周期为$4v$(几乎)平衡理想二进制序列构造研究

彭秀平*[①③④]　冀惠璞[①]　林洪彬[②]　刘　刚[②]
[①](燕山大学信息科学与工程学院　秦皇岛　066004)
[②](燕山大学电气工程学院　秦皇岛　066004)
[③](河北省信息传输与信号处理重点实验室　秦皇岛　066004)
[④](通信网信息传输与分发技术重点实验室　石家庄　050081)

摘　要：具有理想自相关特性的序列在无线通信、雷达以及密码学中具有重要的作用。因此为了扩展更多可应用于通信系统的理想序列，该文基于2阶分圆类和中国剩余定理，提出3类新的周期为$T=4v$(v是奇素数)平衡或几乎平衡理想二进制序列构造方法。构造所得序列的周期自相关函数满足：当$v\equiv 3 \pmod 4$时，序列的周期自相关函数旁瓣值取值集合为$\{0,-4\}$或$\{0,4,-4\}$；当$v\equiv 1 \pmod 4$时，相应的取值集合为$\{0,4,-4\}$。通过该文方法拓展了周期为$4v$平衡理想二进制序列的存在范围，从而可为工程应用提供更多性能优良的理想序列。

关键词：二进制序列；几乎差集；分圆；理想自相关性
中图分类号：TN911.2　　**文献标识码**：A　　**文章编号**：1009-5896(2022)01-0271-08
DOI: 10.11999/JEIT200829

Study on the Constructions of Balanced Optimal Binary Sequences with Period $4v$ (almost)

PENG Xiuping[①③④]　JI Huipu[①]　LIN Hongbin[②]　LIU Gang[②]
[①](*School of Information Science & Engineering, Yanshan University, Qinhuangdao* 066004, *China*)
[②](*School of Electrical Engineering, Yanshan University, Qinhuangdao* 066004, *China*)
[③](*Hebei Province Key Laboratory of Information Transmission and Signal Processing, Qinhuangdao* 066004, *China*)
[④](*Key Laboratory of Communication Network Information Transmission and Distribution Technology, Shijiazhuang* 050081, *China*)

Abstract: Sequences with optimal autocorrelation property have important roles in wireless communication, radar and cryptography. Therefore, in order to expand more ideal sequences that can be applied to communication systems, based on cyclotomy of order 2 and Chinese remainder theorem, three new constructions of balanced or almost balanced binary sequences of period $T=4v$(v is odd prime) are presented in this paper. The periodic autocorrelation function of the constructed sequence satisfies: when $v\equiv 3 \pmod 4$, the out-of-phase autocorrelation value set of the sequence is $\{0,-4\}$ or $\{0,4,-4\}$; when $v\equiv 1 \pmod 4$, the corresponding value set is $\{0,4,-4\}$. The existing range of balanced optimal binary sequences with period of $4v$ is extended by this method, so that more optimal sequences with good property can be provided for engineering applications.

Key words: Binary sequences; Almost difference set; Cyclotomy; Optimal autocorrelation property

---

收稿日期：2020-09-23；改回日期：2021-04-15；网络出版：2021-07-13
*通信作者：　彭秀平　pengxp@ysu.edu.cn
基金项目：国家重点研发计划(2017YFB0306402)，河北省自然科学基金(F2021203040, E2020203188)，河北省高等学校科学技术研究基金(BJ2018018, ZD2019039, QN2019133)，弹性网络服务自主适应管控技术研究(6142104190109)
Foundation Items: The National Key Research and Development Project (2017YFB0306402), The Natural Foundation of Hebei Province(F2021203040, E2020203188), Science and Technology Program of Universities and Colleges in Hebei Province (BJ2018018, ZD2019039, QN2019133), The Research on Self-Adaptive Control Technology of Elastic Network Service (6142104190109)

1 引言

在通信、密码、雷达和声呐等实际应用系统中，为了实现同步、抗多径干扰、防止载波泄漏和实现设备简易性等需求，具有理想自相关特性的二进制序列在这些领域中发挥着重要作用[1,2]。如在码分多址(Code Division Multiple Access, CDMA)通信系统中，需要这些序列来获取接收信号的准确定时信息，在密码学中，序列用于以流密码加密生成密钥流。通常要求所采用的序列应具有尽可能低的自相关函数旁瓣值和好的平衡性[3,4]。而目前已有的研究结果表明，最佳序列存在数目比较有限，最佳二进制序列仅存在长度为4的(1, 1, 1, –1)的情况[5,6]。为了获得更多满足实际需求的序列，学者在不断寻求其他形式理想序列。按序列周期不同，理想二进制序列分为4类[4,7]，本文将对其中周期为$T\equiv 0\,(\mathrm{mod}4)$的理想二进制序列的直接构造方法进行研究。

近20年来，周期为$T\equiv 0\ (\mathrm{mod}4)$且具有理想自相关特性的二进制序列一直都是学者研究的热点[7–16]，目前关于这类周期长度的序列的构造方法主要有3类：一是基于特征多项式法，代表性成果有基于多项式$z\,(1-z)$法[8]，基于广义多项式$(z+1)^d+az^d+b$法[9]，通过这类方法得到了周期为$T=p^m-1\equiv 0\ (\mathrm{mod}4)$ 且自相关函数值为$\{0,-4\}$的平衡或几乎平衡二进制序列；二是基于交织法，代表性成果有文献[10]利用交织法，对两个周期均为$v\equiv 3\ (\mathrm{mod}4)$的理想二进制序列做交织和移位操作，得到了周期为$T\equiv 4v$，旁瓣值为$\{0,-4\}$的几乎平衡理想二进制序列。文献[11]对周期为$v=2^{2k}-1$的二进制GMW序列和完备二进制序列做交织和移位操作，得到了周期为$T=4v$旁瓣值为$\{0,\pm 4\}$的理想二进制序列，目前此类序列大多数都是基于交织法[7,10–14]，但基于交织法得到的理想二进制序列普遍存在特性受所采用的移位序列和基序列限制的问题；三是基于中国剩余定理法，基于2阶分圆类和中国剩余定理得到参数为$(4v,2v+1,v,v-1)$的几乎差集，根据几乎差集与二进制序列之间的等价关系可得到周期为$T=4v$，其中$v\equiv 3\ (\mathrm{mod}4)$，旁瓣值为$\{0,-4\}$的几乎平衡理想二进制序列[15]；以及基于中国剩余定理将一个完备二进制序列和任意的理想二进制序列结合起来，构造得到了一类几乎平衡理想二进制序列[16]。

