doi:10.11959/j.issn.1000-436x.2017030

最小距离为 4 的最优五元循环码

田叶[1]，张玉清[1,2]，胡予濮[1]

（1. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 中国科学院大学国家计算机网络入侵防范中心，北京 101408）

摘 要：循环码是线性分组码中最重要的一个子类，由于其具有代数结构清晰、编译码简单且易于实现，被广泛地应用于通信系统和储存设备中。目前，大部分已有的研究工作最多只能实现三元最优循环码，对五元循环码的研究工作较少。对一类五元最优循环码 $C_{(1,e,t)}$ 进行研究。首先，给出一种有效且快速判断五元循环码 $C_{(1,e,t)}$ 是否最优的方法；其次，基于提出的方法得到当 $e=5^k+1$ 及 $e=5^m-2$ 时，循环码 $C_{(1,e,t)}$ 为最优循环码；最后，基于有限域 F_{5^m} 中的完全非线性函数，构造一类具有参数 $\left[5^m-1,5^m-2m-2,4\right]$ 的五元最优循环码。

关键词：有限域；循环码；最小距离；完全非线性函数
中图分类号：TN918 **文献标识码**：A

Optimal quinary cyclic codes with minimum distance four

TIAN Ye[1], ZHANG Yu-qing[1,2], HU Yu-pu[1]

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China)

Abstract: Cyclic codes are an extremely important subclass of linear codes. They are widely used in the communication systems and data storage systems because they have efficient encoding and decoding algorithm. Until now, how to construct the optimal ternary cyclic codes has received a lot of attention and much progress has been made. However, there is less research about the optimal quinary cyclic codes. Firstly, an efficient method to determine if cyclic codes $C_{(1,e,t)}$ were optimal codes was obtained. Secondly, based on the proposed method, when the equation $e=5^k+1$ or $e=5^m-2$ hold, the theorem that the cyclic codes $C_{(1,e,t)}$ were optimal quinary cyclic codes was proved. In addition, perfect nonlinear monomials were used to construct optimal quinary cyclic codes with parameters $[5^m-1,5^m-2m-2,4]$ optimal quinary cyclic codes over F_{5^m}.

Key words: finite field, cyclic codes, minimum distance, perfect nonlinear function

1 引言

循环码是一类重要的线性码，因其具有有效的编码和解码算法，在通信系统、数据存储系统及消费类电子产品等有着广泛的应用[1~4]。因此，关于循环码的研究一直是编码研究者所关心的热点问题。近期已有较多关于循环码的研究。

文献[5,6]通过序列设计的方法对循环码的性质进行研究。Carlet 等[7]首次利用完全非线性函数构造了具有参数 $[3^m-1,3^m-2m-1,4]$ 的三元循环码。然后，利用完全非线性函数与几乎非线性函数构造最优循环码受到了广泛的研究[7~22]。Ding 与 Helleseth[8]利用有限域 F_{3^m} 上的几乎完全非线性函数及其他多项式函数构造了几类最佳三元循环码，

收稿日期：2016-10-15；**修回日期**：2016-12-18
基金项目：国家自然科学基金资助项目（No.61572460, No.61272481）；国家重点研究计划基金资助项目（No.2016YFB0800703）；国家发展改革委员会信息安全专项基金资助项目（No.(2012)1424）；高等学校学科创新引智计划（“111”计划）基金资助项目（No.B16037）
Foundation Items: The National Natural Science Foundation of China (No.61572460, No.61272481), The National Key Research and Development Project (No.2016YFB0800703), The National Information Security Special Projects of National Development, the Reform Commission of China (No.(2012)1424), China 111 Project (No.B16037)

并提出了关于三元循环码的 9 个公开问题。文献[9,10]利用低次多项式的分解解决了其中 2 个公开的问题。

设 α 为 F_{p^n} 中的一个本原元，当 p 是素数时，记 $m_\alpha(x)$ 为素域 F_{p^n} 上的极小多项式，考察生成多项式为 $m_\alpha(x)m_{\alpha^{i_1}}(x)\cdots m_{\alpha^{i_s}}(x)$ 循环码的性质是一个热门的研究课题，其中，$1<i_1,i_2,\cdots,i_s<p^n-1$。研究较多的一类循环码是生成多项式为 $m_\alpha(x)m_{\alpha^e}(x)$ 的循环码，记此类循环码为 $C_{(1,e)}$，其中，$1<e<p^n-1$。Li 等[10]构造出具有参数 $[3^m-1,3^m-2m-1,4]$ 的循环码 $C_{(1,e)}$ 和具有参数为 $[3^m-1,3^m-2m-2,4]$ 的三元最优循环码 $C_{(1,e,t)}$，其中，$t=\dfrac{5^m-1}{2}$，$m>1$。文献[11]分析了由几乎完全非线性函数构造的循环码的重量分布。而对于 $p>3$ 的情形，循环码 $C_{(1,e)}$ 的研究不受学者关注，因为 $C_{(1,e)}$ 的最小距离至多为 3，即其不是最优码。$p>3$ 时生成多项式为 $m_{\alpha^{i_1}}(x)\cdots m_{\alpha^{i_s}}(x)$ 的最优循环码的构造是目前较热门的难点问题。Xu 等[12]对五元循环码 $C_{(0,1,e)}$ 进行了研究，其中，$C_{(0,1,e)}$ 表示生成多项式为 $(x-1)m_\alpha(x)m_{\alpha^e}(x)$ 的循环码，并证明在 $p\geqslant 5$ 条件下，当 $e=p^k+1$ 及 $e=p^m-2$ 时，循环码 $C_{(0,1,e)}$ 具有参数 $\left[p^m-1,p^m-2m-2,4\right]$，为最优循环码。

