环 $F_2 + uF_2 + u^2F_2$ 上的$(1+u+u^2)$—循环码*

余海峰[1]，朱士信[2]
（1. 合肥学院 数理系，合肥 230601；2. 合肥工业大学 数学学院，合肥 230009）

摘 要：通过定义一种从环 $F_2+uF_2+u^2F_2$ 到域 F_2 上新的 Gray 映射，将环 $F_2+uF_2+u^2F_2$ 上的线性$(1+u+u^2)$—循环码等距映射成域 F_2 的线性循环码；进一步又给出了在码长 $n=3(\mathrm{mod}\ 4)$ 时环 $F_2+uF_2+u^2F_2$ 上的线性$(1+u+u^2)$—循环码的 Gray 象的生成多项式，这对构造新的好码具有重要意义。

关键词：等距映射；循环码；生成多项式
中图分类号：TN911.22 **文献标志码**：A **文章编号**：1001-3695(2010)05-1845-02
doi:10.3969/j.issn.1001-3695.2010.05.067

$(1+u+u^2)$-cyclic codes over $F_2+uF_2+u^2F_2$

YU Hai-feng[1], ZHU Shi-xin[2]
(1. *Dept. of Mathematics, Hefei University, Hefei* 230601, *China*; 2. *School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: This paper defined a new Gray map between codes over $F_2+uF_2+u^2F_2$ and codes over F_2. By means of this map, it shown that the Gray image of a linear $(1+u+u^2)$-cyclic code over $F_2+uF_2+u^2F_2$ is a binary-distance-invariant linear cyclic code. Furthermore, if $n=3(\mathrm{mod}\ 4)$, obtained the generator polynomial of the Gray images of $(1+u+u^2)$-cyclic codes. It is significant to construct new good codes.

Key words: isometric map; cyclic codes; generator polynomial

众所周知，Gray 映射在联系环 z_4 上线性码与一些重要的二元非线性码之间扮演了一个非常重要的角色[1~4]，各种不同有限环上的 Gray 映射也人们加以定义和研究[5~8]。1999 年，Wolfmann 在文献[5]中讨论了 Z_4 环上一类常数循环码即负循码的结构与性质，证明了 Z_4 环上负循码的 Gray 象恰是域 F_2 上的循环码，Tapia-Recillas 等人[8]将其推广至 Z_{2k} 环上，而 Lin San 等人[6]又将其进一步推广，讨论了 Z_{pk+1} 环上$(1-P^k)$—循环码，在上述推广中，作者都是将上述常循环码与域 F_2（或域 F_p）上的准循环码联系起来，能否将其与循环码联系起来也是一个比较有意义的问题。本文在环 $R=F_2+uF_2+u^2F_2$（为方便起见，下文均将该环简记为 R）上重新定义一种新的 Gray 映射，在该映射之下，环 R 上线性$(1+u+u^2)$—循环码能等距映射成域 F_2 的线性循环码。

1 环R上的循环码与$(1+u+u^2)$—循环码

首先来定义一下环 R 上的循环码与$(1+u+u^2)$—循环码。

定义 1 设 C 为 R 上长为 n 的线性码，如果 $\forall c=(c_0,c_1,\cdots,c_{n-1})\in C$ 均有 $(\lambda c_{n-1},c_0,\cdots,c_{n-2})\in C$（此时称 $(\lambda c_{n-1},c_0,\cdots,c_{n-2})$ 为 $(c_0,\cdots,c_{n-1})$ 的一个 λ—循环移位），则称 C 为 R 上的 λ—循环码，特别地，若 $\lambda=1$，则称 C 为 R 上的循环码，若 $\lambda=1+u+u^2$，则称 C 为 R 上的$(1+u+u^2)$—循环码。

若记从 R^n 到 $R[x]$ 的一同构映射 $\omega(c)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 为 R^n 上码字 $c=(c_0,c_1,\cdots,c_{n-1})$ 的多项式表示，则类似于文献[2]，本文有如下结论：

定理 1 R^n 上子模是 R 上$(1+u+u^2)$—循环码$\Leftrightarrow\omega(C)$ 是环 $B_n=R[x]/(x^n+1+u+u^2)$（B_n 上元素均简记为 $b(x)=\sum_{i=0}^{n-1}b_ix^i$）的理想。

