_{12}+\cdots+n_{19}+n_{21}+n_{23}+\cdots n_{29}+\cdots+n_{91}+\cdots+n_{98}$. Thus we have that $w(x+y, \ -i(x-y))=2(n_{12}+\cdots+n_{19})+(2(n_{21}+\cdots+n_{29})-n_{22}-n_{23}+\cdots+2(n_{91}+\cdots+n_{99})-n_{95}-n_{99}\geqq w(x)$ and $w(y)$.

$-I-iS$ and $-I+iS$ are equivalent under the field automorphism, and so they have the same minimum weight.

§ 2. The minimum weight of $-I_1-iT$ is equal to or smaller than by one that of $-I-iS$, where I_1 is the identity matrix of degree q. Now let G be a generalized quadratic residue code of J. H. van Lint and F. J. McWilliams [2] of $GF(q)$ over $GF(3^2)$. Since $(1, \cdots, 1)$ belongs to both $-I_1-iT$ and G, and since $G=(-I-iT)+J$, where J is the all 1 matrix of degree q, we see that $-I_1-iT$ is a generator for G. Thus by a theorem of J. H. van Lint and F. J. McWilliams [2, Theorem 2, *i*] the minimum weight of $-I-iT$ is at least $\sqrt{q}$.

Remark. The case $q\equiv 3 \pmod 4$ is treated in [1].

Bibliography

[1] N. Ito: Note on symmetry code over $GF(3)$, to appear in JCT (A).

[2] J. H. van Lint and F. J. MacWilliams: Generalized quadratic residue codes, IEEE Trans. Inf. Th. IT 24 (1978) 730–737.

[3] V. Pless: Symmetry codes over $GF(3)$ and new five-designs, JCT (A) 12 (1972), 119–142.

Department of Mathematics
University of Illinois at Chicago Circle

* This work is partially supported by NSF Grant MCS 7902750