Pure Mathematics 理论数学, 2020, 10(2), 49-54
Published Online February 2020 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2020.102009

Hans汉斯

The Construction of a Class of MDS Symbol-Pair Codes over F_p

Shaopei Li, Xilin Tang

School of Mathematics, South China University of Technology, Guangzhou Guangdong
Email: li628525@163.com

Received: Jan. 17th, 2020; accepted: Feb. 4th, 2020; published: Feb. 11th, 2020

Abstract

Symbol-pair codes are designed to protect against pair error in data reading. The pair-distance is an important parameter to measure the error correction ability of the symbol pair in the symbol pair reading channel. MDS symbol pair codes are the best symbol pair codes with the largest symbol pair distance when the length and dimension of the symbol pair codes are constant. One of the important problems of symbol-pair codes is to construct MDS symbol-pair codes with a large code length and a large minimum pair-distance. In this paper, we analyze the method of characterizing pair-distance by repeated-root cyclic codes and construct a new class of MDS symbol-pair codes with different parameters and larger symbol pair-distance.

Keywords

MDS Symbol-Pair Codes, Minimum Pair-Distance, Constacyclic Codes

F_p上一类MDS符号对码的构造

李少培，唐西林

华南理工大学数学学院，广东 广州
Email: li628525@163.com

收稿日期：2020年1月17日；录用日期：2020年2月4日；发布日期：2020年2月11日

摘　要

符号对码是一类可以很好地处理在数据读取过程中出现对错误的情况的编码方法。符号对距离是衡量符号对码在符号对读取信道中的纠错能力的一个重要参数指标。在符号对码的长度和维数一定的情况下，MDS符号对码是符号对距离最大的一类最佳符号对码。符号对码的研究的主要内容之一是构造MDS符号

文章引用: 李少培, 唐西林. F_p上一类 MDS 符号对码的构造[J]. 理论数学, 2020, 10(2): 49-54.
DOI: 10.12677/pm.2020.102009

对码，特别是构造出符号对距离较大的MDS符号对码。本文分析了重根循环码的符号对距离的刻画方法，并且利用重根循环码构造出参数不同于已知构造且符号对距离较大的一类MDS符号对码。

关键词

MDS符号对码，最小符号对距离，循环码

1. 研究背景

随着高密度数据存储技术的发展，人们能够使用高分辨率的存储技术对数据进行快速的存储和读取。然而通常由于物理条件的限制，在数据的读取过程中并不总能使用高分辨率的读取设备来读取由高分辨率的写入设备所存储的数据。这种用较低的分辨率的读取头来读取通过高分辨率写入储存介质的信息的过程中，信息读取结果可能不会如一般情形一样得到单个符号，而是得到一个符号对，我们把这种信道称为符号对读取信道。具体而言，设 Σ 表示一个字符串的集合，$(x_0,x_1,\cdots,x_{n-1})$ 为待传输的码字，在符号对读取信道中该信息被读取为 $((x_0,x_1),(x_1,x_2),\cdots,(x_{n-1},x_1))$。然而，由于外界干扰等因素的影响，码字在传输的过程中可能会发生错误，使得读取出的码字的符号对中有一个和多个符号对出现错误。一个符号对错误是指在一个符号对中存在一个或两个符号的读取错误。针对这种情况，Cassuta 和 Blaum [1] [2]提出了符号对码来刻画在符号对读取信道中出现符号对错误的情况下如何设计好的码。

设 C 是 F_q^n 上长度为 n、含有 M 个向量、符号对距离是 d_P 的符号对码，记为 $(n,M,d_P)_q$ 符号对码。与经典纠错码类似，符号对距离可以反映符号对码的对错误的纠错能力，当符号对距离为 d_P 时，这个符号对码至多可以纠正 $\lfloor (d_P-1)/2 \rfloor$ 个符号对错误[2]。为了得到具有较强纠错能力的符号对码，研究人员期望构造出符号对距离较大的符号对码。另外，如何构造出码字较多的码也是编码理论的一个重要问题。如果 $2 \le d_P(C) \le n$，那么 $M \le q^{n-d_P+2}$，该上界被称为 Singleton-type 界[3]。如果 $M = q^{n-d_P+2}$，那么称 C 为最大距离可分(MDS)符号对码，记为 $(n,d_P)_q$ MDS 符号对码。

