基于 Zadoff-Chu 矩阵的最优码本构造方法

李玉博[1,2]，刘胜毅[1,2]，张景景[1,2]，贾冬艳[3]

（1. 燕山大学信息科学与工程学院，河北 秦皇岛 066004；2. 河北省信息传输与信号处理重点实验室，河北 秦皇岛 066004；
3. 河北科技师范学院数学与信息科技学院，河北 秦皇岛 066004）

摘 要：具有低相关性质的码本在同步码分多址系统（CDMA）、量子信息理论以及压缩感知领域都有重要应用。为扩展码本数量，放宽了变换矩阵的限制条件。基于 Zadoff-Chu 矩阵，利用差集、几乎差集以及有限域特征和构造了新的码本，得到的码本依照 Welch 界限或 Levenstein 界是最优或几乎最优的。通过实验仿真发现，基于该类码本构造的确定性测量矩阵在压缩感知中具有良好的性能。

关键词：码本；差集；几乎差集；Welch 界；Levenstein 界

中图分类号：TN911.2

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020021

Construction method of optimal codebook based on Zadoff-Chu matrix

LI Yubo[1,2], LIU Shengyi[1,2], ZHANG Jingjing[1,2], JIA Dongyan[3]

1. School of Information Science & Engineering, Yanshan University, Qinhuangdao 066004, China
2. Hebei Key Laboratory of Information Transmission and Signal Processing, Qinhuangdao 066004, China
3. School of Mathematics and Information Science & Technology, Hebei Normal University of Science & Technology, Qinhuangdao 066004, China

Abstract: Codebooks with low-coherence have wide utilization in code division multiple access (CDMA) communications, quantum information theory, compressed sensing and so on. In order to expand the number of codebooks, the restrictions on the transformation matrix were relaxed. Based on the Zadoff-Chu matrix, new codebooks were constructed using the difference set, almost difference set, and finite field character sum. The proposed codebooks were optimal or near optimal according to the Welch bound or Levenstein bound. Through experimental simulation, it is found that the deterministic measurement matrices constructed using these codebooks also have good performance in the process of compressed sensing.

Key words: codebook, difference set, almost difference set, Welch bound, Levenstein bound

1 引言

码本是一类具有较低相关性的信号集，在同步码分多址（CDMA, code division multiple access）通信系统[1]、量子编码理论[2]以及压缩感知领域具有重要应用[3]。构造参数达到理论界限的最优码本是现代通信理论的重要研究课题之一，因此码本构造方法的研究受到人们的广泛关注。一般来说，码本 $\boldsymbol{C}$ 由 2 个参数进行表示，即 (N,K)，其中，N 表示码本的数量，K 表示码本的长度。码本的字符集是码本中所有码字的坐标所采用的不同复数值的集合，字符集大小是字符集中元素的数量。在实际应用中，字符集较小的码本具有重要的意义。另外，码本的最大互相关幅度值用 $I_{\max}(\boldsymbol{C})$ 表示。在通信系统中，希望码本的最大互相关幅度值 $I_{\max}(\boldsymbol{C})$ 越小越好，以尽可能消除信号之间的干扰。在压缩感知领域，具有低相关性的码本可用于构造测量矩阵。根据压缩感知理论可知，码本最大互相关幅度值

收稿日期：2019–07–18；**修回日期：**2019–12–07

基金项目：国家自然科学基金资助项目（No.61501395）

Foundation Item: The National Natural Science Foundation of China (No.61501395)

$I_{\max}(\boldsymbol{C})$越低，其对应的测量矩阵 RIP（restricted isometry property）性能越好[2]。除此之外，在量子信息领域中[3], 码本还用于构造 SIC-POVM（symmetric informationally complete positive operator-valued measure）和无偏正交基（MUB, mutually unbiased base）。码本的参数受到理论界限的制约，当$N \geqslant K$时，称最大互相关幅度值满足 Welch 界限的码本为最优码本；当$N > K^2$时，称最大互相关幅度值满足 Levenstein 界限的码本为最优码本。近年来，研究人员提出了很多近似达到 Welch 界或 Levenstein 界的码本构造方法。文献[4]首次利用差集构造了最优码本。Ding 等[5-6]进一步利用差集和几乎差集构造了参数达到 Welch 界的最优码本。文献[7-10]利用分圆类方法构造了具有优良参数的码本。除此之外，还有一些利用 bent 函数[11]、平坦函数[12]、有限域上的特征和理论[13-16]以及二元线性码[17]来构造码本的方法。

近年来，文献[18]提出一类基于二元序列与变换矩阵的码本构造框架。该框架包含了已有的许多码本构造方法，如文献[4-6]的方法等。该类方法有 2 个关键因素：1) 满足一定条件的变换矩阵的构造；2) 二元序列支撑集的选取。现有的码本构造方法大部分都是基于已有的变换矩阵如离散傅里叶逆变换（IDFT, inverse discrete Fourier transform）矩阵、Hadamard 矩阵，通过选取不同的二元序列支撑集来构造码本。基于同样的思想，文献[19-20]通过选取一类新的二元序列构造了一类新的最优码本。本文放宽了文献[18]对初始变换矩阵的条件限制，构造了一类新的变换矩阵，并结合现有的一些特殊的整数集合构造了参数达到渐进最优的码本。

