最优和渐近最优码本的新构造

高 有[1,2],谢明月[1],王 刚[1]
(1.中国民航大学理学院,天津 300300;2.天津市智能信号与图像处理重点实验室,天津 300300)

摘 要: 码本是一类具有较低相关性的信号集,满足Welch界或Levenshtein界的码本(又称信号集)主要用于码分多址(CDMA,code-division multiple-access)系统中不同用户信号的区分,也可用于压缩感知、编码理论和量子计算。本文提供了两类关于Levenshtein界的最优和渐近最优码本的新构造。首先,利用设计理论对象网和Hadamard矩阵构造了一类新的关于Levenshtein界的最优码本;其次,利用有限域上的置换函数构造了一类关于Levenshtein界的渐近最优码本。参数对比表明,这两类码本的构造参数和方法均为新成果。

关键词: 最优码本;渐近最优码本;Levenshtein界;设计理论对象网;置换函数;有限域
中图分类号: O157.4;TN911.2 **文献标志码:** A **文章编号:** 1674-5590(2026)01-0086-05

New constructions of optimal and asymptotically optimal codebooks

GAO You[1,2], *XIE Mingyue*[1], *WANG Gang*[1]
(1. *College of Science, CAUC, Tianjin* 300300, *China*; 2. *Tianjin Key Laboratory of Intelligent Signal and Image Processing, Tianjin* 300300, *China*)

Abstract: Codebooks are signal sets with low mutual correlation. Those codebooks meeting the Welch bound or the Levenshtein bound are mainly used to distinguish signals from different users in code-division multiple-access (CDMA) systems, and can also be applied in compressed sensing, coding theory, and quantum computing. This paper presents two new constructions of optimal and asymptotically optimal codebooks with respect to the Levenshtein bound. Firstly, a new class of optimal codebooks with respect to the Levenshtein bound is constructed using design-theoretic object nets and Hadamard matrices. Secondly, a new class of asymptotically optimal codebooks with respect to the Levenshtein bound is constructed using permutation functions over finite fields. Parameter comparisons demonstrate that the construction parameters and methods for these two classes of codebooks represent novel contributions.

Key words: optimal codebook; asymptotically optimal codebook; Levenshtein bound; design-theoretic object net; permutation function; finite field

码本是一类具有较低相关性的信号集,可以作为传递信息的载体,起到信息保密的作用,所以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,本文在现有研究基础上提出了两类新码本,丰富了码本的理论。

对于参数为(N,K)的码本$\boldsymbol{C}$来说,最大内积相关值$I_{\max}(\boldsymbol{C})$越小,码本的应用越广泛,所以如何得到$I_{\max}(\boldsymbol{C})$小的码本成为学者关注的重点。研究发现,码本参数受到理论界限约束,N和K之间需要满足一定的界,即Welch界[1]和Levenshtein界[2]。因此,构造参数达到理论界限的最优码本在实际应用中是非常有意义的,其中关于达到Welch界的最优码本的构造可参考文献[3-4]。

目前,国内外学者对于达到Levenshtein界的码本的研究已有很多优秀成果:Wootters等[5]和Xiang等[6]构造了参数为$(2^{2m-1}+2^m,2^m)$的最优码本;Ding等[7]和Han等[8]构造了参数为$(p^{2m}+p^m,p^m)$的最优码本;Zhou等[9]构造了参数为$(2^{2m-1}+2^m,2^m)$和$(p^{2m}+p^m,p^m)$的最

收稿日期:2023-10-11; **修回日期:**2024-04-19
基金项目:国家自然科学基金项目(11701558);天津市智能信号与图像处理重点实验室开放基金项目(230122011003)
作者简介:高有(1966—),男,内蒙古乌兰察布人,教授,博士,研究方向为代数、密码与编码.

