数理解析研究所講究録
第 786 巻 1992 年 22-26

On the existence of pseudo-cyclic MDS codes

名城大学短期大学部 丸田辰哉 (Tatsuya Maruta)

本稿では pseudo-cyclic MDS codes の存在性について、特に次元 3 の場合の最近の結果を報告する。

p を素数，$q=p^h$ (h: 正整数)，$F=GF(q)$，C : (n,k)-MDS code over F (i.e. F^n の k 次元部分空間) とする。C の最小距離 d に関して

Singleton bound : $d \le n-k+1$

がよく知られている。C が $d=n-k+1$ をみたすとき，C は maximum distance separable (MDS) であるという。

以下 $3 \le k \le q$ とする。

(n,k)-MDS codes over F の存在性については q : even かつ $k=3$ or $q-1$ のとき以外は $n \le q+1$ が存在するための必要十分条件であると予想されており，k に比して q が十分大きい場合及びいくつかの次元の場合について幾何学的に証明されている。詳細は [4], [3, §§27] を参照。

MDS code の中で最も有名なものの 1 つに Reed-Solomon code がある。これは長さ $q-1$ の cyclic MDS code over F である。では，他の長さの cyclic MDS code はどれ程存在するのだろうか。

まず、(n,k)-MDS codes が存在するような n の最大値であると目される長さ $q+1$ の場合は k: even, q: odd のときは存在しないがそれ以外のときは必ず存在することが知られている([2])。ところが cyclicity を次の pseudo-cyclicity に弱めると例外なく存在することがわかる。

$F \ni \alpha \neq 0$ として $C: \alpha\text{-cyclic} \overset{\text{def}}{\Longleftrightarrow} (x_1, \cdots, x_n) \in C \Rightarrow (\alpha x_n, x_1, \cdots, x_{n-1}) \in C$

$C: \text{pseudo-cyclic} \overset{\text{def}}{\Longleftrightarrow} C: \alpha\text{-cyclic for some } \alpha \in F \setminus \{0\}$.

"pseudo-cyclic" の概念は "consta cyclic" とか "semi-cyclic" と呼ばれることもある。(n,k)-MDS code over F を調べるのに n-arc in $PG(k-1, q)$ を調べる([4]を見よ)のと同様に、cyclic code を射影幾何学的に調べようとすると pseudo-cyclic の概念の方が自然である。([5]参照)。また、cyclic であることによる有効性(decoding algorithm 等)は pseudo-cyclic にしても失なうことはないので pseudo-cyclic MDS codes の存在性について考察する。

定理1([5], [6]) $(n,q) \neq 1$ なる (n,k)-MDS code over F は $n=p$ のときに限り存在する。

従って、以下 $(n,q)=1$ とする。

定理2 $q \equiv \pm 1 \bmod n$ のとき pseudo-cyclic (n,k)-MDS code over F

は存在する。

$(n,q)=1$, $q\not\equiv\pm1 \bmod n$ の場合については、一般の k に対して調べるのが困難であるため、以下 $k=3$ とする。

定理3. C を pseudo-cyclic $(n,3)$-MDS code over F とすると、次の(i)〜(iii)のどれか1つが満たされる:

(i) $q\equiv\pm1 \bmod n$

(ii) $q^2+q+1\equiv 0 \bmod n$

(iii) $n=8t$, $q\equiv 4t-1 \bmod n$ (t: 正整数), $\exists m$: 整数; $p^m=4t-1$

(ii)の場合については次のように予想される:

予想1. $5\le n\le q-2$, $n \mid q^2+q+1$ のとき
pseudo-cyclic $(n,3)$-MDS code over F が存在する $\Leftrightarrow$ $p^2+p+1\nmid n$

これは次のような difference set に関する問題とみなすことができる: $0<k<v$, $\Gamma=\mathbb{Z}/v\mathbb{Z}$, D: Γ の k 点部分集合とする。$\{d-d' \bmod v \,;\, d\neq d'\in D\}=\{1,2,3,\dots,v-1\}$ のとき、D を (v,k)-perfect difference set という。

予想 1′. $5 \le n \le q-2$. $n \mid q^2+q+1$ のとき、$q^2+q+1 = ns$, $K = \{ms \,;\, m = 0, 1, 2, \cdots, n-1\}$ とおくと

$\exists D$: $(q^2+q+1, q+1)$-perfect difference set $\ni 0$ s.t. $|(D-j) \cap K| \le 2$ for $^\forall j \in D$

$\Leftrightarrow$ $p^2+p+1 \nmid n$.　　但し $D-j = \{d-j \in \Gamma \,;\, d \in D\}$.

定理 4. $n = 7, 13, 21$ に対して、予想 1 は真.

$n = 7, 13$ のときは cyclic で存在するが、$n = 21$ のときは cyclic では存在しない。次の結果は difference set を調べることにより証明された。

定理 5. ([1]). $q = p^h$, h : even

$\Rightarrow$ pseudo-cyclic $(q-\sqrt{q}+1, 3)$-MDS code over F は存在する.

(iii) の場合については、cyclic の場合についてのみ考えれば十分.

定理 6. $n = 8t$, $q \equiv 4t-1 \mod n$ のとき、有限個の p を除いて cyclic $(n, 3)$-MDS code over F は存在する.

“有限個の p” とはどのような p なのだろうか. $t = 1, 2, 3$

については次の予想が証明できる。

予想 2. $q \equiv 4t-1 \mod 8t$, $4t-1$: 素数 p' の巾のとき cyclic $(8t, 3)$-MDS code over F が存在する $\Longleftrightarrow$ $p \neq p'$.

$t = 4$, $4t-1 = 15 = 3 \cdot 5$ のときは "有限個の p" は 47 と 79 であることが証明される。

参考文献

[1] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas (1986), "Complete arcs in planes of square order," Annals of Discrete Math., 30, 243-250.

[2] J. Georgiades (1982), "Cyclic $(q+1, k)$-codes of odd order q and even dimension k are not optimal," Atti Sem. Mat. Fis. Univ. Modena 30, 284-285.

[3] J.W.P. Hirschfeld and J.A. Thas (1991), "General Galois Geometries," Oxford Univ. Press, Oxford.

[4] F.J. MacWilliams and N.J.A. Sloane (1977), "The Theory of Error Correcting Codes," North-Holland, Amsterdam.

[5] T. Maruta (1991), "A geometric approach to semi-cyclic codes," Advances in finite geometries and designs, Oxford Univ. Press, Oxford, 311-318.

[6] Jens P. Pedersen and Carsten Dahl (1991), "Classification of pseudo-cyclic MDS codes, IEEE Trans. Inform. Theory, 37, 365-370.