受文献[10,12]中工作的启发，本文将研究生成多项式为 $(x-1)m_\alpha(x)m_{\alpha^e}(x)$ 的五元循环码 $C_{(1,e,t)}$。首先对五元循环码 $C_{(1,e,t)}$ 的最小距离进行分析，得到了一种快速判断循环码 $C_{(1,e,t)}$ 是否为最优的方法，并分析了 2 类由单项式函数构造的循环码 $C_{(1,e,t)}$ 的参数情况（$e=5^k+1$ 及 $e=5^m-2$），然后通过利用有限域 F_{5^m} 上的完全非线性函数，构造出一类具有参数 $[5^m-1,5^m-2m-2,4]$ 的五元最优循环码。

2　相关知识

本节介绍将要用到的循环码相关的一些基础知识。

设 F_q 为含有 q 个元素的有限域，其中，$q=p^m$，p 为素数，m 为正整数。本文用 C 表示参数为 $[n,k,d]$ 的线性码，其中，码 C 的长度为 n，维数为 k，最小距离为 d。

若对 C 中的任意码字进行循环移位后仍然是 C 的码字，则 C 称为循环码。每一个循环码可对应一个多项式环，任取一个码字 $(c_1,c_2,\cdots,c_{n-1})\in C$，定义 $c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in\dfrac{F_p[x]}{x^n-1}$，从而 F_p 上任意长度为 n 的循环码 C 对应一个多项式剩余类环 $\dfrac{F_p[x]}{x^n-1}$。若一个循环码的所有码字多项式都是一个次数最低的非零首一多项式 $g(x)$ 的倍式，则称 $g(x)$ 为循环码的生成多项式，其校验多项式定义为 $h(x)=\dfrac{x^n-1}{g(x)}$。首先给出下文用到的一些基本定理及推论。

定理 1[1]　汉明界。任何 F_{p^m} 上 $[n,k]$ 线性分组码满足汉明不等式

$$p^{n-k}\geqslant 1+(p-1)\binom{n}{1}+(p-1)^2\binom{n}{2}+\cdots+(p-1)^t\binom{n}{t}$$

其中，$t=\left\lfloor\dfrac{d-1}{2}\right\rfloor$。

给定素数 p 且 $0\leqslant j\leqslant p^m-2$，则包含 j 在内的模 p^m-1 的 p-次分圆陪集定义为

$$C_j=\{jp^s \bmod (p^m-1): s=0,1,\cdots,m-1\}$$

分圆陪集 C_j 的大小记为 l_j，l_j 是 C_j 中使 $jp^s\equiv j(\mathrm{mod}(p^m-1))$ 成立的 s 的最小值。

推论 1[12]　设 p 为素数且 $n=p^m-1$，对于任一正整数 e 且 $1\leqslant e\leqslant n-1$，并满足 $\gcd(e,n)=r$。如果 $1\leqslant r\leqslant p-1$，则模 p^m-1 的 p-次分圆陪集 C_j 的大小为 m，即 $l_e=m$。

推论 2[12]　设 $p=5$，记 C_e 为包含 e 的模 p^m-1 的分圆陪集，如果 e 为偶数或满足 $e\equiv 3(\mathrm{mod}\,4)$ 时，$e\notin C_1$。

本文分析在 $p=5$ 时，有限域 F_{5^m} 上的循环码。

设 α 为有限域 F_{5^m} 中的一个本原元，$m_{\alpha^i}(x)$ 表示元素 α^i 在 F_{5^m} 上的极小多项式。令 $t=\dfrac{5^m-1}{2}$，那么 $\alpha^t=-1$，-1 的极小多项式为 $x+1$。生成多项式为 $(x+1)m_\alpha(x)m_{\alpha^e}(x)$ 的五元码可以简记为 $C_{(1,e,t)}$。