2　基本概念

一个参数为(N,K)的码本是一个复向量集合$\boldsymbol{C}=\{\boldsymbol{C}_0,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_{N-1}\}$，其中每个向量$\boldsymbol{C}_n=(c_{n,0}, c_{n,1},\cdots,c_{n,K-1})$是长度为$K$的单位复向量，其中$0\leqslant n\leqslant N-1$，$\sum_{k=0}^{K-1}(c_{n,k})^2=1$。对于任意 2 个向量$\boldsymbol{C}_{n_1},\boldsymbol{C}_{n_2}\in\boldsymbol{C}$，定义厄米特（Hermitian）内积为$\boldsymbol{C}_{n_1}(\boldsymbol{C}_{n_2})^{\mathrm{H}}=\sum_{k=0}^{K-1}c_{n_1,k}c_{n_2,k}^{*}$，其中$(\cdot)^{\mathrm{H}}$表示向量的共轭转置。向量集合$\boldsymbol{C}$中最大互相关幅度值定义为

$$I_{\max}(\boldsymbol{C})=\max_{0\leqslant n_1\neq n_2\leqslant N-1}\left|\boldsymbol{C}_{n_1}(\boldsymbol{C}_{n_2})^{\mathrm{H}}\right| \tag{1}$$

对于码本的最大互相关幅度值，有以下界限成立。

引理 1[4]　对于一个参数为(N,K)的码本$\boldsymbol{C}$，其中$N\geqslant K$，则有

$$I_{\max}(\boldsymbol{C})\geqslant\sqrt{\frac{N-K}{(N-1)K}} \tag{2}$$

式(2)中等号成立的条件是当且仅当对于任意的$0\leqslant n_1\neq n_2\leqslant N-1$，有

$$\left|\boldsymbol{C}_{n_1}\left(\boldsymbol{C}_{n_2}\right)^{\mathrm{H}}\right|=\sqrt{\frac{N-K}{(N-1)K}} \tag{3}$$

当式(3)成立时，则码本最大互相关幅度值达到 Welch 界限，称为 MWBE（maximum-Welch-bound-equality）码本；当$N>K^2$时，不存在达到 Welch 界的(N,K)码本，此时 Levenstein 界更紧。

引理 2[11]　对于任意参数为(N,K)的实码本，若$N>\frac{K(K+1)}{2}$，则有

$$I_{\max}(\boldsymbol{C})\geqslant\sqrt{\frac{3N-K^2-2K}{(N-K)(K+2)}} \tag{4}$$

对于任意参数为(N,K)的复数码本，若$N>K^2$，则有

$$I_{\max}(\boldsymbol{C})\geqslant\sqrt{\frac{2N-K^2-K}{(N-K)(K+1)}} \tag{5}$$

一般称达到 Welch 界或 Levenstein 界的码本为最优码本，对于最优码本的构造方法研究具有重要的应用价值。

设p为素数，$\mathbb{F}_p$表示包含有p个元素的有限域，$\mathbb{F}_p^*=\mathbb{F}_p\setminus\{0\}$。令$\mathbb{Z}_N=\{0,1,2,\cdots,N-1\}$表示一个模$N$的整数环。

定义 1　设$q=p^n$是素数幂，p为素数，令α表示循环群$\mathbb{F}_{q^s}^*$的生成元，有限域$\mathbb{F}_{q^s}$上的乘法特征定义为

$$\chi_a(\alpha^i)=\omega_{q^s-1}^{ai},a\in\mathbb{F}_{q^s},0\leqslant i\leqslant q^s-2 \tag{6}$$

其中，$\omega_{q^s-1}=\mathrm{e}^{\frac{2\pi\sqrt{-1}}{q^s-1}}$。当$a=0$时，称$\chi_a$为平凡乘法特征，否则称$\chi_a$为非平凡乘法特征。定义$\chi(0)=0$，对于乘法特征，满足$\chi(xy)=\chi(x)\chi(y),x,y\in\mathbb{F}_{q^s}$。

定义 2　设集合$D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$表示有限域$\mathbb{F}_p$上一个子集，定义集合$D$的差函数为$f_D(\tau)=\left|(\tau+D)\bigcap D\right|$，$\tau\in\mathbb{F}_p$。如果满足当$\tau$取遍$\mathbb{F}_p$上非 0 元素时，差函数$f_D(\tau)$取值为$\lambda$出现$p-1$次，

则称集合 D 是有限域 $\mathbb{F}_p$ 上的一个差集，参数表示为 (p,K,λ)-DS。

显然，对于差集 (p,K,λ)-DS，有 $K(K-1)=(p-1)\lambda$ 成立。

定义 3 设集合 $D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$ 表示有限域 $\mathbb{F}_p$ 上一个子集，定义集合 D 的差函数为 $f_D(\tau)=\left|(\tau+D)\bigcap D\right|$，$\tau\in\mathbb{F}_p$。如果满足当 τ 取遍 $\mathbb{F}_p$ 上非 0 元素时，差函数 $f_D(\tau)$ 取值为 λ 出现 t 次，取值为 λ+1 出现 $p-1-t$ 次，则称集合 D 是有限域 $\mathbb{F}_p$ 上的一个几乎差集，参数表示为 (p,K,λ,t)-ADS。

定义 4 令 $D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$ 表示整数环 $\mathbb{Z}_J$ 上一个含有 K 个不同整数的集合，$d_k\in\mathbb{Z}_J$，$0\leqslant k\leqslant K-1$。集合 D 的特征序列定义为一个二元序列 $a=(a_0,a_1,\cdots,a_{J-1})$，其中有

$$a_t=\begin{cases}1, & t\in D\\ 0, & t\notin D\end{cases},\quad 0\leqslant t\leqslant J-1 \tag{7}$$

则称集合 D 为序列 $a=(a_0,a_1,\cdots,a_{J-1})$ 的支撑集。显然，序列的汉明重量 $\mathrm{wt}(a)=\left|D\right|=K$。

定义 5 设 N,γ 是 2 个互质的正整数，则 Zadoff-Chu 序列族的第 γ 行序列可以表示为

$$s_\gamma(k)=\begin{cases}\exp\left(-\dfrac{\mathrm{i}\pi\gamma k(k+2g)}{N}\right), & N\text{是偶数}\\ \exp\left(-\dfrac{\mathrm{i}\pi\gamma k(k+1+2g)}{N}\right), & N\text{是奇数}\end{cases} \tag{8}$$