本文在现有成果基础上，将素数v分为$v\equiv 3\ (\mathrm{mod}4)$和$v\equiv 1\ (\mathrm{mod}4)$两种情况，基于2阶分圆类和中国剩余定理将提出3种周期均为$T=4v$的理想二进制序列w的普遍构造方法，得到的二进制序列不仅具有理想自相关特性，而且具有很好的平衡性。拓展了现有周期为$T\equiv 0\ (\mathrm{mod}4)$的理想二进制序列存在范围。

2 基本概念

定义1 设周期为T的序列$w=(w(0),w(1),\cdots w(T-1))$，其中$w(t)\in\{1,-1\}$，则称序列$w$为二进制序列，设$N_i(w)=|\{0\le t<T:w(t)=i\}|$，当满足式(1)所示条件时，称序列$w$为平衡二进制序列

$$\left.\begin{array}{l}|N_1(w)-N_{-1}(w)|=0,\ \ T\text{为偶数}\\ |N_1(w)-N_{-1}(w)|=1,\ \ T\text{为奇数}\end{array}\right\}\tag{1}$$

当满足式(2)所示条件时，称序列w为几乎平衡二进制序列

$$\left.\begin{array}{l}N_1(w)=\dfrac{T}{2}\pm 1, T\ \text{为偶数}\\ N_1(w)=\dfrac{T\pm 3}{2}, T\ \text{为奇数}\end{array}\right\}\tag{2}$$

定义2 设w是周期为T的二进制序列，其周期自相关函数为

$$R_w(\tau)=\sum_{t=0}^{T-1}w(t)\,w(t+\tau)\tag{3}$$

其中，$0\le\tau<T$，$t+\delta=(t+\delta)\bmod N$，当$1\le\tau\le T-1$时，$R_w(\tau)$称作序列$w$的自相关函数旁瓣值。

定义3 设w是周期为T的二进制序列，$W=\{w(t)=1:0\le t\le T-1\}$，则$W$称为序列$w$的特征集，反之，$w$称为$W$的特征序列。序列$w$的差函数$d_W(\tau)$定义为

$$d_W(\tau)=|W\cap(W+\tau)|\tag{4}$$

则$R_w(\tau)$可以表示为$R_w(\tau)=T-4\,(|W|-d_W(\tau))$，其中$(W+\tau)\in\{w+\tau:w\in W\}$，$|W|$表示集合$W$的长度。根据式(4)，当$0<\tau<T$时，可以得到$R_w(\tau)=T\,(\mathrm{mod}4)$。因此，具有理想自相关值的二进制序列有以下4种情况[4,7]：(1)当$T\equiv 0\ (\mathrm{mod}4)$时，$R_w(\tau)=0$；(2)当$T\equiv 1\ (\mathrm{mod}4)$时，$R_w(\tau)\in\{-3,1\}$；(3)当$T\equiv 2\ (\mathrm{mod}4)$时，$R_w(\tau)\in\{-2,2\}$；(4)当$T\equiv 3\ (\mathrm{mod}4)$时，$R_w(\tau)=-1$。其中情况(1)中的序列称为最佳二进制序列。当$T\equiv 0\ (\mathrm{mod}4)$，$R_w(\tau\ne 0)\in\{0,4\}$或$\{0,-4\}$时，称序列$w$为具有理想自相关函数值的二进制序列，当$R_w(\tau\ne 0)\in\{0,\pm 4\}$时，称序列$w$为具有理想自相关函数幅值的二进制序列[5,6]。

定义4[9] 设$T>1$，W为序列w的特征集，其中$|W|=l$，$d_W(\tau)$如式(4)所示，当且仅当τ取遍Z_T^*中所有元素后，$d_W(\tau)=\lambda$出现e次，$d_W(\tau)=\lambda+1$

出现$T-1-e$次时，集合W称为参数为(T,l,λ,e)的几乎差集。几乎差集的参数之间的关系为

$$l\left(l-1\right)=e\lambda+\left(T-1-e\right)\left(\lambda+1\right) \tag{5}$$

根据式(4)和式(5)可以得到，当特征集合W是Z_T上的参数为$(4v,2v-1,v-2,v-1)$或$(4v,2v+1,v,v-1)$的几乎差集时，序列w是周期为$4v$且自相关值为$\{0,-4\}$的几乎平衡理想序列。

分圆类是构造理想二进制或四进制序列的一种重要数学工具。关于2阶分圆类的介绍如下所示：

定义5[15]　设$v=2d+1$为一奇素数，其中d为正整数。α是Z_v上的本原元，令

$$D_j^{(2,v)}=\left\{\alpha^{j+2m}:0\le m\le d-1\right\},j=0,1 \tag{6}$$

则集合$D_0^{(2,v)}$和$D_1^{(2,v)}$都称为2阶分圆类，$D_j^{(2,v)}$可以简写为D_j。令

$$(j,w)=\left|(D_j+1)\cap D_w\right|,j,w=0,1 \tag{7}$$

其中，"$+$"代表和模v。则(j,w)称作Z_v上的2阶分圆数。

引理1[15]　设素数$v\equiv 3\ (\mathrm{mod}4)$，则
$(0,1)=\dfrac{v-1}{4}$, $(0,0)=(1,0)=(1,1)=\dfrac{v-3}{4}$,