显然地，若 x 是有限域 F_{5^m} 中的非零平方元，则 $x^{\frac{5^m-1}{2}}=1$；若 x 是有限域 F_{5^m} 中的非平方元，则

$x^{\frac{5^m-1}{2}}=-1$。

推论 3 设 $p=5$，$m>1$，对于任意 $e\notin C_1$ 且 $|C_e|=m$，则有限域 F_{5^m} 上循环码 $C_{(1,e,t)}$ 的最小距离 d 满足 $d\leqslant 4$。

证明 由条件 $e\notin C_1$ 且 $|C_e|=m$ 可知循环码 $C_{(1,e,t)}$ 的长度为 5^m-1 且维数为 5^m-2m-2。利用定理 1，可知循环码 $C_{(1,e,t)}$ 的最小距离 d 满足 $d\leqslant 4$。

当循环码 $C_{(1,e,t)}$ 的最小距离 $d=4$ 时，具有参数 $[5^m-1,5^m-2m-2,4]$ 的循环码 $C_{(1,e,t)}$ 为最优循环码。

3 五元最优循环码的构造

本节首先给出一种有效且快速判断五元循环码 $C_{(1,e,t)}$ 是否最优的方法，并基于提出的方法判断当 $e=5^k+1$ 及 $e=5^m-2$ 时，循环码 $C_{(1,e,t)}$ 是否最优，最后利用完全非线性函数构造出一类具有参数 $[5^m-1,5^m-2m-2,4]$ 的最优五元循环码。

定理 2 设 $m>1$，正整数 $e\notin C_1$，且 e 所在的分圆陪集的大小 $l_e=m$，$t=\dfrac{5^m-1}{2}$，如果下列条件成立，则五元循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。

1) 当 $e\equiv 3(\bmod 4)$ 时，式(1)和式(2)在有限域 F_{5^m} 中均不存在除了 $x=\pm 1$ 以外的非零解。

$$\begin{cases}x^t=1\\ x^e+(x+1)^e+1=0\end{cases}\tag{1}$$

$$\begin{cases}x^t=-1\\ x^e+(x-1)^e-1=0\end{cases}\tag{2}$$

2) 当 e 为偶数时，式(3)~式(6)在有限域 F_{5^m} 中均不存在除了 $x=\pm 1$ 以外的非零解。

$$\begin{cases}x^t=1\\ x^e+2(x+1)^e+1=0\end{cases}\tag{3}$$

$$\begin{cases}x^t=1\\ x^e-2(x+1)^e+1=0\end{cases}\tag{4}$$

$$\begin{cases}x^t=-1\\ x^e+2(x-1)^e-1=0\end{cases}\tag{5}$$

$$\begin{cases}x^t=-1\\ x^e-2(x-1)^e-1=0\end{cases}\tag{6}$$

证明 首先由推论 2 可知，当 e 为偶数或者满足 $e\equiv 3(\bmod 4)$ 时，$e\notin C_1$。当 $e\equiv 1(\bmod 4)$ 时，$5^i e\equiv 1(\bmod 5)$，其中，$1\leqslant i\leqslant n$，即当 $e\equiv 1(\bmod 4)$ 时，$e\in C_1$。所以本文只考虑满足条件 e 为偶数或满足 $e\equiv 3(\bmod 4)$ 的正整数 e。当 $e\notin C_1$ 且 e 所在的分圆陪集的大小 $l_e=m$ 时，循环码 $C_{(1,e,t)}$ 的维数为 5^m-2m-2。下面证明循环码 $C_{(1,e,t)}$ 的最小距离为 4。

对于给定的正整数 e，为了证明循环码 $C_{(1,e,t)}$ 的最小距离为 4，需要证明循环码 $C_{(1,e,t)}$ 不含有汉明重量为 ω 的码字，其中，$\omega\in\{1,2,3\}$。根据循环码 $C_{(1,e,t)}$ 的定义，$C_{(1,e,t)}$ 含有汉明重量为 ω 的码字，当且仅当分别存在 ω 个非零元素 $c_1,c_2,\cdots,c_\omega\in F_5$ 和 ω 个两两不同的元素 $x_1,x_2,\cdots,x_\omega\in F_{5^m}$ 使下面的等式成立。

$$\begin{cases}c_1x_1+c_2x_2+\cdots+c_\omega x_\omega=0\\ c_1x_1^e+c_2x_2^e+\cdots+c_\omega x_\omega^e=0\\ c_1x_1^t+c_2x_2^t+\cdots+c_\omega x_\omega^t=0\end{cases}\tag{7}$$

显然，当 $\omega=1$ 时，式(7)不成立。当 $\omega=2$ 时，可以得到式(8)。

$$\begin{cases}c_1x_1+c_2x_2=0\\ c_1x_1^e+c_2x_2^e=0\\ c_1x_1^t+c_2x_2^t=0\end{cases}\tag{8}$$