针对如何构造符号对距离较大的 MDS 符号对码的问题，2015 年，Kai [4]等人利用常循环码性质构造了一系列符号对距离为 5 和 6 的 MDS 符号对码。2016 年，Chen [5]等人通过重根循环码构造了符号对距离为 7 和 8 的 MDS 符号对码。2018 年，文献[6]进一步利用重根循环码给出了 3 类新的符号对距离为 6 和 7 的 MDS 符号对码。

本文首先分析了符号对码的相关性质，刻画了重根循环码的符号对距离，并构造出符号对距离为 7 的新参数的 MDS 符号对码。利用 Magma 软件，给出了若干 MDS 符号对码的实例并给出了具体参数，列举出决定符号对距离的码字。这些实例显示了符号对距离的码字的一些特征，将为进一步研究重根循环码的符号对距离提供参考。

2. 预备知识

设 $x=(x_0,x_1,\cdots,x_{n-1}) \in \Sigma^n$，那么 x 对应的符号对向量为

$$\pi(x)=[(x_0,x_1),(x_1,x_2),\cdots,(x_{n-1},x_0)], \tag{1.1}$$

$\pi(x)$的每一个分量(x_i,x_{i+1})被称为一个符号对，显然$\pi(x)$由x唯一确定。对$\forall(a,b),(c,d)\in\Sigma\times\Sigma$，有$(a,b)=(c,d)$当且仅当$a=b$，$c=d$。设$x=(x_0,x_1,\cdots,x_{n-1})$，$y=(y_0,y_1,\cdots,y_{n-1})\in\Sigma^n$，定义

$$d_P(x,y)=d_H(\pi(x),\pi(y)) \tag{1.2}$$

作为x，y的符号对距离，这里$d_H(\pi(x),\pi(y))$表示$\pi(x)$和$\pi(y)$的Hamming距离。关于向量$x=(x_0,x_1,\cdots,x_{n-1})$，定义$x$的符号对重量为

$$d_P(x)=\left|\{x_i\neq 0\mid x_i\in x\}\right|, \tag{1.3}$$

如果定义

$$gap(x)=\left|\left\{0\le i\le n-1\mid x_i\in F_q^*,x_{i+1}=0\right\}\right|, \tag{1.4}$$

那么可以得到x的Hamming距离和符号对距离具有关系式：

$$d_P(x)=wt_H(x)+gap(x). \tag{1.5}$$

关于$C\in\Sigma^n$的符号对距离，定义如下，

$$d_P(C)=\min\left\{d_P(x,y):\forall x,y\in C,x\neq y\right\}. \tag{1.6}$$

定理1 [7]：对任意$C\in\Sigma^n$，如果$1\le d_H(C)\le n-1$，那么$d_H+1\le d_P(C)\le 2d_H$。

线性码$C\in F_q^n$是一个λ-循环码，当且仅当C是环$F_q[x]/(x^n-\lambda)(\lambda\in F_q)$的一个理想。如果$ord(\lambda)=r$，$ord_{rn}(q)=t$，那么$\exists\delta\in F_{q^t}$ s.t. $\delta^n=\lambda$。根据$x^n-\lambda$的根组成集合$\left\{\delta^{1+rj}\mid 0\le j\le n-1\right\}$，定义集合

$$\Omega=\left\{1+rj\mid 0\le j\le n-1\right\}, \tag{1.7}$$

如果对于$\forall s\in\Omega$，定义

$$C_S=\left\{s,sq,sq^2,\cdots\right\}(\mathrm{mod}\,nr), \tag{1.8}$$

那么所有的集合C_s组成Ω的一个分割。取Ω^*为所有分割的代表元素组成的集合，则C的生成多项式$g(x)$可以表示为

$$g(x)=\prod_{s\in A}\prod_{i\in C_s}(x-\delta^i), \tag{1.9}$$

其中，$A\subset\Omega^*$。

如果$(n,p)\neq 1$，那么C为重根循环码。设F_q^n上的重根λ-循环码C，其中$\lambda\in F_q$，$n=lp^s(s\ge 1)$，$l\ge 1$且$(p,l)=1$，$\exists g(x)$ s.t. $C=\langle g(x)\rangle$。设$g(x)$在F_q的完全因式分解为