优码本;Calderbank 等[10]和 Heng 等[11]构造了参数为$(2^{2m}+2^m,2^m)$的最优码本。

然而,最优码本的构造较困难,因此,多位学者开始尝试构造渐近达到 Levenshtein 界的码本,即 $I_{\max}(\boldsymbol{C})$稍微大于 Levenshtein 界,但当 N 足够大时可以几乎达到 Levenshtein 界。Xiang 等[6]构造了参数为$(2^{2m}+2^m,2^m)$的渐近最优码本;Tan 等[12]构造了参数为$(p^{2m}-1,p^m-1)$的渐近最优码本;Heng 等[13]构造了参数为$(p^{2m}-p^m-1,p^m-2)$的渐近最优码本;Tang 等[14]和 Heng[15]构造了参数为$(p^{2m}+p^m-1,p^m)$的渐近最优码本;Wang 等[16]构造了参数为(p^2+p,p)和$(p^{2m}+p^m-1,p^m)$的渐近最优码本;Han 等[8]构造了参数为$(p^{2m}+p^m,p^m-1)$和$(p^{2kmp}+p^{kmp},p^{kmp}-h)$的渐近最优码本。

1　基础知识

1.1　码本的相关概念及界

定义 1[1]　一个参数为(N,K)的码本 $\boldsymbol{C}$ 是由字符 A 上的 N 个单位复向量组成的集合$\{\boldsymbol{c}_0,\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{N-1}\}$,其中,$N$ 表示码本的数量,K 表示码本的长度,字符 A 的大小即为码本 $\boldsymbol{C}$ 的字符集大小,向量 $\boldsymbol{c}_j$ 称为码本的码字,$0\leqslant j\leqslant N-1$。

定义 2[1]　码本 $\boldsymbol{C}$ 的最大相关幅度定义为

$$I_{\max}(\boldsymbol{C})=\max_{0\leqslant j\neq j'\leqslant N-1}\left|\boldsymbol{c}_j\boldsymbol{c}_{j'}^{\mathrm{H}}\right|$$

式中,$\boldsymbol{c}_{j'}^{\mathrm{H}}$表示复数向量 $\boldsymbol{c}_{j'}$的共轭转置。

引理 1(Welch 界[1])对任意参数为(N,K)的码本 $\boldsymbol{C}$,且 $N\geqslant K$,有

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

当且仅当对任意的 $j\neq j'$都有 $\left|\boldsymbol{c}_j\boldsymbol{c}_{j'}^{\mathrm{H}}\right|=\sqrt{\frac{N-K}{(N-1)K}}$时,等号成立。为方便起见,记 $I_{\mathrm{W}}=\sqrt{\frac{N-K}{(N-1)K}}$。

引理 2(Levenshtein 界[2])对任意参数为(N,K)的实数码本 $\boldsymbol{C}$,且 $N>\frac{K(K+1)}{2}$,有

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

式中,I_{L} 为 Levenshtein 界。

对任意参数为(N,K)的复数码本 $\boldsymbol{C}$,且 $N>K^2$,有

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

1.2　设计理论对象网和 Hadamard 矩阵的相关知识

本节结合网的定义[17]和文献[18]中的定义 1,给出定义 3,并给出有关行向量 $\boldsymbol{h}\in\mathbb{C}^s$ 和二元向量 $\boldsymbol{m}$ 的相关内容。

定义 3　设 $\boldsymbol{m}=(m_1,m_2,\cdots,m_{s^2})$为长度为 s^2、模为 $\sqrt{ks}$ 的二元向量,其中 s 为偶数,k 为 s 的偶因子。记上述 $\frac{ts}{k}$个二元向量 $\boldsymbol{m}$ 组成的集合为

$$\boldsymbol{M}=\{\boldsymbol{m}_{11},\cdots,\boldsymbol{m}_{1\frac{s}{k}},\boldsymbol{m}_{21},\cdots,\boldsymbol{m}_{2\frac{s}{k}},\cdots,\boldsymbol{m}_{t1},\cdots,\boldsymbol{m}_{t\frac{s}{k}}\}$$

将 $\boldsymbol{M}$ 分成 t 块,则每块中有 $\frac{s}{k}$个二元向量。$\boldsymbol{m}_{bi}$ 表示在第 b 块中的第 i 个向量,其中,$b=1,2,\cdots,t$;$i=1,2,\cdots,\frac{s}{k}$。

如果上述二元向量 $\boldsymbol{m}$ 满足以下条件,则 $\boldsymbol{M}$ 可以构成一个$(t,\frac{s}{k};k)$-网:

(1)同一个块内的向量两两正交,即 $\boldsymbol{m}_{bi}^{\mathrm{T}}\boldsymbol{m}_{bi'}=0$,其中,$1\leqslant b\leqslant t$,$1\leqslant i\neq i'\leqslant\frac{s}{k}$;