分析式(8)的第 3 个等式，由 t 的定义 $t=\dfrac{p^m-1}{2}$ 可知 x^t，$y^t\in\{1,-1\}$，因此 c_1，$c_2\in\{1,-1\}$。当 $c_1=c_2$ 时，由式(8)的第 1 个等式可以得到 $x_1=-x_2$，因为 $t=\dfrac{p^m-1}{2}$ 为偶数，所以 $x_1^t=(-x_2)^t=x_2^t$，但由式(8)的第 3 个等式可以得到 $x_1^t=-x_2^t$，因此是矛盾的，即当 $c_1=c_2$ 时，式(8)无解。当 $c_1=-c_2$ 时，由式(8)的第 1 个等式可以得到 $x_1=x_2$，这与条件 $x_1\neq x_2$ 是矛盾的。综上分析可得，循环码 $C_{(1,e,t)}$ 不含有重量为 2 的码字。下面研究循环码 $C_{(1,e,t)}$ 是否含有汉明重量为 $\omega=3$ 的码字。

当 $\omega=3$ 时，通过化简式(7)，得

$$\begin{cases}1+\dfrac{c_2x_2}{c_1x_1}+\dfrac{c_3x_3}{c_1x_1}=0\\ 1+\dfrac{c_2x_2^e}{c_1x_1^e}+\dfrac{c_3x_3^e}{c_1x_1^e}=0\\ 1+\dfrac{c_2x_2^t}{c_1x_1^t}+\dfrac{c_3x_3^t}{c_1x_1^t}=0\end{cases}\tag{9}$$

令 $x=\frac{x_2}{x_1}$，$y=\frac{x_3}{x_1}$，式(9)可以等价为式(10)，并且 $x\neq 1$，$y\neq 1$。

$$\begin{cases}1+\frac{c_2}{c_1}x+\frac{c_3}{c_1}y=0\\ 1+\frac{c_2}{c_1}x^e+\frac{c_3}{c_1}y^e=0\\ 1+\frac{c_2}{c_1}x^t+\frac{c_3}{c_1}y^t=0\end{cases}\tag{10}$$

首先考虑式(10)中的第 3 个等式 $1+\frac{c_2}{c_1}x^t+\frac{c_3}{c_1}y^t=0$。由 c_1、c_2、c_3 的对称性，对下面几种情况进行分析。

1) 当 $c_1=c_2=1$ 时，式(10)中的第 3 个等式为 $1+x^t+c_3y^t=0$。由 $t=\frac{p^m-1}{2}$ 可知 $x^t,y^t\in\{1,-1\}$，因此当 $c_3=\pm 1$ 时，等式无解。当 $c_3=2$ 时，$1+x^t+2y^t=0$，则 $x^t=1$，$y^t=-1$。因此式(10)可以化简为

$$\begin{cases}1+x+2y=0\\ 1+x^e+2y^e=0\end{cases}\tag{11}$$

由式(11)的第 1 个等式得到 $y=2x+2$，把 $y=2x+2$ 代入到式(11)第 2 个等式中得到 $1+x^e+2(2x+2)^e=1+x^e+2^{e+1}(x+1)^e=0$。显然地，当 $e\equiv 0(\mathrm{mod}\,4)$ 时，$2^{e+1}\equiv 2(\mathrm{mod}\,5)$，因此，式(11)第 2 个等式等价于 $1+x^e+2(x+1)^e=0$。当 $e\equiv 2(\mathrm{mod}\,4)$ 时，$2^{e+1}\equiv 3(\mathrm{mod}\,5)$，式(11)第 2 个等式等价于 $1+x^e+3(x+1)^e=0$。当 $e\equiv 3(\mathrm{mod}\,4)$ 时，$2^{e+1}\equiv 1(\mathrm{mod}\,5)$，式(11)第 2 个等式等价于 $1+x^e+(x+1)^e=0$。

当 $c_3=-2$ 时，$1+x^t-2y^t=0$，则 $x^t=1$，$y^t=1$。于是式(10)可以化简为

$$\begin{cases}1+x-2y=0\\ 1+x^e-2y^e=0\end{cases}\tag{12}$$

由第 1 个等式得到 $y=-2x-2$，把 $y=-2x-2$ 代入到式(12)第 2 个等式中得到 $1+x^e-2(-2x-2)^e=1+x^e-2(-2)^e(x+1)^e=0$。当 $e\equiv 0(\mathrm{mod}\,4)$ 时，$2\times(-2)^e\equiv 2(\mathrm{mod}\,5)$，因此式(12)第 2 个等式等价于 $1+x^e-2(x+1)^e=0$。当 $e\equiv 2(\mathrm{mod}\,4)$ 时，$2(-2)^e\equiv 3(\mathrm{mod}\,5)$，因此式(12)第 2 个等式等价于 $1+x^e-3(x+1)^e=0$。当 $e\equiv 3(\mathrm{mod}\,4)$ 时，$2(-2)^e\equiv -1(\mathrm{mod}\,5)$，因此式(12)第 2 个等式等价于 $1+x^e+(x+1)^e=0$。