其中，$k=0,1,\cdots,N-1$，g 是一个整数。

3 基于二元序列的码本构造框架

文献[18]提出一类基于二元序列的码本构造框架，其构造过程如下。

步骤 1 定义一个变换矩阵 $\boldsymbol{\Phi}=\left[\phi_{i,l}\right]_{J\times N}$，令 $\phi_{i,l}$ 表示矩阵中任意元素，$0\leqslant i\leqslant J-1$，$0\leqslant l\leqslant N-1$。矩阵 $\boldsymbol{\Phi}=\left[\phi_{i,l}\right]_{J\times N}$ 满足以下性质。

性质 1 每个矩阵元素具有单位幅值，即 $\left|\phi_{i,l}\right|=1$。

性质 2 任意 2 个不同列向量满足 $\phi_{i,l_1}^{*}\phi_{i,l_2}=\phi_{i,l}$，$0\leqslant l_1\neq l_2$，$l\leqslant N-1$，$0\leqslant i\leqslant J-1$。

性质 3 矩阵 $\boldsymbol{\Phi}$ 的第一列为全 1 向量，即 $\phi_{i,0}=1$，$0\leqslant i\leqslant J-1$。

性质 4 对于任意 $0<l\leqslant N-1$，有 $\sum_{i=0}^{J-1}\phi_{i,l}=0$。

满足上述性质的变换矩阵已知的有 $N\times N$ 的 Hadamard 矩阵和 IDFT 矩阵。

步骤 2 取二元序列 $a=\left(a_0,a_1,\cdots,a_{J-1}\right)$，序列的汉明重量 $\mathrm{wt}(a)=K$，设集合 $D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$ 是序列 a 的支撑集。构造码本 $\boldsymbol{C}_{\boldsymbol{\Phi}}(a)=\{\boldsymbol{C}_0,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_{N-1}\}$ 为

$$C_l=\frac{1}{\sqrt{K}}(\phi_{d_0,l},\phi_{d_1,l},\cdots,\phi_{d_{K-1},l}),\quad 0\leqslant l\leqslant N-1 \tag{9}$$

其中，C_l 为构造的码本中的一个行向量，集合 D 是变换矩阵 $\boldsymbol{\Phi}$ 的行索引集，即元素 $\phi_{d_k,l}(0\leqslant k\leqslant K-1)$ 是矩阵中第 d_k 行、第 l 列元素，则 $\boldsymbol{C}_{\boldsymbol{\Phi}}(a)$ 即为得到的 (N,K) 码本，其最大互相关幅度值 $I_{\max}(\boldsymbol{C}_{\boldsymbol{\Phi}}(a))$ 可以由变换矩阵与二元序列的支撑集计算得到。

文献[18]构造的框架包含了已有的一些码本构造方法作为特殊情况。例如，当选取 $N\times N$ 阶的 IDFT 矩阵作为变换矩阵 $\boldsymbol{\Phi}$ 时，若选取的二元序列对应的支撑集为差集时，得到的码本 $\boldsymbol{C}_{\boldsymbol{\Phi}}(a)$ 即为文献[4]的结果。若二元或复 Hadamard 矩阵作为矩阵 $\boldsymbol{\Phi}$，则选取的二元序列对应支撑集为几乎差集时，得到的码本 $\boldsymbol{C}_{\boldsymbol{\Phi}}(a)$ 为文献[5-6]的结果。该构造框架有 2 个关键因素：1) 变换矩阵 $\boldsymbol{\Phi}$ 的选取；2) 二元序列 a 的支撑集选取。基于该构造框架，文献[19]通过选取不同的二元序列构造了参数几乎最优的码本。同时文献[19]也指出，可以通过构造新的变换矩阵来构造新的码本，然而并没有给出新的变换矩阵构造方法。文献[20]同样采用 Hadamard 矩阵作为变换矩阵，通过设计一类新的二元序列进而构造了一类最优码本。本文从另一个角度出发，通过设计新的变换矩阵来构造新的码本。

4 最优码本的构造

本文提出的新的构造方法介绍如下。

步骤 1 根据定义 5，令 $g=0$，$\gamma=1$，N 是偶数，得到 Zadoff-Chu 矩阵的第一行。令 $\phi_k=\mathrm{e}^{\frac{-\mathrm{i}\pi k^2}{N}}$，$k=0,1,\cdots,N-1$，由此定义 Zadoff-Chu 矩阵 $\boldsymbol{\Phi}=\left[\phi_{s,t}\right]_{N\times N}$ 为

$$\phi_{s,t}=\mathrm{e}^{\frac{-\pi\sqrt{-1}(s-t)^2}{N}} \tag{10}$$

其中，$0\leqslant s,t\leqslant N-1$。文献[21]中令矩阵 $\boldsymbol{\Phi}$ 的 N 为偶数来构造测量矩阵，而本文取 N 为奇数的情况来构造码本。

步骤 2 设 $D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$ 表示整数环

$\mathbb{Z}_N$ 上一个含有 K 个不同整数的集合，$d_k \in \mathbb{Z}_N$，$0 \leqslant k \leqslant K-1$。构造码本 $\boldsymbol{C}_{\boldsymbol{\Phi}} = \{\boldsymbol{C}_0, \boldsymbol{C}_1, \cdots, \boldsymbol{C}_{N-1}\}$ 为

$$\boldsymbol{C}_l = \frac{1}{\sqrt{K}}\left(\phi_{d_0,l}, \phi_{d_1,l}, \cdots, \phi_{d_{K-1},l}\right),\ 0 \leqslant l \leqslant N-1 \tag{11}$$