(2)不同块中的任意两个向量满足 $\boldsymbol{m}_{bi}^{\mathrm{T}}\boldsymbol{m}_{b'i'}=k$,其中,$1\leqslant b\neq b'\leqslant t$,$1\leqslant i,i'\leqslant\frac{s}{k}$。

Hadamard 矩阵 $\boldsymbol{H}$ 是由 1 和–1 构成的,且满足 $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}=s\boldsymbol{I}_s$ 的 s 阶方阵,其中,$\boldsymbol{H}^{\mathrm{T}}$ 是 $\boldsymbol{H}$ 的转置,$\boldsymbol{I}_s$ 为 s 阶单位方阵。$\boldsymbol{H}$ 中任意两行(列)的内积是 0,同时 s 满足 $s=1$ 或 $s=2$ 或 $s\equiv0(\bmod 4)$。

定义 4[18]　令 $\boldsymbol{h}\in\mathbb{C}^s$ 为任意行向量,$\boldsymbol{m}'\in\{0,1\}^{s^2}$ 为任意长度为 s^2、模为$\sqrt{s}$ 的二元向量,定义 $\boldsymbol{h}\in\mathbb{C}^s$ 到 $\boldsymbol{m}'$的嵌入为 $\boldsymbol{h}\uparrow\boldsymbol{m}'=\sum_{r=1}^{s}h_r\boldsymbol{R}_r$,其中,$h_r$ 表示 $\boldsymbol{h}$ 的第 r 项,$\boldsymbol{R}_r$ 为 $\mathbb{C}^{s^2}$ 中第 r 位为 1,其余位置为 0 的向量,$\{\boldsymbol{R}_1,\boldsymbol{R}_2,\cdots,\boldsymbol{R}_s\}$为 $\boldsymbol{m}'$的基。具体定义向量的方法如下:$\boldsymbol{m}'$中的第 1个非零项被 $\boldsymbol{h}$ 中的第 1 项代替;$\boldsymbol{m}'$中的第 2 个非零项被 $\boldsymbol{h}$ 中的第 2 项代替,以此类推。

下面用一个简单的例子解释上述定义。

例 1　$\boldsymbol{m}'=(1,0,1,0,0,0,1,0,0)\in\{0,1\}^9$;

$\boldsymbol{h}=(1,-1,-1)\in\mathbb{C}^3$;

$\boldsymbol{h}\uparrow\boldsymbol{m}'=(1,0,-1,0,0,0,-1,0,0)\in\mathbb{C}^9$。

1.3　有限域及有限域上特殊函数的相关知识

本节回顾了关于有限域上特征和一些特殊函数的相关知识,同时给出了有限域上置换函数特征和的绝对值。

令 F_{p^n}为 p^n 元有限域,其中 p 为素数方幂,n 为正整数;令 $\mathrm{Tr}_1^n(x)$为 F_{p^n}到 F_p 的迹映射;记 $\zeta_p=\mathrm{e}^{\frac{2\pi i}{p}}$ 为 1

的复 p 次根；令$(\mathrm{F}_p,+)$的加法特征群为$\widehat{\mathrm{F}_{p^n}}=\{\chi_d:d\in\mathrm{F}_{p^n}\}$，其中，加法特征$\chi_d:\mathrm{F}_{p^n}\to\langle\zeta_p\rangle$定义为$\chi_d(x)=\zeta_p^{\mathrm{Tr}_1^n(dx)}$$(x\in\mathrm{F}_{p^n})$，$\chi_0=1$ 称为平凡加法特征。

取 F_{p^n}的一个本原元 γ，则 γ 是 F_{p^n}的乘法群 $\mathrm{F}_{p^n}^*=\mathrm{F}_{p^n}\backslash\{0\}=\langle\gamma\rangle$的一个生成元，记 F_{p^n}的乘法特征群为$\widehat{\mathrm{F}_{p^n}^*}=\{\psi^\omega:0\leqslant\omega\leqslant p^n-2\}$，其中，乘法特征 $\psi:\mathrm{F}_{p^n}^*\to\langle\zeta_{p^n-1}\rangle$定义为 $\psi(\gamma^\omega)=\zeta_{p^n-1}^\omega$，$(0\leqslant\omega\leqslant p^n-2)$，$\psi^0=1$ 称为平凡乘法特征。