定理 2 若 μ 是 $A_n=R[x]/(x^n-1)$ 到 B_n 的满足 $\mu(c(x))=c((1+u+u^2)x)$ 的映射，则当 $n=3(\mathrm{mod}\ 4$ 时，μ 为一环同构。

由此可得如下推论：

推论 1 设 I 为 A_n 的子集，J 为 B_n 的子集且满足 $J=\mu(I)$，则 I 是 A_n 的理想当且仅当 J 是 B_n 的理想。

推论 2 设 D 为 R^n 的一子模，若记 $\bar{\mu}$ 为 R^n（其中 $n=3(\mathrm{mod}\ 4)$）的变换：$\bar{\mu}(c_0,c_1,\cdots,c_{n-1})=(c_0,(1+u+u^2)c_1,\cdots,(1+u+u^2)^ic_i,\cdots,(1+u+u^2)^{n-1}c_{n-1})$，则 D 是循环码当且仅当 $\bar{\mu}D$ 是$(1+u+u^2)$—循环码。

与环 z_{pk} 的结论类似，很容易得到环 R 上循环码的结构：

定理 3 若 C 是环 R 上长度为 n 的循环码，则存在惟一的两两互素的多项式 f,g,h,r，使得 $C=(fhr,ufgr,u^2fgh)$。其中 $x^n-1=fghr$ 且 $|C|=8^{\deg(g)}4^{\deg(h)}2^{\deg(r)}$。

借助于定理 2 中的环同构 μ，可得：

定理 4 若 C 是环 R 上长度为 n（其中 $n=3(\mathrm{mod}\ 4)$）的

收稿日期：2009-09-08；**修回日期**：2009-10-27 **基金项目**：国家自然科学基金资助项目(60673074)；国家教育部科学技术研究重点项目(107065)；安徽省教育厅重点资助项目(KJ2008A140)；安徽省高校青年基金资助项目(2007JQ1146)；合肥学院科研发展基金重点项目(10KY01ZD)

作者简介：余海峰(1975-)，男，安徽岳西人，副教授，主要研究方向为编码与密码(yuhfslx@hfuu.edu.cn)；朱士信(1962-)，男，安徽枞阳人，教授，博士，主要研究方向为编码与密码.

$(1+u+u^2)$循环码,则存在惟一的两两互素的多项式f_0,f_1,f_2,f_3,使得 $C=(f_0f_2f_3, uf_0f_1f_3, u^2f_0f_1f_2)$。其中,$x^n+1+u+u^2=f_0f_1f_2f_3$,且$|C|=8^{\deg(f_1)}4^{\deg(f_2)}2^{\deg(f_3)}$。

2 R上$(1+u+u^2)$—循环码的 Gray 象

为不致引起混淆,下面均将 $R,R^n,R[x]$上加法记为“+”,将 $F_2,F_2^{4n},F_2[x]$上加法记为“⊕”。

若将 R 上任一元素 a 记为 $a=r_0(a)+ur_1(a)+u^2r_2(a)$。其中 $r_i(a)\in F_2$。

则可定义如下的 Gray 映射:

定义 2 $\forall a\in R, a=r_0(a)+ur_1(a)+u^2r_2(a)$,则称 $\phi(a)=(r_2(a), r_2(a)\oplus r_1(a), r_2(a)\oplus r_0(a), r_2(a)\oplus r_1(a)\oplus r_0(a))$为 R 到 F_2 的 Gray 映射。可自然延伸至 R^n 上码字 c 的 Gray 映射以及 $R[x]$上多项式 $a(x)$的 Gray 映射:

$\forall c=(c_0,c_1,\cdots,c_{n-1})\in R^n$,记 $r_i(c)=(r_i(c_0),r_i(c_1),\cdots,r_i(c_{n-1}))$, $i=0,1,2$,则

$\phi(c)=(r_2(c), r_2(c)\oplus r_1(c), r_2(c)\oplus r_0(c), r_2(c)\oplus r_1(c)\oplus r_0(c))$为 R^n 到 F_2^{4n} 的 Gray 映射;$\forall c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in R[x]$,记 $p_i(x)=\sum_{j=0}^{n-1}r_i(c_j)x^j$, $i=0,1,2$,则 $\phi_p(c(x))=p_2(x)+x^n(p_2(x)\oplus p_1(x))+x^{2n}(p_2(x)\oplus p_0(x))+x^{3n}(p_2(x)\oplus p_1(x)\oplus p_0(x))$为 $R[x]$到 $F_2(x)$的 Gray 映射。