则 $\boldsymbol{C}_{\boldsymbol{\Phi}}$ 即为得到的 (N,K) 码本。

定理 1　令 $\boldsymbol{C}_{\boldsymbol{\Phi}}$ 为本文新的构造法得到 (N,K) 码本，则最大相关幅度值为

$$I_{\max}(\boldsymbol{C}_{\boldsymbol{\Phi}}) = \frac{1}{K}\left|\sum_{d_k \in D} \omega_N^{\Delta d_k}\right| \tag{12}$$

其中，$0 < |\Delta| \leqslant N-1$ 为一个非 0 的实数。

证明　设 $\boldsymbol{C}_l, \boldsymbol{C}_t \in \boldsymbol{C}_{\boldsymbol{\Phi}}$，$0 \leqslant t \neq l \leqslant N-1$，则有

$$\begin{aligned}
&\left|\boldsymbol{C}_t(\boldsymbol{C}_l)^{\mathrm{H}}\right| = \left|\frac{1}{K}\sum_{k=0}^{K-1}\phi_{d_k,t}(\phi_{d_k,l})^*\right| = \\
&\frac{1}{K}\left|\sum_{d_k \in D} \mathrm{e}^{\frac{-\pi\sqrt{-1}(t-d_k)^2}{N}} \mathrm{e}^{\frac{\pi\sqrt{-1}(l-d_k)^2}{N}}\right| = \\
&\frac{1}{K}\left|\mathrm{e}^{\frac{\pi\sqrt{-1}(l^2-t^2)}{N}} \sum_{d_k \in D} \mathrm{e}^{\frac{2\pi\sqrt{-1}d_k(l-t)}{N}}\right| = \\
&\frac{1}{K}\left|\sum_{d_k \in D} \omega_N^{(l-t)d_k}\right|
\end{aligned} \tag{13}$$

其中，$\omega_N = \mathrm{e}^{\frac{2\pi\sqrt{-1}}{N}}$。令 $\Delta = l - t$，所以 $\left|\boldsymbol{C}_t(\boldsymbol{C}_l)^{\mathrm{H}}\right| = \frac{1}{K}\left|\sum_{d_k \in D} \omega_N^{\Delta d_k}\right|$，由 $0 \leqslant t \neq l \leqslant N-1$ 可知 $0 < |\Delta| \leqslant N-1$，定理 1 成立。

证毕。

容易验证，新的构造法中设计的变换矩阵 $\boldsymbol{\Phi} = \left[\phi_{\mathrm{s,t}}\right]_{N\times N}$ 满足文献[18]中变换矩阵的性质 1，但不满足性质 2~性质 4，因此本文方法放松了对变换矩阵的限制条件。文献[18]采用的变换矩阵为 $N \times N$ 的 Hadamard 矩阵和 IDFT 矩阵，其构造的码本的字符集大小为 p，而本文设计的变换矩阵放松了限制条件，但是对码本带来的性能上的损失是码本的字符集变大了。由定理 1 可知，码本的最大相关幅度值与二元序列的支撑集有关。具体地，可以选择合适的集合 $D = \{d_0, d_1, d_2, \cdots, d_{K-1}\}$，使所对应的 $\left|\sum_{d_k \in D} \omega_N^{\Delta d_k}\right|$ 值尽可能小。下面通过选取不同的集合 $D = \{d_0, d_1, d_2, \cdots, d_{K-1}\}$ 来构造码本。

4.1　基于差集的最优码本

引理 3[5]　令集合 $D = \{d_0, d_1, d_2, \cdots, d_{K-1}\}$ 表示有限域 $\mathbb{F}_p$ 上的一个差集 (p,K,λ)-DS，则对于任意 $\gamma \neq 0 (\mathrm{mod}\ p)$ 有

$$\left|\sum_{k=0}^{K-1} \omega_p^{\gamma d_k}\right| = \sqrt{\frac{K(p-K)}{p-1}} \tag{14}$$

其中，$\omega_p = \mathrm{e}^{\frac{2\pi\sqrt{-1}}{p}}$。

根据引理 3，可以得到下面结论。

定理 2　令 $N = p$ 为素数，若集合 $D = \{d_0, d_1, d_2, \cdots, d_{K-1}\}$ 为有限域 $\mathbb{F}_p$ 上的一个差集 (p,K,λ)-DS，则式(9)定义的码本参数为 (p,K)，码本的字符集大小为 $2p$，最大相关幅度值为 $I_{\max}(\boldsymbol{C}_{\boldsymbol{\Phi}}) = \sqrt{\frac{p-K}{(p-1)K}}$，该码本达到 Welch 界。

证明　码本的最大相关幅度值可以由定理 1 和引理 3 直接得到。根据引理 1 可知，该码本最大相关幅度值等于 Welch 界，是一类最优的码本。

证毕。

例 1　令 $p = 7$，取集合 $D = \{1,2,4\}$，可知其是一个差集(7,3,1)-DS，得到(7,3)码本为

$$\boldsymbol{C}_0 = \frac{1}{\sqrt{3}}(\zeta_7^1, \zeta_7^4, \zeta_7^2),\ \boldsymbol{C}_1 = \frac{1}{\sqrt{3}}(\zeta_7^0, \zeta_7^1, \zeta_7^9),$$

$$\boldsymbol{C}_2 = \frac{1}{\sqrt{3}}(\zeta_7^1, \zeta_7^0, \zeta_7^4),\ \boldsymbol{C}_3 = \frac{1}{\sqrt{3}}(\zeta_7^4, \zeta_7^1, \zeta_7^1),$$