$$g(x)=\prod_{i=1}^{k}m_i(x)^{e_i}, \tag{1.10}$$

其中，$(m_i(x),m_j(x))=1(i\neq j)$且$e_i\le p^s(i=1,2,\cdots,k)$。定义

$$D_t=\langle g_t(x)\rangle, \tag{1.11}$$

其中，$g_t(x)=\prod_{e_i>t}m_i(x)$，那么$\exists\lambda_0\in F_q$ s.t. $\lambda_0^{p^s}=\lambda$，从而D_t是F_q^n上的单根λ_0-循环码。规定

$$d_H\left(D_t\right)=\begin{cases}\infty, & g_t\left(x\right)=x^l-\lambda_0\\ 1, & g_t(x)=1\end{cases}, \tag{1.12}$$

那么我们可以利用如下定理确定重根循环码的 Hamming 距离。

定理 2 [2]：设 $n=lp^s\ (s\geq 1)$ 且 $(l,p)=1$，q 是素数 p 幂次，C 是 F_q^n 上的重根循环码，那么有

$$d_H\left(C\right)=\min\left\{P_t\cdot d_H\left(D_t\right)\mid 0\leq t\leq p^s-1\right\} \tag{1.13}$$

其中 $P_t=\prod_{i=0}^{m-1}\left(t_i+1\right)$，$\left[t_{m-1},\cdots,t_1,t_0\right]$ 是 t 的 p 进制表示。

如果 C 满足一定的条件我们可以得到关于 C 的 Hamming 距离和符号对距离的相关性质，具体如下：

定理 3 [5]：设 C 是 F_q 上的 $\left(n,k,d_H\right)\left(2\leq d_H<n\right)$ 常循环码。如果 C 中存在一个长度为 d_H+s 的码字，且该码字是连续的，那么有 $n-d_H\leq k+s-1$。

定理 4 [5]：设 C 是 F_q^n 上的 $\left(n,k,d_H\right)$ 常循环码且 $2\leq d_H\leq n$。那么 $d_P\left(C\right)\geq d_H+2$ 当且仅当 C 不是 MDS 码。

3. F_p 上长为 $2p$ 的 MDS 符号对码

定理 5：设 p 是素数且 $p\geq 5$，那么存在 $\left(2p,7\right)_p$ MDS 符号对码。

证明：设 $C=\left\langle g\left(x\right)\right\rangle$，$g\left(x\right)=\left(x-1\right)^3\left(x+1\right)^2\in F_5\left[x\right]$，那么 C 形成 $GR=\dfrac{F_p\left[x\right]}{\left\langle x^{2p}-1\right\rangle}$ 的理想。由定理 2 可得：$d_H=4$，此时 C 不是 MDS 码，因此 $d_P\left(C\right)\geq d_H+2$，下面分析 $d_P\left(C\right)=d_H+2$ 是否成立。如果 $d_P=d_H+2$，意味着 $\exists c\in C$ s.t. $d_P\left(c\right)=d_H+2$，具体而言存在两种情况：

Case1: $wt_H\left(c\right)=5$，$gap\left(c\right)=1$

由于 $lp-d_H>k$，由定理 3 可知不存在这样的码字 c；

Case2: $wt_H\left(c\right)=4$，$gap\left(c\right)=2$

(i) $c\left(x\right)=c_0+c_1x+c_ix^i+c_{i+1}x^{i+1},\left(3\leq i\leq 2p-2\right)$，其中 $c_0,c_1,c_i,c_{i+1}\in F_q^*$，由于 $g\left(x\right)\mid c\left(x\right)$，那么

$$\begin{cases}c_0+c_1+c_i+c_{i+1}=0\\ c_1+ic_i+\left(i+1\right)c_{i+1}=0\\ i\left(i-1\right)c_i+\left(i+1\right)ic_{i+1}=0\\ c_0-c_1+\left(-1\right)^i c_i+\left(-1\right)^{i+1}c_{i+1}=0\\ c_1+i\left(-1\right)^{i-1}c_i+\left(i+1\right)\left(-1\right)^i c_{i+1}=0\end{cases} \tag{2.1}$$