设素数$v\equiv 1\ (\mathrm{mod}4)$，则
$(0,0)=\dfrac{v-5}{4}$, $(0,1)=(1,0)=(1,1)=\dfrac{v-1}{4}$。

根据中国剩余定理[17]，$Z_{4v}\cong Z_4\times Z_v$存在以下映射关系

$$\varphi(\tau)=(\tau_0,\tau_1) \tag{8}$$

其中，$\tau_0=\tau\ (\mathrm{mod}4)$, $\tau_1=\tau\ (\mathrm{mod}v)$。因此，构造周期为$T=4v$具有理想自相关特性的二进制序列就相当于在$Z_4\times Z_v$上进行构造。

引理2　设$D=\{i\}\times D_j\cup\{i+1,i+2,i+3\}\times D_{1-j}$，其中$D_j,D_{1-j}\subseteq Z_v$, $0\le j\le 1$, $0\le i\le 3$。设$\tau=(\tau_1,\tau_2)\in Z_4\times Z_v$，那么$D$的差函数$d_D\left(\tau_1,\tau_2\right)$为

$$d_D(\tau_1,\tau_2)=\begin{cases}2\left(v-1\right),\tau_1=0,\tau_2=0\\ v-1,\tau_1=1,2,3,\tau_2=0\\ (j,j)+3\left(1-j,1-j\right),\tau_1=0,\tau_2\in D_0\\ (j+1,j+1)+3\left(j,j\right),\tau_1=0,\tau_2\in D_1\\ (1-j,j)+(j,1-j)+2\left(1-j,1-j\right),\tau_1=1,2,3,\tau_2\in D_0\\ (j,j+1)+(1+j,j)+2\left(j,j\right),\tau_1=1,2,3,\tau_2\in D_1\end{cases} \tag{9}$$

证明

$$\begin{aligned}d_D(\tau_1,\tau_2)&=\left|(\{i\}\times D_j\cup\{i+1,i+2,i+3\}\times D_{1-j})\cap(\{i\}\times D_j\cup\{i+1,i+2,i+3\}\times D_{1-j}+(\tau_1,\tau_2))\right|\\&=\left|\{i\}\cap\{i+\tau_1\}\right|\left|D_j\cap(D_j+\tau_2)\right|+\left|\{i+1,i+2,i+3\}\cap\{i+\tau_1\}\right|\left|D_{1-j}\cap\{D_j+\tau_2\}\right|\\&\quad+\left|\{i\}\cap(i+1+\tau_1,i+2+\tau_1,i+3+\tau_1)\right|\left|D_j\cap D_j\cap(D_{1-j}+\tau_2)\right|\\&\quad+\left|\{i+1,i+2,i+3\}\cap(i+1+\tau_1,i+2+\tau_1,i+3+\tau_1)\right|\left|D_{1-j}\cap(D_{1-j}+\tau_2)\right|\\&=\begin{cases}2\left(v-1\right),\tau_1=0,\tau_2=0\\ v-1,\tau_1=1,2,3,\tau_2=0\\ (j,j)+3\left(1-j,1-j\right),\tau_1=0,\tau_2\in D_0\\ (j+1,j+1)+3\left(j,j\right),\tau_1=0,\tau_2\in D_1\\ (1-j,j)+(j,1-j)+2\left(1-j,1-j\right),\tau_1=1,2,3,\tau_2\in D_0\\ (j,j+1)+(1+j,j)+2\left(j,j\right),\tau_1=1,2,3,\tau_2\in D_1\end{cases}\end{aligned} \tag{10}$$

证毕

3　几乎平衡具有理想自相关函数值二进制序列构造

这部分将提出一种周期为$T=4v$具有理想自相关函数值的几乎平衡二进制序列的普遍构造方法。

定理1　设$v=2d+1$为一奇素数，其中$v\equiv 3\ (\mathrm{mod}4)$，当序列$w$的特征集$W$满足

$$W=\{i\}\times D_j\cup\{i+1,i+2,i+3\}\times D_{1-j}\cup V \tag{11}$$

其中

$V\in\{\{(i,0)\},\{(2+i,0)\},\{(i+1,0),(i+2,0),(i+3,0)\},\{(i,0),(i+1,0),(i+3,0)\}\}$ ($0\le i\le 3$, $0\le j\le 1$)。

那么得到的序列w是周期为$T=4v$且$R_w\left(\tau\ne 0\right)\in\{0,-4\}$的几乎平衡理想二进制序列。

证明　以$V=\{(2+i,0)\}$为例进行证明，其他情况的证明方法类似。根据式(4)，计算得到W的差函数$d_W\left(\tau_1,\tau_2\right)$为

$$\begin{aligned}d_W(\tau_1,\tau_2)=&\left|D\cap(D+(\tau_1,\tau_2))\right|\\&+\left|D\cap(D+(2+i+\tau_1,\tau_2))\right|\\&\left|(2+i,0)\cap(D+(\tau_1,\tau_2))\right|\\&+\left|(2+i,0)\cap(D+(2+i+\tau_1,\tau_2))\right|\end{aligned} \tag{12}$$