$$\boldsymbol{C}_4 = \frac{1}{\sqrt{3}}(\zeta_7^9, \zeta_7^4, \zeta_7^0),\ \boldsymbol{C}_5 = \frac{1}{\sqrt{3}}(\zeta_7^2, \zeta_7^9, \zeta_7^1),$$

$$\boldsymbol{C}_6 = \frac{1}{\sqrt{3}}(\zeta_7^{11}, \zeta_7^2, \zeta_7^4)$$

其中，$\zeta_7 = \mathrm{e}^{\frac{-\pi\sqrt{-1}}{7}}$。该码本最大相关幅度值为 0.471 4。

定理 2 得到的码本与文献[4,18]具有相同的参数和相同的最大相关幅值，但不是同一类码本。由于变换矩阵的选择不同，2 类码本内部的元素也不相同。文献[4,18]的码本选取的变换矩阵是 IDFT 矩阵，字符集更小；而定理 2 构造的码本的变换矩阵是 Zadoff-Chu 矩阵，限制条件更少，构造更灵活。例如，选取同样的差集 $D = \{1,2,4\}$，文献[4,18]得到的码本为

$$\boldsymbol{C}_0 = \frac{1}{\sqrt{3}}(\omega_7^0, \omega_7^0, \omega_7^0),\ \boldsymbol{C}_1 = \frac{1}{\sqrt{3}}(\omega_7^1, \omega_7^2, \omega_7^4),$$

$$\boldsymbol{C}_2=\frac{1}{\sqrt{3}}(\omega_7^2,\omega_7^4,\omega_7^1),\quad \boldsymbol{C}_3=\frac{1}{\sqrt{3}}(\omega_7^3,\omega_7^6,\omega_7^5),$$

$$\boldsymbol{C}_4=\frac{1}{\sqrt{3}}(\omega_7^4,\omega_7^1,\omega_7^2),\quad \boldsymbol{C}_5=\frac{1}{\sqrt{3}}(\omega_7^5,\omega_7^3,\omega_7^6),$$

$$\boldsymbol{C}_6=\frac{1}{\sqrt{3}}(\omega_7^6,\omega_7^5,\omega_7^3)$$

其中，$\omega_7=\mathrm{e}^{\frac{2\pi\sqrt{-1}}{7}}$。

4.2 基于几乎差集的最优码本

令 $p=ef+1$ 为素数，其中 e 和 f 是正整数。定义集合 $D_i^{(e,p)}=\left\{\alpha^j\mid\alpha\in\mathbb{F}_p^*, j=i \bmod e\right\}$ 为有限域 $\mathbb{F}_p$ 上的 e 阶分圆类。

引理 4[5] 令 $p=1(\bmod 4)$，则2阶分圆类 $D_0^{(2,p)}$ 是有限域 $\mathbb{F}_p$ 上的几乎差集，参数为 $\left(p,\frac{p-1}{2},\frac{p-5}{4},\frac{p-1}{2}\right)$-ADS。对于该几乎差集，$\Delta\neq 0$，有

$$\sum_{d_k\in D_0^{(2,p)}}\omega_p^{\Delta d_k}=\frac{-1\pm\sqrt{p}}{2} \tag{15}$$

根据引理 4，可以得到下面结论。

定理 3 令 $N=p$ 为素数，若集合 $D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$ 为有限域 $\mathbb{F}_p$ 上的几乎差集 $\left(p,\frac{p-1}{2},\frac{p-5}{4},\frac{p-1}{2}\right)$-ADS，即 $D=D_0^{(2,p)}$，则式(9)定义的码本参数为 $\left(p,\frac{p-1}{2}\right)$，码本的字符集大小为 $2p$，最大相关幅度值为 $I_{\max}(\boldsymbol{C}_{\boldsymbol{\phi}})=\frac{1+\sqrt{p}}{p-1}$。该码本渐进达到 Welch 界。

证明 根据构造过程可知向量数目 $N=p$，向量长度 $K=\frac{p-1}{2}$，计算其互相关幅度如下。由引理 4 可知，对于几乎差集 $D=D_0^{(2,p)}$，有 $\left|\sum_{d_k\in D_0^{(2,p)}}\omega_p^{\Delta d_k}\right|\leqslant\frac{1+\sqrt{p}}{2}$。又由定理 1 可得，码本最大相关幅度值为

$$I_{\max}(\boldsymbol{C}_{\boldsymbol{\phi}})=\frac{1+\sqrt{p}}{2}\frac{2}{p-1}=\frac{1+\sqrt{p}}{p-1} \tag{16}$$

根据引理 1 可知，对于 $\left(p,\frac{p-1}{2}\right)$ 码本，相关幅度值的 Welch 界为 $I_{\mathrm{Welch}}(\boldsymbol{C}_{\boldsymbol{\phi}})=\frac{\sqrt{p+1}}{p-1}$。则有

$$\lim_{p\to\infty}\left\{\frac{I_{\max}(\boldsymbol{C}_{\boldsymbol{\phi}})}{I_{\mathrm{Welch}}(\boldsymbol{C}_{\boldsymbol{\phi}})}\right\}=\lim_{p\to\infty}\left\{\frac{1+\frac{1}{\sqrt{p}}}{\sqrt{1+\frac{1}{p}}}\right\}=1 \tag{17}$$

可以看出，当 p 增大时，该码本渐进达到 Welch 界。

证毕。

4.3 基于特征和的最优码本

令 ξ_K 表示 K 维希尔伯特空间的标准正交基所构成的集合，即由下面 K 个长度为 K 的向量 $\boldsymbol{e}_i(1\leqslant i\leqslant K)$ 组成的集合为

$$\xi_K=\begin{Bmatrix}\boldsymbol{e}_1\\ \boldsymbol{e}_2\\ \vdots\\ \boldsymbol{e}_K\end{Bmatrix}=\begin{Bmatrix}1,0,0,\cdots,0,0\\ 0,1,0,\cdots,0,0\\ \vdots\ \vdots\ \vdots\ \ddots\ \vdots\ \vdots\\ 0,0,0,\cdots,0,1\end{Bmatrix}$$