由方程组(2.1)中第二、五个方程可得：

$$i\left[1-\left(-1\right)^{i-1}\right]c_i+\left(i+1\right)\left[1-\left(-1\right)^i\right]c_{i+1}=0, \tag{2.2}$$

当 i 是奇数时，由(2.2)可得：

$$\left(i+1\right)c_{i+1}=0, \tag{2.3}$$

若 $i+1\neq 0$，那么 $c_{i+1}=0$，推出矛盾；

若 $i+1=0$，由(2.1)中第三个方程可得：$2c_i=0$，即 $c_i=0$，推出矛盾；

当 i 是偶数时，由(2.2)可得：$ic_i=0$，由于 $3\leq i\leq 2p-1$，则 $i\neq 0$，从而 $c_i=0$，推出矛盾。

(ii) $c\left(x\right)=c_0+c_1x+c_2x^2+c_ix^i,\left(4\leq i\leq 2p-1\right)$，其中 $c_0,c_1,c_2,c_i\in F_q$，由于 $g\left(x\right)\mid c\left(x\right)$，那么

$$\begin{cases} c_0+c_1+c_2+c_i=0 \\ c_1+2c_2+ic_i=0 \\ 2c_2+i\left(i-1\right)c_i=0 \\ c_0-c_1+c_2+\left(-1\right)^i c_i=0 \\ c_1-2c_2+i\left(-1\right)^{i-1} c_i=0 \end{cases} \tag{2.4}$$

如果 $i\left(i-1\right)=0$，由(2.4)中第三个方程可得：$c_2=0$，推出矛盾，下面分析 $i\left(i-1\right)\neq 0$ 的情况。

由方程组(2.4)中第一、四个方程可得：

$$2c_1+\left[1-\left(-1\right)^i\right]c_i=0, \tag{2.5}$$

当 i 是偶数时，由(2.5)可得：$c_1=0$，推出矛盾；

当 i 是奇数时，由(2.5)可得：

$$c_1+c_i=0, \tag{2.6}$$

联立(2.4)中第二个方程和(2.6)可得：

$$2c_2+\left(i-1\right)c_i=0, \tag{2.7}$$

由(2.4)第三个方程和(2.7)可得：$\left(i-1\right)^2 c_i=0$，即 $c_i=0$ 推出矛盾；

从而 $d_P\geq d_H+3=7$，又 C 满足 Singleton-type 界，因此 $d_P=7$，从而 C 是 $\left(2p,7\right)_p$ MDS 符号对码，证毕。

下述实例根据定理 5 条件给出实例，并且通过 C 中码字的 Hamming 距离不同情况来确定 C 的符号对距离，为简化分析，我们把可以由同一个码字循环移位得到的所有码字简记为一个码字。

例 1：设 $C=\left\langle g\left(x\right)\right\rangle$，$g\left(x\right)=\left(x-1\right)^3\left(x+1\right)^2\in F_5\left[x\right]$，由 MAGMA 运行结果可知：$C$ 是 $\left(10,5,4\right)$ 纠错码。记

$$C_i=\left\{c\in C:wt_H=i\right\}, \tag{2.8}$$

$4\leq i\leq 10$，C 中码字按照 Hamming 距离分类处理如下：

1) $\left|C_4\right|=40$，C_4 中的码字具有 4 中的形式：$\left(0102030400\right)$、$\left(0204010300\right)$、$\left(0301040200\right)$、$\left(0403020100\right)$，可知 $\forall c\in C_4$，$gap\left(c\right)=4$，从而 $d_P\left(c\right)=8$；

2) $\left|C_5\right|=8$，C_5 中的码字具有 4 中的形式：$\left(0101010101\right)$、$\left(0202020202\right)$、$\left(0303030303\right)$、$\left(0404040404\right)$，可知 $\forall c\in C_5$，$gap\left(c\right)=5$，从而 $d_P\left(c\right)=10$；