令 G 和 H 为阿贝尔群，函数 $g:G\to H$，对任意 $a\in G$，定义差分算子 $\Delta_{g;a}(x)=g(x+a)-g(x)$。如果对于任意 $a\neq 1_G$，$\Delta_{g;a}$ 是均匀分布的，则称函数 g 为完全非线性函数。$|G|=|H|$ 且函数 g 是完全非线性函数，则 $\Delta_{g;a}$ 对任意 $a\neq 1_G$ 是一个置换函数。根据上述置换函数 $\Delta_{g;a}$，由文献[18]可以得到以下结论。

引理 3[19]　令 F_{p^n}为 p^n 元有限域，其中，p 为素数方幂，n 为正整数，$g(x)$为 F_{p^n}到 F_{p^n}的一个函数满足 $g(0)=0$，且对任意 $y\neq 1$，$g(xy)-g(x)$为 F_{p^n}上的一个置换函数。因此，对任意乘法特征 $\psi\in\widehat{\mathrm{F}_{p^n}^*}$，加法特征$\chi\in\widehat{\mathrm{F}_{p^n}}$，$d\in\mathrm{F}_{p^n}$，有

$$\left|\sum_{x\in\mathrm{F}_{p^n}^*}\psi(x)\chi(dg(x))\right|=\begin{cases}0 & \psi\neq\psi_0,d=0\\ 1 & \psi=\psi_0,d\neq 0\\ \sqrt{p^n} & \psi\neq\psi_0,d\neq 0\end{cases}$$

2　最优码本及渐近最优码本的构造

令 s 为偶数，k 为 s 的偶因子，对于 $b\geqslant\frac{s^2+2}{2}$可以得到一个$(b,\frac{s}{k};k)$–网，即

$$\boldsymbol{M}=\{\boldsymbol{m}_{11},\cdots,\boldsymbol{m}_{1\frac{s}{k}},\boldsymbol{m}_{21},\cdots,\boldsymbol{m}_{2\frac{s}{k}},\cdots,\boldsymbol{m}_{b1},\cdots,\boldsymbol{m}_{b\frac{s}{k}}\}。$$

如果 $b>\frac{s^2+2}{2}$，则任取其中 $\frac{s^2+2}{2}$ 块，得到 $\left(\frac{s^2+2}{2},\frac{s}{k};k\right)$–网，即

$$\boldsymbol{M}=\{\boldsymbol{m}_{11},\cdots,\boldsymbol{m}_{1\frac{s}{k}},\cdots,\boldsymbol{m}_{\frac{s^2+2}{2}1},\cdots,\boldsymbol{m}_{\frac{s^2+2}{2}\frac{s}{k}}\},$$

令 $\boldsymbol{h}_l$ 为 $ks\times ks$ Hadamard 矩阵的第 l 行，其中 $1\leqslant l\leqslant ks$.

定义二元向量 $\boldsymbol{c}_j$ 为

$$\boldsymbol{c}_j=\frac{1}{\sqrt{ks}}(\boldsymbol{h}_l\uparrow\boldsymbol{m}_{bi})\quad 1\leqslant j\leqslant\frac{s^4+2s^2}{2}\tag{1}$$

式中，$1\leqslant l\leqslant ks$，$1\leqslant b\leqslant\frac{s^2+2}{2}$，$1\leqslant i\leqslant\frac{s}{k}$。

定理 1　令 $\boldsymbol{C}_1=\left\{\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_{\frac{s^4+2s^2}{2}}\right\}$，其中，$\boldsymbol{c}_j$ 表达式为式(1)。$(N_1=\frac{s^4+2s^2}{2},K_1=s^2)$码本 $\boldsymbol{C}_1$ 是关于 Levenshtein 界的最优码本，且其字符集大小为 3，$I_{\max}(\boldsymbol{C}_1)=\frac{1}{s}$。