2) 当 $c_1=1$、$c_2=-1$ 时，与上面的情况分析类似，式(10)中的第 3 个等式转化为 $1-x^t+c_3y^t=0$。当 $c_3=\pm 1$ 时，等式无解。当 $c_3=2$ 时，$1-x^t+2y^t=0$，则 $x^t=-1$、$y^t=-1$。于是式(10)可以化简为

$$\begin{cases}1-x+2y=0\\ 1-x^e+2y^e=0\end{cases}\tag{13}$$

由式(13)的第 1 个等式得到 $y=-2x+2$，把 $y=-2x+2$ 代入到式(13)第 2 个等式中得到 $1-x^e+2(-2x+2)^e=1-x^e+2(-2)^e(x-1)^e=0$。当 $e\equiv 0(\mathrm{mod}\,4)$ 时，$2(-2)^e\equiv 2(\mathrm{mod}\,5)$，因此式(13)第 2 个等式等价于 $1-x^e-2(x-1)^e=0$。当 $e\equiv 2(\mathrm{mod}\,4)$ 时，$2(-2)^e\equiv 3(\mathrm{mod}\,5)$，因此式(13)第 2 个等式等价于 $1-x^e-3(x-1)^e=0$。当 $e\equiv 3(\mathrm{mod}\,4)$ 时，$2(-2)^e\equiv -1(\mathrm{mod}\,5)$，因此，式(13)第 2 个等式等价于 $1-x^e-(x-1)^e=0$。

当 $c_3=-2$ 时，$1-x^t-2y^t=0$，则 $x^t=-1$，$y^t=1$。式(10)可以化简为

$$\begin{cases}1-x-2y=0\\ 1-x^e-2y^e=0\end{cases}\tag{14}$$

由式(14)第 1 个等式得到 $y=2x-2$，把 $y=2x-2$ 代入到式(14)第 2 个等式中得到 $1-x^e-2(2x-2)^e=1-x^e-2^{e+1}(x-1)^e=0$。当 $e\equiv 0(\mathrm{mod}\,4)$ 时，$2^{e+1}\equiv 2(\mathrm{mod}\,5)$，因此式(14)的第 2 个等式等价于 $1-x^e-2(x-1)^e=0$。当 $e\equiv 2(\mathrm{mod}\,4)$ 时，$2^{e+1}\equiv 3(\mathrm{mod}\,5)$，因此式(14)第 2 个等式等价于 $1-x^e-3(x-1)^e=0$。当 $e\equiv 3(\mathrm{mod}\,4)$ 时，$2^{e+1}\equiv 1(\mathrm{mod}\,5)$，因此式(14)的第 2 个等式等价于 $1-x^e-(x-1)^e=0$。

对上述描述的情况与式(10)等价的等式进行总结得到定理 2 中描述的式(1)~式(6)，当式(1)~式(6)都不存在除了 ±1 以外的非零解时，式(10)就不存在除了 ±1 以外的非零解，也就是说循环码 $C_{(1,e,t)}$ 不含有汉明重量为 3 的码字，即五元循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。证毕。

注：1)当 $e\equiv 0(\mathrm{mod}\,4)$，$m$ 为偶数时，循环码

$C_{(1,e,t)}$ 的最小距离为 3。考察式(9)，令 $c_1=1$，$c_2=1$，$c_3=-2$，通过简单计算可以得到式(9)存在解为 $x_1=z$、$x_2=2z$、$x_3=-z$，其中，z 是有限域 F_{5^m} 上的任意非零元，即五元循环码 $C_{(1,e,t)}$ 在有限域 F_{5^m} 上存在重量为 3 的码字，则其最小距离为 3，参数为 $[5^m-1,5^m-2m-2,3]$。

2) 当 $e\equiv 2(\bmod 4)$，m 为奇数时，循环码 $C_{(1,e,t)}$ 的最小距离为 3，参数为 $[5^m-1,5^m-2m-2,3]$。考察式(9)，令 $c_1=1$、$c_2=-1$、$c_3=-2$，经过计算得式(9)存在解为 $x_1=z$、$x_2=2z$、$x_3=-2z$，其中，z 是有限域 F_{5^m} 上的任意非零元，即五元循环码 $C_{(1,e,t)}$ 在有限域 F_{5^m} 上存在重量为 3 的码字，则其最小距离为 3，参数为 $[5^m-1,5^m-2m-2,3]$。