显然，当$(\tau_1,\tau_2)\ne(0,0)$时，可以得到

$$d_W(\tau_1,\tau_2)=d_D(\tau_1,\tau_2)+\varDelta(\tau_1,\tau_2) \tag{13}$$

其中，$d_D(\tau_1,\tau_2)$如式(9)所示，对于任意的整数$i\,(0\le i\le 3)$，$\varDelta(\tau_1,\tau_2)$可以表示为

$$\begin{aligned}\varDelta(\tau_1,\tau_2)&=|D\cap(2+i+\tau_1,\tau_2)|+|(2+i,0)\cap(D+(\tau_1,\tau_2))|\\&=|\{i\}\cap(2+i+\tau_1)|\,|D_j\cap\{\tau_2\}|+|\{i+2\}\cap(i+\tau_1)|\,|\{0\}\cap(D_j+\tau_2)|\\&\quad+|\{i+1,i+2,i+3\}\cap(2+i+\tau_1)|\,|D_{1-j}\cap\{\tau_2\}|\\&\quad+|\{i+2\}\cap(i+1+\tau_1,i+2+\tau_1,i+3+\tau_1)|\,|\{0\}\cap(D_{1-j}+\tau_2)|\\&=\begin{cases}|D_{1-j}\cap\{\tau_2\}|+|\{0\}\cap(D_{1-j}+\tau_2)|\,,\tau_1=0,1,3,\tau_2\neq 0\\|D_j\cap\{\tau_2\}|+|\{0\}\cap(D_j+\tau_2)|\,,\tau_1=2,\tau_2\neq 0\\0,\tau_1=1,2,3,\tau_2=0\end{cases}\end{aligned}\tag{14}$$

在下面的证明中，以$j=0$为例来计算$d_W(\tau_1,\tau_2)$，可以得到

$$d_W(\tau_1,\tau_2)=\begin{cases}(0,0)+3\,(1,1)+|D_1\cap\{\tau_2,-\tau_2\}|\,,\tau_1=0,\tau_2\in D_0\\(1,1)+3\,(0,0)+|D_1\cap\{\tau_2,-\tau_2\}|\,,\tau_1=0,\tau_2\in D_1\\(1,0)+(0,1)+2\,(1,1)+|D_1\cap\{\tau_2,-\tau_2\}|\,,\tau_1=1,3,\tau_2\in D_0\\(0,1)+(1,0)+3\,(0,0)+|D_1\cap\{\tau_2,-\tau_2\}|\,,\tau_1=1,3,\tau_2\in D_1\\(1,0)+(0,1)+2\,(1,1)+|D_0\cap\{\tau_2,-\tau_2\}|\,,\tau_1=2,\tau_2\in D_0\\(0,1)+(1,0)+3\,(0,0)+|D_0\cap\{\tau_2,-\tau_2\}|\,,\tau_1=2,\tau_2\in D_1\\v-1,\tau_1=1,2,3,\tau_2=0\end{cases}\tag{15}$$

由于$-1=\alpha^{\frac{v-1}{2}}=\alpha^d\in D_1$，式(15)可以简化为

$$\begin{aligned}d_W(\tau_1,\tau_2)&=\begin{cases}(0,0)+3\,(1,1)+1,\tau_1=0,\tau_2\in D_0\\(1,1)+3\,(0,0)+1,\tau_1=0,\tau_2\in D_1\\(1,0)+(0,1)+2\,(1,1)+1,\tau_1=1,2,3,\tau_2\in D_0\\(0,1)+(1,0)+3\,(0,0)+1,\tau_1=1,2,3,\tau_2\in D_1\\v-1,\tau_1=1,2,3,\tau_2=0\end{cases}\\&=\begin{cases}v-2,\tau_1=0,\tau_2\in Z_v^*\\v-1,\tau_1=1,2,3,\tau_2=Z_v\end{cases}\end{aligned}\tag{16}$$

根据式(4)和引理1，由集合W得到的二进制序列w的自相关函数值为

$$R_w(\tau_1,\tau_2)=\begin{cases}4v,\,(\tau_1,\tau_2)=(0,0)\\-4,\tau_1=0,\tau_1\in Z_v^*\\0,\tau_1=1,2,3,\tau_1\in Z_v\end{cases}\tag{17}$$

当V不变，i和j取其他值时，证明方法相同。由于序列w中1的个数为$|W|=2v-1$，所以，所得的二进制序列是几乎平衡的。 证毕

例1 设$v=7$，取本原元$\alpha=3$，那么，$D_0=\{1,2,4\}$, $D_1=\{3,5,6\}$。设$i=0$, $j=0$, $V=\{(2+i,0)\}$。可以得到$W=\{0\}\times D_1\cup\{1,2,3\}\times D_0\cup\{(2,0)\}$。根据中国剩余定理，构造得到的二进制序列为

$$\begin{aligned}w=(&-1,1,1,-1,-1,-1,-1,-1,-1,1,-1,1,1,\\&-1,1,1,-1,-1,1,-1,1,-1,1,1,1,1,-1,-1)\end{aligned}$$

且其自相关函数值为

$$[R_w(\tau)]_{\delta=0}^{27}=[28,\underbrace{0,0,0,-4}_{6次},0,0,0]$$

令$i=0$，$j=0$，当$V=\{(2+i,0)\}$时，定理1构造得到的特征集$W=\{0\}\times D_0\cup\{1,2,3\}\times D_1\cup\{(0,0)\}$为文献[15]中得到的几乎差集；当$V=\{(i,0),(i+1,0),(i+3,0)\}$时，特征集$W=\{0\}\times D_0\cup\{1,2,3\}\times D_1\cup\{(0,0),(1,0),(3,0)\}$，与文献[16]中相同。因此，通过定理1构造方法，不仅可以得到文献[15,16]中已知的理想二进制序列，还可以得到一些新的具有理想自相关特性的几乎平衡二进制序列，所以定理1方法较文献[15,16]方法更为普遍。此外，根据几乎差集和三值自相关二进制序列之间的关系，定理1还得到了一些新的几乎差集，其参数为Z_{4v}上的$(4v,2v-1,v-2,v-1)$或$(4v,2v+1,v,v-1)$。