证明　所有二元向量 $\boldsymbol{h}_l\uparrow\boldsymbol{m}_{bi}$ 的模均为$\sqrt{ks}$，其中，$1\leqslant l\leqslant ks$，$1\leqslant b\leqslant\frac{s^2+2}{2}$，$1\leqslant i\leqslant\frac{s}{k}$，因此，$\boldsymbol{C}_1$ 中的向量都是标准化的。根据 $\boldsymbol{C}_1$ 的定义，$\boldsymbol{C}_1$ 中包含$\frac{s^4+2s^2}{2}$个长度为 s^2 的码字，因此，$N_1=\frac{s^4+2s^2}{2}$，$K_1=s^2$，字符集大小为 3。

令 $1\leqslant b=b'\leqslant\frac{s^2+2}{2}$，对于任意 $\boldsymbol{c}_1,\boldsymbol{c}_2\in\boldsymbol{C}_1$，其中

$$\boldsymbol{c}_1=\frac{1}{\sqrt{ks}}(\boldsymbol{h}_l\uparrow\boldsymbol{m}_{bi})$$

$$\boldsymbol{c}_2=\frac{1}{\sqrt{ks}}(\boldsymbol{h}_{l'}\uparrow\boldsymbol{m}_{bi'})$$

满足$(l,i)\neq(l',i')$。若 $i\neq i'$，由定义 3 可知，$\boldsymbol{m}_{bi}$ 和 $\boldsymbol{m}_{bi'}$是正交的，即 $\boldsymbol{m}_{bi}\boldsymbol{m}_{bi'}^{\mathrm{T}}=0$；如果 $i=i'$，$l\neq l'$，由 Hadamard 矩阵的正交性可知 $\boldsymbol{h}_l$ 和 $\boldsymbol{h}_{l'}$是正交的，即 $\boldsymbol{h}_l\boldsymbol{h}_{l'}^{\mathrm{T}}=0$。因此，根据定义 3 和定义 4，有$|\boldsymbol{c}_1\boldsymbol{c}_2^{\mathrm{H}}|=0$。

令 $1\leqslant b\neq b'\leqslant\frac{s^2+2}{2}$，对于任意 $1\leqslant i,i'\leqslant\frac{s}{k}$；$1\leqslant l,l'\leqslant ks$，有

$$\boldsymbol{c}_1=\frac{1}{\sqrt{ks}}(\boldsymbol{h}_l\uparrow\boldsymbol{m}_{bi})$$

$$\boldsymbol{c}_2=\frac{1}{\sqrt{ks}}(\boldsymbol{h}_{l'}\uparrow\boldsymbol{m}_{b'i'})$$

由定义 3 可知，$|\boldsymbol{c}_1\boldsymbol{c}_2^{\mathrm{H}}|\leqslant\frac{1}{s}$。令 Hadamard 矩阵的第一行为 $\boldsymbol{h}_l$，且满足 $\boldsymbol{h}_l=\boldsymbol{h}_{l'}$，则有$|\boldsymbol{c}_1\boldsymbol{c}_2^{\mathrm{H}}|=\frac{1}{s}$，$I_{\max}(\boldsymbol{C}_1)=\frac{1}{s}$。

$\boldsymbol{C}_1$ 为实值码本，且 $N_1>\frac{K_1(K_1+1)}{2}$，令 $K_1=s^2$，$N_1=\frac{s^4+2s^2}{2}$，得到 $\boldsymbol{C}_1$ 的 Levenshtein 界为$\frac{1}{s}$。因此，$(N_1=\frac{s^4+2s^2}{2},K_1=s^2)$码本 $\boldsymbol{C}_1$ 是关于 Levenshtein 界的最优码本。

关于寻找满足条件的$\left(\frac{s^2+2}{2},\frac{s}{k};k\right)$–网的问题，可以参考文献[17]，利用网、横向设计、正交拉丁方

块和正交阵列的等价性来解决。本文利用正交阵列和网的等价性来解决$\left(\frac{s^2+2}{2},\frac{s}{k};k\right)$–网的存在性问题。根据文献[17]可以得到以下等价结论:一个正交阵列 $\boldsymbol{OA}_k\left(\frac{s}{k},\frac{s^2+2}{2}\right)$等价于一个$\left(\frac{s^2+2}{2},\frac{s}{k};k\right)$–网(对偶结构)。因此,可以查看文献[17]中的表 4.19 和表 4.20 来确定$\left(\frac{s^2+2}{2},\frac{s}{k};k\right)$–网。