文献[12]证明了当 $e=5^k+1$ 及 $e=5^m-2$ 时，循环码 $C_{(0,1,e)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$，其中 $0\leqslant k\leqslant m-1$ 且 $k\neq\frac{m}{2}$。通过应用定理 2 进行验证，可以得到当 $e=5^k+1$ 及 $e=5^m-2$ 时，循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。具体证明如下。

定理 3 设 $e=5^m-2$，$m>1$，则循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。

证明 显然有 $e\notin C_1$ 且 $\gcd(5^m-2,5^m-1)=1$，由推论 1 可得，e 所在的分圆陪集 C_e 的大小为 m。则循环码 $C_{(1,e,t)}$ 的维数为 5^m-2m-2。下面证明 $C_{(1,e,t)}$ 的最小距离为 4。

可以计算出 $5^m-2\equiv 3(\bmod 4)$。根据定理 2，首先考虑式(15)解的情况。

$$\begin{cases}x^t=1\\ x^{5^m-2}+(x+1)^{5^m-2}+1=0\end{cases}\tag{15}$$

当任意 $x\in F_{5^m}$，$x\neq 0$ 及 $x\neq -1$ 时，则有 $x^{5^m-1}=1$ 且 $(x+1)^{5^m-1}=1$。对式(15)的第 2 个等式两边同时乘以 $x(x+1)$，并进行化简可以得到 $(x-1)^2=0$，则 $x=1$，且 $x^t=1^t=1$，那么式(15)的解只有 $x=1$，即式(15)不存在除了 $x=1$ 以外的非零解。

其次，考虑式(16)解的情况。

$$\begin{cases}x^t=-1\\ x^{5^m-2}+(x-1)^{5^m-2}-1=0\end{cases}\tag{16}$$

方法同上，对式(16)的第 2 个等式两边同时乘以 $x(x-1)$，并进行化简可以得到 $(x+1)^2=0$。则 $x=-1$。但是 $(-1)^t=(-1)^{\frac{5^m-1}{2}}=1$，这与式(16)的第一个等式 $x^t=-1$ 矛盾，即 $x=-1$ 不是式(16)的解。因此式(16)不存在非零解。

综上所述，再根据定理 2 即得，当 $e=5^m-2$ 时，循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。

下面的定理给出当 $e=5^k+1$ 时，循环码 $C_{(1,e,t)}$ 的参数情况。

定理 4 设 $e=5^k+1$，m 为偶数，$m>2$，$0\leqslant k\leqslant m-1$ 且 $k\neq\frac{m}{2}$，则循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。

证明 显然 e 为偶数且 $e\equiv 2(\bmod 4)$。当 $k\neq\frac{m}{2}$ 时，$(5^k+1,5^m-1)=2$，则 $|C_e|=m$。根据定理 2，考虑式(17)~式(20)在 F_{5^m} 上解的情况。

$$\begin{cases}x^t=1\\ x^{5^k+1}+2(x+1)^{5^k+1}+1=0\end{cases}\tag{17}$$

$$\begin{cases}x^t=1\\ x^{5^k+1}-2(x+1)^{5^k+1}+1=0\end{cases}\tag{18}$$

$$\begin{cases}x^t=-1\\ x^{5^k+1}+2(x-1)^{5^k+1}-1=0\end{cases}\tag{19}$$

$$\begin{cases}x^t=-1\\ x^{5^k+1}-2(x-1)^{5^k+1}-1=0\end{cases}\tag{20}$$

对式(17)第 2 个等式进行化简得

$$\begin{aligned}&x^{5^k+1}+2(x+1)^{5^k+1}+1\\&=x^{5^k+1}+2(x+1)(x^{5^k}+1)+1\\&=3x^{5^k+1}+2x^{5^k}+2x+3\\&=-2(x-1)^{5^k+1}\\&=0\end{aligned}\tag{21}$$

式(21)在 F_{5^m} 只有一个解为 $x=1$，那么式(17)不存在除了 $x=1$ 以外的非零解。

同理，可以计算得到式(18)~式(20)不存在除了 $x=\pm 1$ 以外的非零解。根据定理 2 可得到，循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。

下面，利用完全非线性(PN, perfect nonlinear) 函数构造一类具有参数 $[5^m-1,5^m-2m-2,4]$ 的五元循

环码 $C_{(1,e,t)}$。

设 p 为素数，函数 $f:F_{p^n}\to F_{p^n}$。令 $\psi(a,b)$ 为 F_{p^n} 上满足 $f(x+a)-f(x)=b$ 的解的个数，即 $\psi(a,b)=\left|\left\{x\in F_{p^n}\,|\,f(x+a)-f(x)=b\right\}\right|$，其中 a、$b\in F_{p^n}$。记 $\Delta_f=\max\limits_{a\neq 0,a,b\in F_{p^n}}\{\psi(a,b)\}$。若 $\Delta_f=1$，则称函数 f 为 PN 函数；若 $\Delta_f=2$，则称函数 f 为几乎完全非线性（APN，almost perfect nonlinear）函数。