由上述定义,显然有:

命题 1 如果 $c(x)=\omega(c)$,则有 $\phi_p(c(x))=\omega(\phi(c))$。

若定义环 R 中元素 $1,u,1+u,1+u^2,u+u^2,1+u+u^2$ 的李重量为 $2,u^2$ 的李重量为 4,0 的李重量为 0, 对 $\forall X=(x_1,x_2,\cdots,x_n)\in R^n$,定义码字 X 的李重量为 $W_L(X)=\sum_{i=1}^{n}W_L(x_i)$。

其中:$W_L(x_i)$是指码元 x_i 的李重量,定义码字 X,Y 的李距离为 $d_L(X,Y)=W_L(X-Y)$,则由 ϕ 的定义可验证:

定理 5 Gray 映射 ϕ 是一个保线性且保距离(R^n 上的李距离到 F_2^{4n} 上的汉明距离)的同构映射。

进一步,还有:

定理 6 若 v 是 R^n 上一个$(1+u+u^2)$—循环移位,σ 是 F_2^{4n} 上的一个循环移位,ϕ 为 R^n 到 F_2^{4n} 的 Gray 映射,则 $\phi v=\sigma\phi$。

证明 设 $c=(c_0,c_1,\cdots,c_{n-1})\in R^n$。其中:$c_i=r_0(c_i)+ur_1(c_i)+u^2r_2(c_i)$, $r_i(c_i)\in F_2$, $i=0,1,\cdots,n-1$; $j=0,1,2$ 则 $\phi(v(c))=\phi((1+u+u^2)c_{n-1},c_0,c_1,\cdots,c_{n-2})=\{r_2((1+u+u^2)c_{n-1}), r_2(c_0),\cdots,r_2(c_{n-2}), r_2((1+u+u^2)c_{n-1})\oplus r_1((1+u+u^2)c_{n-1}), r_2(c_0)\oplus r_1(c_0),\cdots,r_2(c_{n-2})\oplus r_1(c_{n-2}), r_2((1+u+u^2)c_{n-1})\oplus r_0((1+u+u^2)c_{n-1}), r_2(c_0)\oplus r_0(c_0),\cdots,r_2(c_{n-2})\oplus r_0(c_{n-2}), r_2((1+u+u^2)c_{n-1})\oplus r_1((1+u+u^2)c_{n-1})\oplus r_0((1+u+u^2)c_{n-1}), r_2(c_0)\oplus r_1(c_0)\oplus r_0(c_0),\cdots,r_2(c_{n-2})\oplus r_1(c_{n-2})\oplus r_0(c_{n-2})\}=\{r_2(c_{n-1})\oplus r_1(c_{n-1})\oplus r_0(c_{n-1}), r_2(c_0),\cdots,r_2(c_{n-1}), r_2(c_0)\oplus r_1(c_0),\cdots,r_2(c_{n-1})\oplus r_1(c_{n-1}), r_2(c_0)\oplus r_0(c_0),\cdots, r_2(c_{n-1})\oplus r_0(c_{n-1}), r_2(c_0)\oplus r_1(c_0)\oplus r_0(c_0),\cdots,r_2(c_{n-2})\oplus r_1(c_{n-2})\oplus r_0(c_{n-2})\}=\sigma(\phi(c))$,即$\phi v=\sigma\phi$。

由定理 5、6 很容易得到如下定理:

定理 7 设 C 为 R 上长为 n 的线性$(1+u+u^2)$—循环码,则其 Gray 象 $\phi(C)$是 F_2 上长为 $4n$ 的线性循环码。

沿用文献[6]中定义,对于 $c=(c_0,c_1,\cdots,c_{n-1})\in R^n$,记 $r_i(c)=(r_i(c_0),r_i(c_1),\cdots,r_i(c_{n-1}))$, $i=0,1,2$ 则称 $\bar{c}=r_0(c)$为 c 的二元约化。

类似地,若 $a(x)=\sum_{i=0}^{r}a_ix^i\in R[x]$,则称 $\overline{a(x)}=\sum_{i=0}^{r}\bar{a}_ix^i\in F_2[x]$为 $a(X)$的二元约化。