例 2　令 $s=2,k=1$,给出$(3,2;1)$–网 $\boldsymbol{M}$:

$\boldsymbol{M}=\{\boldsymbol{m}_{11},\boldsymbol{m}_{12},\boldsymbol{m}_{21},\boldsymbol{m}_{22},\boldsymbol{m}_{31},\boldsymbol{m}_{32}\}$,

$\boldsymbol{m}_{11}=(1,1,0,0),\boldsymbol{m}_{12}=(0,0,1,1)$;

$\boldsymbol{m}_{21}=(1,0,1,0),\boldsymbol{m}_{22}=(0,1,0,1)$;

$\boldsymbol{m}_{31}=(1,0,0,1),\boldsymbol{m}_{32}=(0,1,1,0)$。

下面将$(3,2;1)$–网 $\boldsymbol{M}$ 和 Hadamard 矩阵 $\boldsymbol{H}=\begin{bmatrix}1&1\\1&-1\end{bmatrix}$应用到上述构造中,得到$(N_1=12,K_1=4)$码本 $\boldsymbol{C}_1$ 的字符集大小为 3,$I_{\max}(\boldsymbol{C}_1)=\frac{1}{2}$,其中

$$\boldsymbol{C}_1=\left\{\frac{1}{\sqrt{2}}(1,1,0,0),\frac{1}{\sqrt{2}}(0,0,1,1),\frac{1}{\sqrt{2}}(1,-1,0,0),\frac{1}{\sqrt{2}}(0,0,1,-1),\frac{1}{\sqrt{2}}(1,0,1,0),\frac{1}{\sqrt{2}}(0,1,0,1),\frac{1}{\sqrt{2}}(1,0,-1,0),\frac{1}{\sqrt{2}}(0,1,0,-1),\frac{1}{\sqrt{2}}(1,0,0,1),\frac{1}{\sqrt{2}}(0,1,1,0),\frac{1}{\sqrt{2}}(1,0,0,-1),\frac{1}{\sqrt{2}}(0,1,-1,0)\right\}$$

显然 $\boldsymbol{C}_1$ 是一个实值码本,且 $N_1>\frac{K_1(K_1+1)}{2}$,令 $N_1=12,K_1=4$,则 $\boldsymbol{C}_1$ 的 Levenshtein 界为$\frac{1}{2}$。因此,上述码本是一个关于 Levenshtein 界的最优码本。

令 p 为素数方幂,n 为正整数,$\xi_1,\xi_2,\cdots,\xi_{p^n-1}$ 表示 $\mathrm{F}_{p^n}^*$ 中所有元素,记 $\boldsymbol{E}_{p^n-1}$ 为(p^n-1)维希尔伯特空间中标准正交基集合,即

$$\boldsymbol{E}_{p^n-1}=\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_{p^n-1}\}$$

$$\boldsymbol{e}_1=(1,0,0,\cdots,0,0)$$

$$\boldsymbol{e}_2=(0,1,0,\cdots,0,0)$$

$$\vdots$$

$$\boldsymbol{e}_{p^n-1}=(0,0,0,\cdots,0,1)$$

令 $g(x)$为 F_{p^n} 到 F_{p^n} 的一个映射,满足 $g(0)=0$,且对任意 $y\neq1$,有 $g(xy)-g(x)$为 F_{p^n} 上的一个置换函数。对任意固定的非平凡加法特征 $\chi\in\widehat{\mathrm{F}_{p^n}}$,定义 $\boldsymbol{c}_{\psi,d}$ 为

$$\boldsymbol{c}_{\psi,d}=\frac{1}{\sqrt{p^n-1}}(\psi(\xi_1)\chi(dg(\xi_1)),\psi(\xi_2)\chi(dg(\xi_2)),\cdots,\psi(\xi_{p^n-1})\chi(dg(\xi_{p^n-1})))\tag{2}$$