4 (几乎)平衡具有理想自相关函数幅值的二进制序列构造

当$v\equiv 3\pmod 4$为素数时，基于定理1构造法得到了旁瓣值$R_w(\tau\neq 0)\in\{0,-4\}$的几乎平衡理想二进制序列。在本部分首先通过对定理1构造法进行适当改进，得到了一类新的周期为$T=4v\,(v\equiv 3\pmod 4$为素数)且具有理想自相关函数幅值的平衡二进制序列。

定理2 设$v=2d+1$为一奇素数，其中$v\equiv 3\pmod 4$，当序列w的特征集W满足

$$W=\{i\}\times D_j\cup\{i+1,i+2,i+3\}\times D_{1-j}\cup V\tag{18}$$

其中，$V\in\{\{(i,0),(i+1,0)\},\{(i+1,0),(i+2,0)\},\{(i,0),(i+2,0)\},\{(i+2,0),(i+3,0)\},\{(i,0),(i+3,0)\},$

$\{(i+1,0),(i+3,0)\}\},(0\le i\le 3,\ 0\le j\le 1)$，那么得到的序列$w$是周期为$T=4v$且$R_w(\tau\ne 0)\in\{0,\pm 4\}$的平衡理想二进制序列。

证明　以$V=\{(i,0),(i+1,0)\}$为例进行证明，证明方法与定理1类似。

由于$(\tau_1,\tau_2)\ne(0,0)$，所以W的差函数$d_W(\tau_1,\tau_2)$为

$$d_W(\tau_1,\tau_2)=d_D(\tau_1,\tau_2)+\varDelta(\tau_1,\tau_2) \tag{19}$$

其中，

$$\begin{aligned}\varDelta(\tau_1,\tau_2)=&\,|(i,0)\cap\{\{i+\tau_1\}\times(D_j+\tau_2),\{i+\tau_1+1\}\times(D_{1-j}+\tau_2),\{i+2+\tau_1\}\times(D_{1-j}+\tau_2),\\&\{i+3+\tau_1\}\times(D_{1-j}+\tau_2)\}|+|(i+1,0)\cap\{\{i+\tau_1\}\times(D_j+\tau_2),\\&\{i+\tau_1+1\}\times(D_{1-j}+\tau_2),\{i+2+\tau_1\}\times(D_{1-j}+\tau_2),\{i+3+\tau_1\}\times(D_{1-j}+\tau_2)\}|\\&+|\{\{i\}\times D_j,\{i+1\}\times D_{1-j},\{i+2\}\times D_{1-j},\{i+3\}\times D_{1-j}\}\cap(i+\tau_1,\tau_2)|\\&+|(i,0)\cap(i+1+\tau_1,\tau_2)|+|(i+1,0)\cap(i+\tau_1,\tau_2)|\\&+|\{\{i\}\times D_j,\{i+1\}\times D_{1-j},\{i+2\}\times D_{1-j},\{i+3\}\times D_{1-j}\}\cap(i+1+\tau_1,\tau_2)|\end{aligned} \tag{20}$$

对于任意的整数$i\,(0\le i\le 3)$, $\varDelta(\tau_1,\tau_2)$可以表示为

$$\varDelta(\tau_1,\tau_2)=\begin{cases}|D_j\cap\{\tau_2,-\tau_2\}|+|D_{1-j}\cap\{\tau_2,-\tau_2\}|,\tau_1=0,\tau_2\ne 0\\|\{D_j,D_{1-j}\}\cap\{-\tau_2\}|+2\,|D_{1-j}\cap\{\tau_2\}|,\tau_1=1,\tau_2\ne 0\\2\,|D_{1-j}\cap\{\tau_2,-\tau_2\}|,\tau_1=2,\tau_2\ne 0\\|\{D_j,D_{1-j}\}\cap\{\tau_2\}|+2\,|D_{1-j}\cap\{-\tau_2\}|,\tau_1=3,\tau_2\ne 0\\1,\tau_1=1,3,\tau_2=0\\0,\tau_1=2,\tau_2=0\end{cases} \tag{21}$$

设$j=1$，类似地，可以得到

$$d_W(\tau_1,\tau_2)=\begin{cases}v-1,\tau_1=0,\tau_2\in Z_v^*\\v+1,\tau_1=1,\tau_2\in D_0\\v-1,\tau_1=1,\tau_2\in D_1\\v,\tau_1=2,\tau_2\in Z_v\\v-1,\tau_1=3,\tau_2\in D_0\\v+1,\tau_1=3,\tau_2\in D_1\\v,\tau_1=1,3,\tau_2\in D_0\\v-1,\tau_1=2,\tau_2=0\end{cases} \tag{22}$$

根据式(22)，可以看出构造所得二进制序列w的自相关函数值及其分布。对于不同的j和V，以及任意的$i\,(0\le i\le 3)$，表1列出了定理2中构造得到的理想二进制序列w的自相关函数值的分布。

因为$|W|=2v$，所以得到的二进制序列都是平衡的。　　证毕

例2　设$v=7$，采用与例1相同长度为例来说明定理2的构造方法。设$i=0$，$j=1$，集合$V=\{(0,0),(1,0)\}$。可以得到二进制序列为

$$\begin{aligned}w=(&1,1,1,-1,-1,-1,-1,-1,-1,1,-1,1,1,\\&-1,-1,1,-1,-1,1,-1,1,1,1,1,1,1,-1,-1)\end{aligned}$$