定理 5　设正整数 $e\notin C_1$，且 e 所在的分圆陪集的大小 $l_e=m$，$e=\dfrac{5^m-1}{2}+r$，其中，r 为偶数，且 x^r 为 PN 函数，则五元循环码 $C_{(1,e,t)}$ 为具有参数 $[5^m-1,5^m-2m-2,4]$ 的最优循环码。

证明　当 $e\notin C_1$，且 e 所在的分圆陪集的大小 $l_e=m$ 时，循环码的维数为 5^m-2m-2。同定理 2 的证明，通过分析式(7)解的情况来判断循环码 $C_{(1,e,t)}$ 是否含有汉明重量为 ω 的码字，其中，$\omega\in\{1,2,3\}$。根据定理 2 的证明，首先可以得到循环码 $C_{(1,e,t)}$ 不含有汉明重量为 1 和 2 的码字。由于式(7)中 c_1、c_2、c_3 的对称性，同定理 2 的证明，分下面 4 种情况讨论循环码 $C_{(1,e,t)}$ 是否含有汉明重量为 3 的码字。

1) 当 $c_1=c_2=1$、$c_3=2$ 时，首先得到 $x^t=1$、$y^t=-1$。则式(11)的第 2 个等式 $1+x^e+2y^e=0$ 等价于 $1+x^r-2y^r=0$。式(11)可以转化为 $x+y=-y-1$、$x^r-y^r=y^r-1$。因为 r 为偶数，所以 $(-y)^r=y^r$。那么式(11)又可以写为 $x-(-y)=(-y)-1$，$x^r-(-y)^r=(-y)^r-1$。又因为 x^r 为 PN 函数，根据 PN 函数的定义有 $(x,-y)=(-y,1)$，即 $y=-1$。但这与 $y^t=-1$ 是矛盾的。

2) 当 $c_1=c_2=1$、$c_3=-2$，首先得到 $x^t=1$、$y^t=1$。则式(12)的第 2 个等式 $1+x^e-2y^e=0$ 等价于 $1+x^r-2y^r=0$。式(12)可以转化为 $x-y=y-1$、$x^r-y^r=y^r-1$。又因为 x^r 为 PN 函数，根据 PN 函数的定义有 $(x,y)=(y,1)$，即 $y=1$。但这与条件 $y\neq 1$ 是矛盾的。

3) 当 $c_1=1$、$c_1=-1$、$c_3=2$，首先得到 $x^t=-1$、$y^t=-1$。则式(13)的第 2 个等式 $1-x^e+2y^e=0$ 等价于 $1+x^r-2y^r=0$。式(13)可以转化为 $x-y=y-(-1)$，$x^r-y^r=y^r-(-1)^r$。又因为 x^r 为 PN 函数，根据 PN 函数的定义有 $(x,y)=(y,-1)$，即 $y=-1$。但这与 $y^t=-1$ 是矛盾的。

4) 当 $c_1=1$、$c_1=-1$、$c_3=-2$ 时，首先得到 $x^t=-1$、$y^t=1$。则式(14)的第 2 个等式 $1-x^e-2y^e=0$ 等价于 $1+x^r-2y^r=0$。式(14)可以转化为 $x-(-y)=(-y)-(-1)$、$x^r-(-y)^r=(-y)^r-(-1)^r$。又因为 x^r 为 PN 函数，根据 PN 函数的定义有 $(x,-y)=(-y,-1)$，即 $y=1$。但这与条件 $y\neq 1$ 是矛盾的。

综上分析，当 $e=\dfrac{5^m-1}{2}+r$，且 x^r 为 PN 函数时，式(7)在有限域 F_{5^m} 上无解，即循环码 $[5^m-1,5^m-2m-2]$ 不含有汉明重量为 3 的码字，因此循环码 $C_{(1,e,t)}$ 具有参数 $[5^m-1,5^m-2m-2,4]$。

通过对五元循环码的分析，可以看出选择合适的指数 e，就可以构造出最优五元循环码 $C_{(1,e,t)}$。

4　结束语

目前，如何构造具有优良性质的循环码受到了编码研究者的广泛关注，已有较多关于三元最优循环码的研究工作，关于五元最优循环码的研究成果较少。本文对五元循环码 $C_{(1,e)}$ 的一类子循环码 $C_{(1,e,t)}$ 进行研究。首先，给出一种有效且快速判断五元循环码 $C_{(1,e,t)}$ 是否最优的方法，应用此方法对 2 类由单项式函数构造的循环码的参数进行分析，得到了当 $e=5^k+1$ 及 $e=5^m-2$ 时，循环码 $C_{(1,e,t)}$ 为最优循环码；最后，基于有限域 F_{5^m} 中的完全非线性函数，构造出一类最小距离为 4 的五元最优循环码，其参数为 $[5^m-1,5^m-2m-2,4]$。对于循环码的重量分布的研究也是一个有难度且热门的课题，下一步将继续研究最优循环码的构造及其重量分布。

参考文献：

[1] MACWILLIAMS F, SLOANE N. The theory of error-correcting codes[M]. North Holland: Elsevier, 1977.