式中:$\psi\in\widehat{\mathrm{F}_{p^n}^*}$;$d\in\mathrm{F}_{p^n}$。

定理 2　令 $\boldsymbol{C}_2=\bigcup_{\psi\in\widehat{\mathrm{F}_{p^n}^*},d\in\mathrm{F}_{p^n}^*}\boldsymbol{c}_{\psi,d}\cup\boldsymbol{E}_{p^n}$,其中,$\boldsymbol{c}_{\psi,d}$ 的表达式为式(2)。参数为$(N_2=p^{2n}-p^n,K_2=p^n-1)$的码本 $\boldsymbol{C}_2$ 是关于 Levenshtein 界的渐近最优码本,且字符集大小为 $p+2$,$I_{\max}(\boldsymbol{C}_2)=\frac{\sqrt{p^n}}{p^n-1}$。

证明　$\boldsymbol{C}_2$ 中每个码字均是标准化的,根据 $\boldsymbol{C}_2$ 定义可知,$\boldsymbol{C}_2$ 包含了 $p^{2n}-p^n$ 个长度为 p^n-1 的码字,所以 $N_2=p^{2n}-p^n,K_2=p^n-1$,字符集大小为 $p+2$。

任取两个不同的向量 $\boldsymbol{c}_{\psi_1,d_1},\boldsymbol{c}_{\psi_2,d_2}\in\boldsymbol{C}_2$,其中 $\psi_1,\psi_2\in\widehat{\mathrm{F}_{p^n}^*}$,$d_1,d_2\in\mathrm{F}_{p^n}^*$,由引理 2 可知

$$\left|\boldsymbol{c}_{\psi_1,d_1}\boldsymbol{c}_{\psi_2,d_2}^{\mathrm{H}}\right|=\frac{1}{p^n-1}\left|\sum_{f=1}^{p^n-1}\psi_1\overline{\psi}_2(\xi_f)\chi((d_1-d_2)g(\xi_f))\right|=\begin{cases}\frac{\sqrt{p^n}}{p^n-1} & \psi_1\neq\psi_2,d_1\neq d_2\\ 0 & \psi_1\neq\psi_2,d_1=d_2\\ \frac{1}{p^n-1} & \psi_1=\psi_2,d_1\neq d_2\end{cases}$$

式中,$\overline{\psi}_2$ 表示 ψ_2 的共轭。

对任意的(ψ,d)和 f 有

$$\left|\boldsymbol{c}_{\psi,d}\boldsymbol{e}_f^{\mathrm{H}}\right|=\frac{1}{\sqrt{p^n-1}}$$

式中:$\psi\in\widehat{\mathrm{F}_{p^n}^*}$;$d\in\mathrm{F}_{p^n}^*$;$1\leqslant f\leqslant p^n-1$。

对于任意 $1\leqslant f_1\neq f_2\leqslant p^n-1$,有 $\left|\boldsymbol{e}_{f_1}\boldsymbol{e}_{f_2}^{\mathrm{H}}\right|=0$,则 $I_{\max}(\boldsymbol{C}_2)=\frac{\sqrt{p^n}}{p^n-1}$。

$\boldsymbol{C}_2$ 显然为一个复数码本,且 $N_2>K_2^2$,则 $\boldsymbol{C}_2$ 对应的 Levenshtein 界为

$$I_{\mathrm{L}}=\sqrt{\frac{2N_2-K_2^2-K_2}{(K_2+1)(N_2-K_2)}}=\frac{1}{\sqrt{p^n-1}}$$

显然有

$$\lim_{p\to\infty}\frac{I_{\mathrm{L}}}{I_{\max}(\boldsymbol{C}_2)}=\lim_{p\to\infty}\sqrt{\frac{p^n-1}{p^n}}=1$$

因此，$\boldsymbol{C}_2$ 是关于 Levenshtein 界的渐近最优码本。

注释 1　图 1 给出了随着 K_2 的增大，$I_{\max}(\boldsymbol{C}_2)$和 I_{L} 的吻合情况。记满足引理 3 条件的集合为 G，即集合中的函数均满足 $g(0)=0$，且对于任意 $y\neq 1$，有 $g(xy)-g(x)$为 F_{p^n}上的一个置换函数，针对 G 的存在性问题，有以下已知结果：

(1)$g(x)=ax^u\in G, a\neq 0, \gcd(u, p^n-1)=1$；

(2)$L(x)=\sum_{v=0}^{n-1} a_v x^{p^v}\in \mathrm{F}_{p^n}[x]$，$L(x)$为 F_{p^n}上的置换多项式，则 $L(x)\in G$；