显然有 $\overline{a(x)}=\overline{a((1+u+u^2)x)}$。

定理 8 若 C 是 R 环上长度为 n(其中 $n=3(\bmod 4)$)的$(1+u+u^2)$—循环码,且 $C=(f_0f_2f_3, uf_0f_1f_3, u^2f_0f_1f_2)$。其中 $x^n+1+u+u^2=f_0f_1f_2f_3, f_0, f_1f_2, f_3$ 为两两互素的多项式,则其 Gray 象 $\phi(C)$是 F_2 上长为 $4n$ 的线性循环码,且有 $\phi(C)=(\bar{f}_0^4\bar{f}_1\bar{f}_2^2\bar{f}_3^3)$

证明 由定理 7 知 $\phi(C)$是 F_2 上长为 $4n$ 的线性循环码,下证:

$$\phi(C)=(\bar{f}_0^4\bar{f}_1\bar{f}_2^2\bar{f}_3^3)$$

记 A_n,B_n 为上述定理 1、2 所设,$A_{4n}=F_2[x]/(x^{4n}-1)$。

由 $C=(f_0f_2f_3, uf_0f_1f_3, u^2f_0f_1f_2)$可知:

$\exists a(x),b(x),c(x)\in B_n$ 使得 C 中任意码字 $D(x)=a(x)f_0f_2f_3+ub(x)f_0f_1f_3+u^2c(x)f_0f_1f_2$。

显然,$D(x)$能写成 $X_0+uX_1+u^2X_2$。其中:$X_0,X_1,X_2\in F_2[X]$,且有 $X_0=\overline{a(x)f_0}\bar{f}_2\bar{f}_3$,则从 $\phi_p(D(x))$定义,有:

$$\phi_p(D(x))=X_2+x^n(X_2\oplus X_1)+x^{2n}(X_2\oplus X_0)+x^{3n}(X_2\oplus X_1\oplus X_0)=X_2(x^n+1)^3\oplus X_1x^n(x^n+1)^2\oplus X_0x^{2n}(x^n+1)=(x^n+1)[(x^n+1)(X_2(x^n+1)\oplus X_1x^n\oplus X_0(x^n+1)\oplus X_0]。$$

由 $x^n+1+u+u^2=f_0f_1f_2f_3$ 两边取二元约化可得 $x^n+1=\bar{f}_0\bar{f}_1\bar{f}_2\bar{f}_3$。因此 $\phi_p(D(x))$能写成$\bar{f}_0^2\bar{f}_1^2\bar{f}_2^2\bar{f}_3^2e(x), e(x)\in F_2[x]$。

故 $\phi_p(C)\subseteq(\bar{f}_0^2\bar{f}_1^2\bar{f}_2^2\bar{f}_3^2)$,若取$\overline{m(x)}\in\phi_p(C)$, $\exists\overline{n(x)}\in A_{4n}$,使得$\overline{m(x)}=\overline{n(x)}\bar{f}_0^2\bar{f}_1^2\bar{f}_2^2\bar{f}_3^2$,因此$\overline{m(x)}\bar{f}_1=\overline{n(x)}(x^{2n}+1)=\phi_p(u\overline{n(x)})$。

故有 $u\overline{n(x)}\in C$,因此,$\exists F(x),G(x),H(x)\in B_n$,使得 $u\overline{n(x)}=F(x)f_0f_2f_3+uG(x)f_0f_1f_3+u^2H(x)f_0f_1f_2$ 即 $\exists\overline{I(x)}\in F_2[x]$使得$\overline{n(x)}=\bar{f}_0\bar{f}_3\overline{I(x)}$,故有$\overline{m(x)}=\bar{f}_0^3\bar{f}_1\bar{f}_2^2\bar{f}_3^3$,即 $\phi_p(C)\subseteq(\bar{f}_0^3\bar{f}_1^2\bar{f}_2^2\bar{f}_3^3)$。类似地,若取$\overline{l(x)}\in\phi_p(C)$,则 $\exists\overline{q(x)}\in A_{4n}$,使得$\overline{m(x)}=\overline{q(x)}\bar{f}_0^3\bar{f}_1^2\bar{f}_2^2\bar{f}_3^3$,因此$\overline{l(x)}\bar{f}_1^2\bar{f}_2=\overline{q(x)}(x^n+1)^3=\phi_p(u^2\overline{q(x)})$,故有 $u^2\overline{q(x)}\in C$,因此$\exists L(x),M(x),N(x)\in B_n$ 使得 $u^2\overline{q(x)}=L(x)f_0f_2f_3+uM(x)f_0f_1f_3+u^2N(x)f_0f_1f_2$,即$\exists\overline{p(x)}\in F_2[x]$使得$\overline{q(x)}=\bar{f}_0\overline{p(x)}$故有$\overline{l(x)}=\bar{f}_0^4\bar{f}_1\bar{f}_2^2\bar{f}_3^3$,即 $\phi_p(C)\subseteq(\bar{f}_0^4\bar{f}_1\bar{f}_2^2\bar{f}_3^3)$。比较 $\phi_p(C)$与$(\bar{f}_0^4\bar{f}_1\bar{f}_2^2\bar{f}_3^3)$码字个数可得 $\phi_p(C)=(\bar{f}_0^4\bar{f}_1\bar{f}_2^2\bar{f}_3^3)$。