[2] ASSMUS E F, KEY J D. Designs and their codes[M]. Cambridge: Cambridge University Press, 1992.

[3] MASSEY J L. Some applications of coding theory in cryptography[C]//Fourth the Institute of Mathematics and its Applications (IMA) Conference on Cryptography and Coding. 1995: 33-47.

[4] HUFFMAN W, PLESS V. Fundamentals of error-correcting codes[M]. Cambridge: Cambridge University Press, 2003.

[5] DING C. Cyclic codes from the two-prime sequences[J]. IEEE Transactions on Information Theory, 2012, 58(6):3881-3891.

[6] DING C. Cyclic codes from cyclotomic sequences of order four[J]. Finite Fields and Their Applications, 2013, 23(96):8-34.

[7] CARLET C, DING C, YUAN J. Linear codes from highly nonlinear functions and their secret sharing schemes[J]. IEEE Transactions on Information Theory, 2005, 51(6): 2089-2102.

[8] DING C, HELLESETH T. Optimal ternary cyclic codes from monomials[J]. IEEE Transactions on Information Theory, 2013, 59(9): 5898-5904.

[9] LI N, ZHOU Z, HELLESETH T. On a conjecture about a class of optimal ternary cyclic codes[C]//Seventh International Workshop on Signal Design and its Applications in Communications. 2015: 62-65.

[10] LI N, LI C, HELLESETH T, et al. Optimal ternary cyclic codes with minimum distance four and five[J]. Finite Fields and Their Applications, 2014, 30(6): 100-120.

[11] LI C, LI N, HELLESETH T, et al. The weight distributions of several classes of cyclic codes from APN monomials[J]. IEEE Transaction on Information Theory, 2014, 60(8): 4710-4721.

[12] XU G, CAO X, XU S. Optimal *p*-ary cyclic codes with minimum distance four from monomials[J]. Cryptography and Communications, 2016, 8(4): 541-554.

[13] YUAN J, CARLET C, DING C. The weight distribution of a class of linear codes from perfect nonlinear functions[J]. IEEE Transactions on Information Theory, 2006, 52(2):712-717.

[14] ZHA Z, WANG X. Almost perfect nonlinear power functions in odd characteristic[J]. IEEE Transaction on Information Theory, 2011, 57(7): 4826-4832.

[15] FENG K, LUO J. Value distributions of exponential sums from perfect nonlinear functions and their applications[J]. IEEE Transactions on Information Theory, 2007, 53(9): 3035-3041.

[16] LI C, QU L, LING S. On the covering structures of two classes of linear codes from perfect nonlinear functions[J]. IEEE Transactions on Information Theory, 2009, 55(1): 70-82.

[17] VAN LINT J. A survey of perfect codes[J]. Journal of Mathematics, 1975, 5(2):199-224.

[18] ZHOU Z, DING C. A class of three-weight cyclic codes[J]. Finite Fields and Their Applications, 2014, 25:79-93.

[19] ZHOU Z, DING C. Seven classes of three-weight cyclic codes[J]. IEEE Transactions on Communications, 2013, 61(10):4120-4126.

[20] YU L, LIU H. The weight distribution of a family of *p*-ary cyclic codes[J]. Designs, Codes and Cryptography, 2016, 78(3):1-15.

[21] KAGEYAMA Y, MARUTA T. On the geometric constructions of optimal linear codes[J]. Designs, Codes and Cryptography, 2016,81(3): 469-480.

[22] ZHENG D, WANG X, YU L. The weight enumerators of several classes of *p*-ary cyclic codes[J]. Discrete Mathematics, 2015, 338(7): 1264-1276.

作者简介：

田叶（1987-），女，山西平遥人，西安电子科技大学博士生，主要研究方向为布尔函数、序列密码的分析与构造。

张玉清（1966-），男，陕西宝鸡人，中国科学院大学教授、博士生导师，主要研究方向为网络与信息系统安全。

胡予濮（1955-），男，河南濮阳人，西安电子科技大学教授、博士生导师，主要研究方向为序列密码与分组密码、网络安全协议的设计与分析。