其自相关函数值为

$$\begin{aligned}[R_w(\tau)]_{\delta=0}^{27}=&[28,4,0,4,-4,-4,0,0,-4,4,0,-4,-4,\\&-4,-4,-4,-4,-4,0,4,-4,0,0,-4,\\&-4,4,0,4]\end{aligned}$$

为了获得更多的理想二进制序列，接下来讨论奇素数$v\equiv 1\ (\mathrm{mod}4)$的情况。

定理3　设$v=2d+1$为一奇素数，其中$v\equiv 1\ (\mathrm{mod}4)$，当序列$w$的特征集$W$满足

$$W=\{i\}\times D_j\cup\{i+1,i+2,i+3\}\times D_{1-j}\cup V \tag{23}$$

其中，$V\in\{\{(i+1,0)\},\{(i,0),(i+1,0),(i+2,0)\},$

表 1　定理2中理想二进制序列的自相关函数值分布

j	$V\in$	$R(\tau_1,\tau_2)$	$(\tau_1,\tau_2)\in$
0	$\{\{(i,0),(i+1,0)\},\{(i+1,0),(i+2,0)\}\}$	–4	$\{1\}\times D_0\cup\{3\}\times D_1\cup\{0\}\times Z_v^*\cup\{(2,0)\},$
1	$\{\{(i,0),(i+3,0)\},\{(i+2,0),(i+3,0)\}\}$	0	$\{2\}\times Z_v^*\cup\{(1,0),(3,0)\},$
		4	$\{1\}\times D_1\cup\{3\}\times D_0$
0		–4	$\{0\}\times Z_v^*\cup\{(1,0),(3,0)\},$
	$\{\{(i,0),(i+2,0)\},\{(i+1,0),(i+3,0)\}\}$	0	$\{1,2,3\}\times Z_v^*,$
1		4	$\{(2,0)\}$
0	$\{\{(i+3,0),(i+2,0)\},\{(i,0),(i+3,0)\}\}$	–4	$\{0\}\times Z_v^*\cup\{1\}\times D_1\cup\{3\}\times D_0\cup\{(2,0)\},$
1	$\{\{(i,0),(i+1,0)\},\{(i+1,0),(i+2,0)\}\}$	0	$\{2\}\times Z_v^*\cup\{(3,0),(1,0)\},$
		4	$\{1\}\times D_0\cup\{3\}\times D_1$

注：$0\le i\le 3$

$\{(i+3,0)\},\{(i,0),(i+2,0),(i+3,0)\}\}$, $(0\le i\le 3$, $0\le j\le 1)$，那么得到的序列w是周期为$T=4v$且$R_w(\tau\ne 0)\in\{0,\pm 4\}$的几乎平衡理想二进制序列。

证明 以$V=\{(i+3,0)\}$为例进行证明，证明方法与定理1类似。

当$(\tau_1,\tau_2)\ne(0,0)$时，W的差函数为

$$d_W(\tau_1,\tau_2)=d_D(\tau_1,\tau_2)+\Delta(\tau_1,\tau_2)\tag{24}$$

其中，$d_D(\tau_1,\tau_2)$如式(9)所示，$\Delta(\tau_1,\tau_2)$可以表示为

$$\begin{aligned}\Delta(\tau_1,\tau_2)=&|D\cap\{3+i+\tau_1,\tau_2\}|\\&+|\{(3+i,0)\}\cap(D+(\tau_1,\tau_2))|\end{aligned}\tag{25}$$

对于任意的整数$i\,(0\le i\le 3)$，

$$\begin{aligned}&\Delta(\tau_1,\tau_2)\\&=\begin{cases}|D_{1-j}\cap\{\tau_2\}|+|D_{1-j}\cap\{-\tau_2\}|,\tau_1=0,2,\tau_2\ne 0\\|D_j\cap\{\tau_2\}|+|D_{1-j}\cap\{-\tau_2\}|,\tau_1=1,\tau_2\ne 0\\|D_{1-j}\cap\{\tau_2\}|+|D_j\cap\{-\tau_2\}|,\tau_1=3,\tau_2\ne 0\\0,\tau_1=1,2,3,\tau_2=0\end{cases}\end{aligned}\tag{26}$$

设$j=1$，显然，当d为偶数时，$-1\in D_0$，式(26)可以简化为

$$\Delta(\tau_1,\tau_2)=\begin{cases}2,\tau_1=0,2,\tau_2\in D_0\\1,\tau_1=1,3,\tau_2\in D_0,D_1\\0,\text{其他}\end{cases}\tag{27}$$

可以得到

$$d_W(\tau_1,\tau_2)=\begin{cases}v-2,\tau_1=0,\tau_2\in Z_v^*\\v-2,\tau_1=1,3,\tau_2\in D_0\\v,\tau_1=1,3,\tau_2\in D_1\\v-1,\text{其他}\end{cases}\tag{28}$$

根据式(28)，可以得到构造所得二进制序列w的自相关函数值及其分布。

类似地，对于任意的i，当j和集合V取不同的值时，构造得到的几乎平衡理想二进制序列的自相关函数值$\{0,4,-4\}$的分布是不同的。表2列出了定理3中不同j和V情况下构造得到的理想二进制序列的自相关函数值分布。

因为$|W|=2v-1$或$2v+1$，所以得到的二进制序列都是几乎平衡的。 证毕

例3 令$v=13$，取本原元$\alpha=2$，那么，$D_0=\{1,3,4,9,10,12\}$，$D_1=\{2,5,6,7,8,11\}$。设$i=0$，$j=1$，集合$V=\{(3,0)\}$，得到的二进制序列为

$$\begin{aligned}w=(&-1,1,-1,1,-1,-1,-1,-1,1,1,1,-1,-1,-1,1,\\&-1,-1,1,-1,-1,1,-1,1,1,1,1,-1,1,1,1,1,\\&-1,1,-1,-1,1,-1,-1,1,1,-1,-1,1,1,1,\\&-1,-1,-1,-1,1,-1,1)\end{aligned}$$