3 结束语

有限环上编码理论是近年来人们很感兴趣的一个热点问题,由此可以对域上编码有更清楚的认识。本文主要在环 R 上重新定义了一种新的 Gray 映射,通过该映射能将环 R 上线性$(1+u+u^2)$—循环码等距映射成域 F_2 的线性循环码,并且讨论了当码长 $n=3(\bmod 4)$时,可由 R 上线性$(1+u+u^2)$—循环码的生成多项式得到其 Gray 象的生成多项式,为寻找更好的码类提供了理论依据。

参考文献:

[1] HAMMONS A R, KUMAR P V, CALDERBANK A R, *et al*. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes[J]. IEEE Trans Inform Theory, 1994, 40(2):301-319.

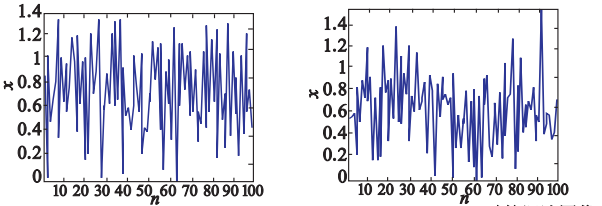
(下转第 1859 页)

n 存在以下关系:

$$d=\frac{n-1}{n}(\ln n-\ln(-\ln p_c))$$

其中: p_c 为全网连通概率。若节点的期望邻居节点数为 n' ($n'<<n$),则两个相邻节点共享一个密钥的概率 $p'=\frac{d}{n'-1}$。在给定 p'的情况下,p 与 k 之间的关系表示如下:

$$p'=1-\frac{((p-k)!)^2}{(p-2k)!\ p!}$$



(a)λ=3.6,x=0.6,n=100时的混沌图像　(b)λ=3.6,x=0.601,n=100时的混沌图像

图2　x=3.6,λ=0.6与0.601时的混沌图像

本文采用的是预配置对密钥预分配改进方案模型,网络内所有的节点都有相同的初值 x_0 和参数 λ,使得传感器网络内每个节点都能够与其任意一个邻居节点建立起共享通信密钥,同时也支持组播通信。在不考虑诸如网络因障碍物阻隔造成的通信延迟及敌方电磁干扰的情况下,本方案的网络密钥连通概率是百分之百。在本文的算法中,生成的每对对密钥都不相同,只有进行通信的双方拥有该对密钥,混沌密钥动态改变,使得可以独立建立起点到点的安全信道,且避免了网络安全对基站的依赖。综上所述,本方案与其他几种对密钥管理方案的比较如表 3 所示。

表 3　几种方案的比较

方案名称	网络扩展性	安全性	内存开销	计算复杂度	连通概率
预配置对密钥	较好	差	小	无	1
随机密钥方案	一般	一般	一般	一般	$p'=1-\frac{(p-k)!}{(p-2k)!}$
基于密钥池方案	一般	一般	较大	一般	$p'=1-\sum_{s=0}^{q-1}(P(s)$, 与密钥池 $\|s\|$ 大小有关
本方案	较好	较好	较小	一般	1

4　结束语

在无线传感器网络安全机制中,密钥管理是系统所有安全服务的基础,它包括加密系统密钥的产生、分配、存储、使用、失效及撤除等全过程。本文提出的针对全网范围内预配置对密钥的改进方案,引入混沌算法和临时初始密钥,混沌序列的不可预测性、不可分解性等非线性特征是混沌算法具有良好安全性的理论基础,利用混沌的遍历性和初值敏感性解决了原方案在密钥安全性方面的不足,动态地改变加密密钥且密钥空间大,抗破译能力强,实现了数据传输的加密和认证,保证了传输数据的安全性、真实性和完整性;在密钥管理方面实现了密钥的更新和撤除。该方案对节点资源要求具有较好的适应性,与目前的随机密钥类型算法相比,在计算量与内存需求增加不大的情况下获得了较好的网络安全性,易于在 Mica2 节点上软件实现。

参考文献:

[1] AKYILDIZ F, SU W, SANKARASUBRAMANIAM Y, *et al*. Wireless sensor network: a survey[J]. Computer Networks, 2002,38(4):393-422.