3) $\left|C_6\right|=400$，$\exists c'=\left(2,3,1,4,2,3,0,0,0,0\right)\in C_6$ s.t. $gap\left(c'\right)=1$，那么 $d_P\left(c'\right)=7$，从而 $\forall c\in C_6$，$d_P\left(c\right)\geq 7$，此处的“=”能够成立；

4) 如果 $wt_H\left(c\right)\geq 7$，那么 $d_P\left(c\right)\geq wt_H\left(c\right)+gap\left(c\right)\geq 7$；

综上可得：$d_P\left(C\right)=7$，此时 C 是 $\left(10,7\right)_5$ MDS 符号对码。

例 2：设 $C=\left\langle g\left(x\right)\right\rangle$，其中 $g\left(x\right)=\left(x-1\right)^3\left(x+1\right)^2\in F_7\left[x\right]$，分析 MAGMA 结果可得：$C$ 是 $\left(14,9,4\right)$ 纠错码，按照 Hamming 距离大小对 C 中码字分类如下，记

$$C_i=\left\{c\in C:wt_H=i\right\}, \tag{2.9}$$

$4\leq i\leq 10$，C 中码字按照 Hamming 距离分类处理如下：

1) $\left|C_4\right|=420$，对 $\forall c\in C_4$，$gap\left(c\right)=4$，此时 $d_P\left(c\right)=8$；

2) $\left|C_5\right|=756$，对 $\forall c\in C_5$，$gap\left(c\right)=5$，此时 $d_P\left(c\right)=10$；

3) $\exists c'' = (1,6,5,2,1,6,0,0,0,0,0,0,0,0) \in C_6$，s.t. $gap(c'') = 1$，那么 $d_P(c'') = 7$，从而 $\forall c \in C_6$，$d_P(c) \geq 7$，此处的“=”能够成立；

4) 如果 $wt_H(c) \geq 7$，那么 $d_P(c) \geq wt_H(c) + gap(c) \geq 7$；

综上可得：$d_P(C) = 7$，此时是 $(14,7)_7$ MDS 符号对码。

4. 结论

本文利用给出了重根循环码的性质结合符号对码的符号对距离特征构造了符号对距离为7 MDS符号对码，构造出参数不同于已知构造且符号对距离较大的新的 MDS 符号对码，扩充了 MDS 符号对码类型。

参考文献

[1] Cassuto, Y. and Blaum, M. (2010) Codes for Symbol-Pair Read Channels. *Proceedings of IEEE International Symposium on Information Theory*, Austin, TX, USA, June 2010, 988-992. https://doi.org/10.1109/ISIT.2010.5513753

[2] Cassuto, Y. and Blaum, M. (2011) Codes for Symbol-Pair Read Channels. *IEEE Transactions on Information Theory*, **57**, 8011-8020. https://doi.org/10.1109/TIT.2011.2164891

[3] Chee, Y.M., Ji, L., Kiah, H.M., *et al.* (2013) Maximum Distance Separable Codes for Symbol-Pair Read Channels. *IEEE Transactions on Information Theory*, **59**, 7259-7267. https://doi.org/10.1109/TIT.2013.2276615

[4] Kai, X., Zhu, S. and Li, P. (2015) A Construction of New MDS Symbol-Pair Codes. *IEEE Transactions on Information Theory*, **61**, 5828-5834. https://doi.org/10.1109/TIT.2015.2481889

[5] Chen, B., Lin, L. and Liu, H. (2016) Constacyclic Symbol-Pair Codes: Lower Bounds and Optimal Constructions. *IEEE Transactions on Information Theory*, **63**, 7661-7666. https://doi.org/10.1109/TIT.2017.2753250

[6] Kai, X., Zhu, S., Zhao, Y., Luo, H. and Chen, Z. (2018) New MDS Symbol-Pair Codes from Repeated-Root Codes. *IEEE Communications Letters*, **22**, 462-465. https://doi.org/10.1109/LCOMM.2018.2791422

[7] Cassuto, Y. and Blaum, M. (2011) Codes for Symbol-Pair Read Channels. *IEEE Transactions on Information Theory*, **57**, 8011-8020. https://doi.org/10.1109/TIT.2011.2164891