(3)$\phi(x)\in G$ 且 $g(x)=ax^u$，其中 $a\neq 0, \gcd(d, p^n-1)=1$，则$(\phi\circ g)(x)=\phi(g(x))\in G$；

(4)$L(x)=\sum_{v=0}^{n-1} a_v x^{p^v}\in \mathrm{F}_{p^n}[x]$，$L(x)$为 F_{p^n}上的置换多项式，则 $L(\phi(x))\in G$。

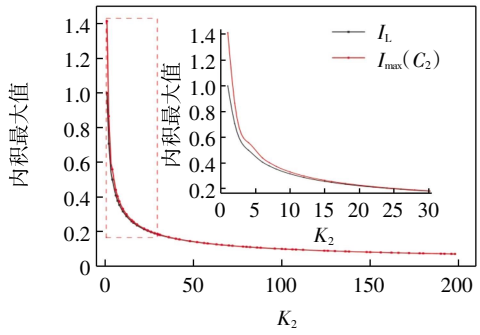

图 1　定理 2 中 $I_{\max}(\boldsymbol{C}_2)$和 I_{L} 的吻合情况

Fig. 1　The matching behavior between $I_{\max}(\boldsymbol{C}_2)$ and I_{L} in theorem 2

3　结语

本文给出了关于 Levenshtein 界的最优码本和渐近最优码本的新构造。首先，利用设计理论对象网和 Hadamard 矩阵构造了最优码本；然后，利用有限域上的置换函数构造了一类关于 Levenshtein 界的渐近最优码本。根据与已有最优码本和渐近最优码本的参数对比可知，本文中两类码本的构造参数和方法均为新成果。

参考文献：

[1] WELCH L. Lower bounds on the maximum cross correlation of signals (Corresp.)[J]. IEEE Transactions on Information Theory, 1974, 20(3): 397–399.

[2] KABATIANSKY G A , LEVENSHTEIN V I. On bounds for packing on a sphere and in space[J]. Problems of Information Transmission, 1978, 14: 1–17.

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

[4] DING C S, FENG T. A generic construction of complex codebooks meeting the Welch bound[J]. IEEE Transactions on Information Theory, 2007, 53(11): 4245–4250.

[5] WOOTTERS W K, FIELDS B D. Optimal state–determination by mutually unbiased measurements[J]. Annals of Physics, 1989, 191(2): 363–381.

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

[7] DING C S, YIN J X. Signal sets from functions with optimum nonlinearity[J]. IEEE Transactions on Communications, 2007, 55(5): 936–940.

[8] HAN L, SUN S M, YAN Y, et al. A new construction of codebooks meeting the Levenshtein bound[J]. IEEE Access, 2020, 8: 77598–77603.

[9] 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): 7382–7387.

[10] CALDERBANK A R, CAMERON P J, KANTOR W M, et al. Z4–kerdock codes, orthogonal spreads, and extremal Euclidean line–sets[J]. Proceedings of the London Mathematical Society, 1997, 75(2): 436–480.

[11] HENG Z L, YUE Q. Optimal codebooks achieving the Levenshtein bound from generalized bent functions over Z4[J]. Cryptography and Communications, 2017, 9(1): 41–53.

[12] TAN P, ZHOU Z C, ZHANG D. A construction of codebooks nearly achieving the Levenstein bound[J]. IEEE Signal Processing Letters, 2016, 23(10): 1306–1309.

[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] TANG X H, ZHOU Z C. New nearly optimal codebooks from relative difference sets[J]. Advances in Mathematics of Communications, 2011, 5(3): 521–527.

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

[16] WANG G, XU D M, FU F W. Constructions of asymptotically optimal codebooks with respect to Welch bound and Levenshtein bound[J]. Advances in Mathematics of Communications, 2023, 17(6): 1526–1541.

[17] COLBOURN CH J. The CRC handbook of combinatorial designs[M]. Boca Raton: CRC Press, 1996.

[18] WOCJAN P, BETH T. New construction of mutually unbiased bases in square dimensions[J]. Quantum Information and Computation, 2005, 5(2): 93–101.

[19] CAO X W, MI J F, XU S D. Two constructions of approximately symmetric informationally complete positive operator–valued measures[J]. Journal of Mathematical Physics, 2017, 58(6): 062201.

（责任编辑：明　月）