其中，$\boldsymbol{e}_1=(1,0,\cdots,0)$，$\boldsymbol{e}_2=(0,1,\cdots,0),\cdots$，$\boldsymbol{e}_K=(0,0,\cdots,1)$。

设 $q=p^n$ 是素数的幂，其中 p 为素数。令 $a\in\mathbb{F}_q$，定义集合 $T_a=\left\{x\in\mathbb{F}_{q^s}^*\mid\mathrm{Tr}_{q^s/q}(x)=a\right\}$，有 $|T_a|=q^{s-1}$。有限域 $\mathbb{F}_{q^s}$ 上的艾森斯坦和（Eisenstein sum）定义为

$$E_1(\chi)=\sum_{x\in T_1}\chi(x) \tag{18}$$

定义 $E_a(\chi)=\sum_{x\in T_a}\chi(x)$，显然对于 $a\in\mathbb{F}_q^*$ 有 $E_a(\chi)=\chi(a)E_1(\chi)$。

引理 5[22] 令 χ 表示有限域 $\mathbb{F}_{q^s}$ 上的非平凡乘法特征，对于任意 $a\in\mathbb{F}_q^*$，有

$$|E_a(\chi)|\in\left\{q^{\frac{s-1}{2}},q^{\frac{s-2}{2}}\right\} \tag{19}$$

定理 4 令 $s=2$，$N=q^2-1$，a 是有限域 $\mathbb{F}_{q^2}$ 的本原元，$a\in\mathbb{F}_q^*$。选取集合 $D=\{d_0,d_1,d_2,\cdots,d_{K-1}\}$ 为

$$d_k=\log_a x,\quad x\in T_a=\left\{x\in\mathbb{F}_{q^s}^*\mid\mathrm{Tr}_{q^s/q}(x)=a\right\} \tag{20}$$

设 $\boldsymbol{C}_{\boldsymbol{\phi}}$ 表示式(9)定义的码本，则 $\boldsymbol{C}_{\boldsymbol{\phi}}\cup\xi_K$ 是 $\left(q^2+q-1,q\right)$ 码本，码本的字符集大小为 $2p+1$，其最大互相关幅度为 $I_{\max}(\boldsymbol{C}_{\boldsymbol{\phi}}\cup\xi_K)=\frac{1}{\sqrt{q}}$。

证明 由上述构造过程可知向量长度 $K=|T_a|=q^{s-1}=q$，向量数目为 $N=q^2+q-1$。其互相关幅度

值计算如下。

当 $\boldsymbol{C}_l,\boldsymbol{C}_t\in\xi_K$ 时，很容易得 $\left|\boldsymbol{C}_l\boldsymbol{C}_t^{\mathrm{H}}\right|=0$。

当 $\boldsymbol{C}_l\in\xi_K$，$\boldsymbol{C}_t\in\boldsymbol{C}_{\boldsymbol{\Phi}}$ 时，有 $\left|\boldsymbol{C}_l\boldsymbol{C}_t^{\mathrm{H}}\right|=\dfrac{1}{\sqrt{q}}$。

当 $\boldsymbol{C}_l,\boldsymbol{C}_t\in\boldsymbol{C}_{\boldsymbol{\Phi}}$ 时，根据定理 1 有

$$\left|\boldsymbol{C}_l\boldsymbol{C}_t^{\mathrm{H}}\right|=\frac{1}{K}\left|\sum_{d_k\in D}\omega_N^{\Delta d_k}\right|=\frac{1}{q}\left|\sum_{x\in T_a}\chi_{\Delta}(x)\right|=\frac{1}{q}\left|E_a(\chi_{\Delta})\right| \quad (21)$$

又根据引理 5，可得 $I_{\max}(\boldsymbol{C}_{\boldsymbol{\Phi}}\cup\xi_K)=\dfrac{\sqrt{q}}{q}=\dfrac{1}{\sqrt{q}}$，定理成立。

定理 5　码本 $\boldsymbol{C}_{\boldsymbol{\Phi}}\cup\xi_K$ 依照 Levenstein 界是渐进最优的。

证明　对于参数为 $\left(q^2+q-1,q\right)$ 的复数码本 $\boldsymbol{C}_{\boldsymbol{\Phi}}\cup\xi_K$，其中 $N>K^2$，根据引理 2 可得，最大互相关幅度值的 Levenstein 界为式(5)，即

$$I_L(\boldsymbol{C}_{\boldsymbol{\Phi}}\cup\xi_K)=\sqrt{\frac{2N-K^2-K}{(N-K)(K+1)}}=\sqrt{\frac{q^2-q-2}{q^3+q^2-q-1}} \quad (22)$$

进一步可得

$$\lim_{q\to\infty}\left\{\frac{I_{\max}(\boldsymbol{C}_{\boldsymbol{\Phi}}\cup\xi_K)}{I_L(\boldsymbol{C}_{\boldsymbol{\Phi}}\cup\xi_K)}\right\}=\lim_{q\to\infty}\sqrt{\frac{1+\dfrac{1}{q}-\dfrac{1}{q^2}-\dfrac{1}{q^3}}{1-\dfrac{1}{q}-\dfrac{2}{q^2}}}=1 \quad (23)$$