[2] ESTRIN D, GOVINDAN R, HEIDEMANN J, *et al*. Next century challenges: Scalable coordination in sensor networks[C]// Proc of ACM/IEEE Int'l Conf on Mobile Computing and Networking. New York: ACM Press, 1999: 263-270.

[3] GENI. Global environment for network innovations [EB/OL]. (2006). http://www.geni.net.

[4] 苏忠,林闯,封富君,等.无线传感器网络密钥管理的方案和协议[J].软件学报,2007,18(5):1218-1231.

[5] 陈菲.无线传感器网络安全问题研究——对密钥管理研究[D].上海:上海交通大学,2005.

[6] ESCHENAUER L, GLIOR V D. A key management scheme for distributedsensor networks[C]// Proc of the 9th ACM Conference on Computer and Communication Security. New York: ACM Press, 2002: 41-47.

[7] CHEN H W, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]// Proc of IEEE Symposium on Security and Privacy. Berkeley, California: IEEE Computer Society, 2003: 197-205.

[8] 张化光,王智良,黄玮.混沌系统的控制理论[M].沈阳:东北大学出版社,2003.

[9] 温蜜,陈克非,郑燕飞,等.传感器网络中一种可靠的对密钥更新方案[J].软件学报,2007,18(5):1232-1245.

[10] 孙利民,李建中,陈渝,等.无线传感器网络[M].北京:清华大学出版社,2005.

[11] 陈帅.无线微传感器网络混沌加密理论及其关键技术研究[D].重庆:重庆大学,2006.

[12] BOLLOBAS B, FULTON W, KATOK A, *et al*. Rand graphs[M]. 2nd ed. Cambridge: Cambridge University Press, 2001:160-200.

[13] 张楠,张建华,陈建英,等.无线传感器网络中基于混沌的密钥预分配方案[J].计算机应用,2007,27(8):1901-1903.

[14] 马虹博,刘连浩.基于混沌的魔方置乱算法设计[J].计算机工程与应用,2006,42(12):138-140.

[15] 付争方.基于标志的无线传感器网络密钥预分配方案[J].计算机工程与设计,2008,29(13):3313-3315.

(上接第 1846 页)

[2] WOLFMANN J. Negacyclic and cyclic codes over Z_4[J]. IEEE Trans Inform Theory, 1999, 45(7):2527-2532.

[3] WOLFMANN J. Binary images of cyclic codes over Z_4[J]. IEEE Trans Inform Theory, 2001, 47(5):1773-1779.

[4] WAN Zhe-xian. Quaternay code[M]. Singapore: World Scientific, 1997.

[5] CARLET C. Z_{2k}-linear codes[J]. IEEE Trans Inform Theory, 1998,44(4):1543-1547.

[6] LIN San, BLACKFORD T T. $Z_{p^{k+1}}$-linear codes [J]. IEEE Trans Inform Theory,2002, 48(9):2592-2605.

[7] BONNECAZE A, UDAYA P. Cyclic codes and self-dual codes over F_2+uF_2[J]. IEEE Trans Inform Theory,1999,45(4): 1250-1255.

[8] TAPIA-RECILLAS H, VEGA G. A generalization of negacyclic codes [C]// AUGOT D, CARLET C. Proc of International Workshop on Coding and Cryptography. 2001:519-529.

[9] UDAYA P, BONNECAZE A. Decoding of cyclic codes over F_2+uF_2 [J]. IEEE Trans Inform Theory,1999,45(4):2148-2157.

[10] DOUGHERTY S T, GABORIT P, HARAD M, *et al*. Type II codes over F_2+uF_2[J]. IEEE Trans Inform Theory,1999,45(1):32-45.

[11] PLESS V, QIAN Z. Cyclic codes and quadratic residue codes over Z_4 [J]. IEEE Trans Inform Theory,1996,42(5):1594-1600.

[12] Mac WILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. Amsterdam: North-Holland,1977.