其自相关函数值为

$$\begin{aligned}[R_w(\tau)]_{\tau=0}^{51}=[&52,-4,0,-4,-4,4,0,4,-4,-4,0,4,\\&-4,0,0,4,-4,-4,0,4,-4,4,0,-4,\\&-4,-4,0,-4,-4,-4,0,-4,-4,4,0,\\&-4,-4,4,0,0,-4,4,0,-4,\\&-4,4,0,4,-4,-4,0,-4]\end{aligned}$$

5 构造方法比较

表3列出了目前已有周期为$T\equiv 0\,(\mathrm{mod}4)$ 理想二进制序列的主要构造方法，与已有成果相比，本文构造方法的优点主要体现在如下几个方面：一是直接构造法，本文提出的3种构造方法都是直接构造法，而文献[7,10–14]采用的均是交织法，所得序列的特性受所采用基序列或移位序列影响；二是平衡性更好，当$v\equiv 3\ (\mathrm{mod}4)$时，文献[7,10–12,14]得到的理想二进制序列都为几乎平衡或不平衡序列，而本文定理2中获得的理想二进制序列都为平衡序列；三是得到的序列更多，同文献[15,16]相比，虽然采用的都是直接构造方法，但该文定理1中构造得到的理想二进制序列不仅包含文献[15,16]中序列，而且还可得到一些新的具有理想自相关特性的几乎平衡二进制序列，从而也可得到一些新的参数为$(4v,2v+1,v,v-1)$的几乎差集。

6 结束语

基于中国剩余定理和2阶分圆类，本文提出3种周期为$T=4v$(v为奇素数)理想二进制序列直接构造方法。构造所得序列的周期自相关函数值均满足理论界：当$v\equiv 3\ (\mathrm{mod}4)$时，序列的周期自相关函数旁瓣值取值集合为$\{0,-4\}$或$\{0,4,-4\}$；当$v\equiv 1$

表 2 定理3中理想二进制序列的自相关函数值分布

j	$V\in$	$R(\tau_1,\tau_2)$	$(\tau_1,\tau_2)\in$
0	$\{\{(i+1,0)\},\{(i+3,0)\}\}$	–4	$\{0\}\times Z_v^*\cup\{1,3\}\times D_1$,
1	$\{\{(i,0),(i+1,0),(i+2,0)\}$,	0	$\{2\}\times Z_v^*\cup\{(1,0),(2,0),(3,0)\}$,
	$\{(i,0),(i+2,0),(i+3,0)\}\}$	4	$\{1,3\}\times D_0$
0	$\{\{(i,0),(i+1,0),(i+2,0)\}$,	–4	$\{0\}\times Z_v^*\cup\{1,3\}\times D_0$,
	$\{(i,0),(i+2,0),(i+3,0)\}\}$	0	$\{2\}\times Z_v^*\cup\{(1,0),(2,0),(3,0)\}$,
1	$\{\{(i+1,0)\},\{(i+3,0)\}\}$	4	$\{1,3\}\times D_1$

注：$0\le i\le 3$

表 3　已知周期为$T\equiv 0\ (\mathrm{mod}4)$的具有理想自相关值/幅度的二进制序列总结

周期 T	$R(\tau\neq 0)$	平衡性	构造方法
$T=4v,\ v\equiv 3(\mathrm{mod}4)$	$\{0,-4\}$	几乎平衡	交织法[10]
$T=4v,\ v=2^{2k}-1$	$\{0,\pm 4\}$	几乎平衡	交织法[11]
$T=4v,\ v=p\,(p+2),\ p$和$p+2$为素数	$\{0,\pm 4\}$	不平衡	交织法[11]
$T=4v,\ v=2^m-1,\ m$为整数	$\{0,\pm 4\}$	几乎平衡	交织法[12]
$T=4v,\ v\equiv 3(\mathrm{mod}4),\ v$为整数	$\{0,-4\}$	几乎平衡	中国剩余定理[16]
$T=4v,\ v\equiv 3(\mathrm{mod}4),\ v$为素数	$\{0,-4\}$	几乎平衡	分圆类[15]
$T=p^m-1,\ \dfrac{p^m-1}{2}$为偶数	$\{0,-4\}$	平衡	基于多项式$z\,(1-z)$[8]
$T=p^m-1,\ p$为奇素数	$\{0,-4\}$	平衡或几乎平衡	基于多项式$(z+1)^d+az^d+b$[9]
$T=4v,\ v\equiv 3(\mathrm{mod}4)$	$\{0,\pm 4\}$	几乎平衡或不平衡	一般化交织法[7]
$T=4v,\ v\equiv 2(\mathrm{mod}4)$	$\{0,\pm 4\}$	几乎平衡	交织法[13]
$T=4v,\ v\equiv 1(\mathrm{mod}4),\ v$为素数	$\{0,\pm 4\}$	平衡或不平衡	交织法[14]
$T=4v,\ v\equiv 3(\mathrm{mod}4),\ v$为素数	$\{0,-4\}$	几乎平衡	广义分圆，定理1
$T=4v,\ v\equiv 3(\mathrm{mod}4),\ v$为素数	$\{0,\pm 4\}$	平衡	广义分圆，定理2
$T=4v,\ v\equiv 1(\mathrm{mod}4),\ v$为素数	$\{0,\pm 4\}$	几乎平衡	广义分圆，定理3

(mod4)时，相应的取值集合为$\{0,4,-4\}$。本文构造方法拓展了现有平衡和几乎平衡理想二进制序列存在空间，可为工程应用提供更多性能优良的理想序列，同时也丰富了组合设计理论。

参 考 文 献

[1] GOLOMB S W and GONG G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Rader[M]. Cambridge: Cambridge University Press, 2005: 105–110.