证毕。

5　最优码本构造方法的对比分析

对基于文献[18]的框架思想提出的几类最优码本构造方法进行比较，如表 1 所示。

由表 1 可以看出，根据文献[18]提出的码本构造框架，可以通过选取不同的变换矩阵和集合来构造不同参数的码本。已有的方法都是基于 IDFT 矩阵或 Hadamard 矩阵，利用不同的集合来构造码本。本文提出了一类新的变换矩阵，利用已有的差集、几乎差集和有限域上的艾森斯坦和定义的一个集合构造了参数最优和渐进最优的码本。定理 2 和定理 3 与已有的文献[4,18]和文献[5]中的最优码本具有相同的参数和最大相关幅度值，因此可以为通信系统或信息处理提供更多的选择。定理 4 构造出一类新的码本，依照 Levenstein 界渐进最优，相比较依照 Welch 界渐进最优的码本，最大互相关幅度值更小。虽然新变换矩阵放宽了限制条件使得字符集变大，但是在构造相同参数的码本时，变换矩阵在选取上具有了更强的灵活性。在构造压缩感知确定性测量矩阵等不要求字符集的应用中，本文构造的码本是更好的选择。

例 2　令 $p=67$，差集 $D=D_0^{(2,p)}$，构造一个参数为 $(67,33)$ 的码本，且最大相关幅值达到 Welch 界。令 $p=61$，几乎差集 $D=D_0^{(2,p)}$，构造一个参数为 $(61,30)$ 的码本且最大相关幅值渐近达到 Welch 界。通过文献[3]的方法分别将构造的码本应用于压缩感

表 1　　**几类最优码本的构造方法**

方法	码本参数	最大相关幅度值	最优性	矩阵 $\boldsymbol{\Phi}$	集合 D
文献[4,18]	(p,K)	$I_{\max}(\boldsymbol{C}_{\Phi})=\sqrt{\dfrac{p-K}{(p-1)K}}$	Welch 界最优	IDFT 矩阵	差集
文献[5]	$\left(p,\dfrac{p-1}{2}\right)$	$I_{\max}(\boldsymbol{C}_{\Phi})=\dfrac{1+\sqrt{p}}{p-1}$	Welch 界渐进最优	Hadamard 矩阵	几乎差集
文献[19]	$\left(q-1,\dfrac{q}{p^2}-1\right)$	$I_{\max}(\boldsymbol{C}_{\Phi})=\dfrac{(p^2-1)\sqrt{q}}{\sqrt{q}-p^2}$	Welch 界几乎最优	IDFT 矩阵	二元序列支撑集
文献[20]	$\left(q,\dfrac{p-1}{2p}(q+\sqrt{q})+1\right)$	$I_{\max}(\boldsymbol{C}_{\Phi})=\dfrac{1}{K}\dfrac{(p+1)\sqrt{q}}{2p}$	Welch 界几乎最优	Hadamard 矩阵	二元序列支撑集
定理 2	(p,K)	$I_{\max}(\boldsymbol{C}_{\Phi})=\sqrt{\dfrac{p-K}{(p-1)K}}$	Welch 界最优	Zadoff-Chu 矩阵	差集
定理 3	$\left(p,\dfrac{p-1}{2}\right)$	$I_{\max}(\boldsymbol{C}_{\Phi})=\dfrac{1+\sqrt{p}}{p-1}$	Welch 界渐进最优	Zadoff-Chu 矩阵	几乎差集
定理 4	(q^2+q-1,q)	$I_{\max}(\boldsymbol{C}_{\Phi}\cup\xi_K)=\dfrac{1}{\sqrt{q}}$	Levenstein 界渐进最优	Zadoff-Chu 矩阵	Eisenstein sum 定义的集合

注：p 为素数，$q=p^n$。

知中构造确定性测量矩阵。根据定理 2 得到的测量矩阵大小为 33×67，根据定理 3 得到的测量矩阵大小为 30×61，最大互相关幅值分别达到和渐近达到 Welch 界。由定理 2 构造出的码本与文献[4,18]中基于 IDFT 矩阵和差集构造出的码本具有相同的参数，因此将文献[4,18]中的码本也构造为确定性测量矩阵。再分别选择相同大小的随机离散傅里叶变换（DFT, discrete Fourier transform）矩阵和随机复高斯矩阵作为随机测量矩阵进行信号恢复和对比分析，得到的信号重建概率随稀疏度变化曲线如图 1 所示。

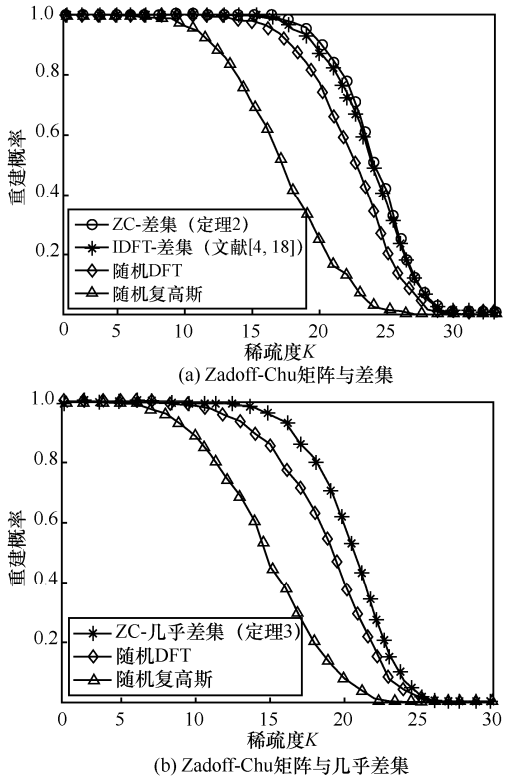

图 1 稀疏度随重建概率变化曲线

由图 1(a)可以看出，由本文定理 2 中的码本构造的确定性测量矩阵在相同稀疏度时，重建信号的概率明显高于随机 DFT 矩阵和随机复高斯矩阵。利用定理 2 构造出的确定性测量矩阵与利用文献[4,18]构造的测量矩阵具有相同的参数，在重建信号的概率上甚至略高于文献[4,18]中的方法。同理，利用本文定理 3 中的码本构造的确定性测量矩阵在重建信号的概率上明显高于随机测量矩阵。

6 结束语

基于文献[18]的码本构造思想，本文放松了变换矩阵的限制条件，提出了一类新的 Zadoff-Chu 矩阵，并利用差集、几乎差集和有限域上的特征和构造了 3 类码本，参数分别为 (p,K)、$\left(p,\frac{p-1}{2}\right)$ 和 (q^2+q-1,q)。本文构造的码本与已有码本的参数和最大互相关幅度值相同并且可以达到最优或渐进最优。本文方法可以为同步 CDMA 通信系统提供大量可用码本，并且可以通过文献[3]的方法将本文得到的码本应用于压缩感知领域中确定性测量矩阵的构造，得到的确定性测量矩阵在重构信号的概率上明显优于随机测量矩阵。

参考文献：

[1] DING C S, GOLIN M, KLØVE T. Meeting the Welch and Karystinos-Pados bounds on DS-CDMA binary signature sets[J]. Design Codes and Cryptography, 2003, 30(1): 73-84.

[2] 冯克勤, 金玲飞. 量子信息理论中的几个数学问题[J]. 中国科学: 数学, 2017, 47(11): 1387-1408.
FENG K Q, JIN L F. Several mathematical problems in quantum information theory[J]. Scientia Sinica (Mathematics), 2017, 47(11): 1387-1408.

[3] LI S X, GE G. Deterministic sensing matrices arising from near orthogonal systems[J]. IEEE Transactions on Information Theory, 2014, 64(4): 2291-2302.

[4] XIA P F, ZHOU S L, GIANNAKIS G B. Achieving the Welch bound with difference sets[J]. IEEE Transactions on Information Theory, 2005, 51(5): 1900-1907.

[5] DING C S. Complex codebooks from combinatorial designs[J]. IEEE Transactions on Information Theory, 2006, 52(9): 4229-4235.

[6] DING C S, FENG T. Codebooks from almost difference sets[J]. Design Codes and Cryptography, 2008(46): 113-126.

[7] 张爱仙，冯克勤. 一类近似最佳码本的构造[J]. 中国科学: 信息科学, 2015, 45(12): 1632-1639.
ZHANG A X, FENG K Q. Construction of a class of codebooks nearly meeting the Welch bound[J]. Scientia Sinica (Informations), 2015, 45(12): 1632-1639.

[8] LI C J, YUE Q, HUANG Y W. Two families of nearly optimal codebooks[J]. Design Codes and Cryptography, 2015, 75(1): 43-57.

[9] ZHANG A X, FENG K Q. Construction of cyclotomic codebooks nearly meeting the Welch bound[J]. Design Codes and Cryptography. 2012, 63(2): 209-224.

[10] 张爱仙, 何春燕, 吉喆. 几类近似达到 Welch 界码本的构造[J]. 纯粹数学与应用数学, 2018, 34(3): 323-330.
ZHANG A X, HE C Y, JI Z. Constructions of some classes of codebooks nearly meeting the Welch bound[J]. Pure and Applied Mathematics, 2018, 34(3): 323-330.

[11] ZHOU Z C, DING C S, LI N. New families of codebooks achieving the Levenstein bound[J]. IEEE Transactions on Information Theory, 2014, 60(11): 2507-2511.

[12] QU L J. A new approach to constructing quadratic pseudo-planar functions over F_2^n[J]. IEEE Transactions on Information Theory, 2016, 62(11): 6644-6658.

[13] HENG Z L, DING C S, YUE Q. New constructions of asymptotically optimal codebooks with multiplicative characters[J]. IEEE Transactions on Information Theory, 2017, 63(10): 6179-6187.

[14] HENG Z L. Nearly optimal codebooks based on generalized Jacobi sums[J]. Discrete Applied Mathematics, 2018(250): 227-240.

[15] LUO G J, CAO X W. Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum[J]. IEEE Transactions on Information Theory, 2018, 64(10): 6498-6505.

[16] LUO G J, CAO X W. Two constructions of asymptotically optimal codebooks[J]. Cryptography and Communications, 2018, 11(4): 825-838.

[17] XIANG C, DING C S, MESNAGER S. Optimal codebooks from binary codes meeting the Levenstein bound[J]. IEEE Transactions on Information Theory, 2015, 61(12):6526-6535.

[18] YU N Y. A construction of codebooks associated with binary sequences[J]. IEEE Transactions on Information Theory, 2012, 58(8): 5522-5533.

[19] CAO X W, CHOU W S, ZHANG X Y. More constructions of near optimal codebooks associated with binary sequences[J]. Advances in Mathematics of Communications, 2017, 11(1): 187-202.

[20] HONG S, PARK H, NO J. Near optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping [J]. IEEE Transactions on Information Theory, 2014, 60(6): 3698-3705.

[21] WANG X, ZHANG J, GE G. Deterministic convolutional compressed sensing matrices[J]. Finite Fields and Their Applications, 2016(42): 102-117.

[22] BERNDT B, EVANS R, WILLIAMS K. Gauss and Jacobi sums[M]. New York: Wiley, 1990.

[作者简介]

李玉博（1985– ），男，河北衡水人，博士，燕山大学副教授，主要研究方向为编码理论、序列设计、信息处理等。

刘胜毅（1994– ），男，河北沧州人，燕山大学硕士生，主要研究方向为编码理论、压缩感知。

张景景（1995– ），女，河北石家庄人，燕山大学硕士生，主要研究方向为编码理论、压缩感知。

贾冬艳（1983– ），女，河北衡水人，博士，河北科技师范学院讲师，主要研究方向为推荐系统、智能信息处理。