[2] LUKE H D, SCHOTTEN H D, and HADINEJAD–MAHRAM H. Binary and quadriphase sequences with optimal autocorrelation properties: A survey[J]. *IEEE Transactions on Information Theory*, 2003, 49(12): 3271–3282. doi: 10.1109/TIT.2003.820035.

[3] 彭秀平, 冀惠璞, 郑德亮, 等. 周期为2q理想几乎四进制序列构造研究[J]. 通信学报, 2019, 40(12): 105–113. doi: 10.11959/j.issn.1000-436x.2019225.

PENG Xiuping, JI Huipu, ZHENG Deliang, *et al*. Study on the constructions of optimal almost quaternary sequences with period 2q[J]. *Journal on Communications*, 2019, 40(12): 105–113. doi: 10.11959/j.issn.1000-436x.2019225.

[4] 刘涛, 许成谦, 李玉博. 一类相互正交的最佳二元零相关区序列集构造法[J]. 电子与信息学报, 2017, 39(10): 2442–2448. doi: 10.11999/JEIT161365.

LIU Tao, XU Chengqian, and LI Yubo. Construction of optimal mutually orthogonal sets of binary zero correlation zone sequences[J]. *Journal of Electronics & Information Technology*, 2017, 39(10): 2442–2448. doi: 10.11999/JEIT161365.

[5] 李玉博, 刘涛, 陈晓玉. 几乎最优二元多子集零相关区序列集构造法[J]. 电子与信息学报, 2018, 40(3): 705–712. doi: 10.11999/JEIT170603.

LI Yubo, LIU Tao, and CHEN Xiaoyu. Construction of almost optimal binary mutiple zero correlation zone sequence sets[J]. *Journal of Electronics & Information Technology*, 2018, 40(3): 705–712. doi: 10.11999/JEIT170603.

[6] 李玉博, 陈邈. 几乎完备高斯整数序列构造法[J]. 电子与信息学报, 2018, 40(7): 1752–1758. doi: 10.11999/JEIT170844.

LI Yubo and CHEN Miao. Construction of nearly perfect gaussian integer sequences[J]. *Journal of Electronics & Information Technology*, 2018, 40(7): 1752–1758. doi: 10.11999/JEIT170844.

[7] YAN Tongjiang, CHEN Zhixiong, and LI Bao. A general construction of binary interleaved sequences of period $4N$ with optimal autocorrelation[J]. *Information Sciences*, 2014, 287: 26–31. doi: 10.1016/j.ins.2014.07.026.

[8] LEMPEL A, COHN M, and EASTMAN W. A class of balanced binary sequences with optimal autocorrelation properties[J]. *IEEE Transactions on Information Theory*, 1977, 23(1): 38–42. doi: 10.1109/TIT.1977.1055672.

[9] NO J S, CHUNG H, SONG H Y, *et al*. New construction for binary sequences of period p^m-1 with optimal autocorrelation using $(z+1)^d+z^d+b$[J]. *IEEE Transactions on Information Theory*, 2001, 47(4): 1638–1644. doi: 10.1109/18.923752.

[10] TANG Xiaohu and DING Cunsheng. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value[J]. *IEEE Transactions*

on Information Theory, 2010, 56(12): 6398–6405. doi: 10.1109/TIT.2010.2081170.

[11] TANG Xiaohu and GONG Guang. New constructions of binary sequences with optimal autocorrelation value/magnitude[J]. *IEEE Transactions on Information Theory*, 2010, 56(3): 1278–1286. doi: 10.1109/TIT.2009.2039159.

[12] NAM Y Y and GONG Guang. New binary sequences with optimal autocorrelation magnitude[J]. *IEEE Transactions on Information Theory*, 2008, 54(10): 4771–4779. doi: 10.1109/TIT.2008.928999.

[13] KRENGEL E I and IVANOV P V. Two constructions of binary sequences with optimal autocorrelation magnitude[J]. *Electronics Letters*, 2016, 52(17): 1457–1459. doi: 10.1049/el.2016.2476.

[14] SU Wei, YANG Yang, and FAN Cuiling. New optimal binary sequences with period $4p$ via interleaving Ding–Helleseth–Lam sequences[J]. *Designs, Codes and Cryptography*, 2018, 86(6): 1329–1338. doi: 10.1007/s10623-017-0398-5.

[15] ZHANG Yuan, LEI Jianguo, and ZHANG Shaopu. A new family of almost difference sets and some necessary conditions[J]. *IEEE Transactions on Information Theory*, 2006, 52(5): 2052–2061. doi: 10.1109/TIT.2006.872969.

[16] ARASU K T, DING C, HELLESETH T, *et al*. Almost difference sets and their sequences with optimal autocorrelation[J]. *IEEE Transactions on Information Theory*, 2001, 47(7): 2934–2943. doi: 10.1109/18.959271.

[17] DING C, PEI D, and SALOMAA A. Chinese Remainder Theorem: Applications in Computing, Coding, Cryptograph[M]. Singapore: World Scientific, 1996: 82–85.

彭秀平：女，1984年生，副教授，研究方向为编码理论、信号设计等.

冀惠璞：女，1995年生，硕士生，研究方向为编码理论、信号设计等.

林洪彬：男，1979年生，副教授，研究方向为RGBD图像/点云/网格曲面语义标注与分割、点云结构推理与纹理修复等.

刘 刚：男，1973年生，讲师，研究方向为无线网络通信等.

责任编辑：马秀强