中国科学 : 数学　2021 年　第 51 卷　第 1 期 : 225 ∼ 238
SCIENTIA SINICA Mathematica
论　文

达到渐近 GV 界的一种线性映射族构造方法 —生成 Shannon 好码渐近序列的新进展

献给张景中、杨路教授 85 华诞

王晓京[1,2], 彭行一[1,2*]

1. 中国科学院成都计算机应用研究所, 成都 610041;
2. 中国科学院大学计算机科学与技术学院, 北京 100049
E-mail: wxjgxlwmd@sina.com, pengxingyi15@mails.ucas.ac.cn

收稿日期: 2019-12-25; 接受日期: 2020-11-27; 网络出版日期: 2020-12-28; * 通信作者

摘要　给定有限域 $\mathbb{F}_q$ ($q \geqslant 2$)、任意正整数 n 和 k ($n > k$), $\mathbb{F}_q$ 上的线性映射序列 (代数族) $\{\boldsymbol{\sigma}_i\}$ ($\boldsymbol{\sigma}_i : \mathbb{F}_q^k \to \mathbb{F}_q^n$ ($i \to \infty$)) 的构造方法已经成为信息科学中编码理论的一个中心问题, 一般称为实现 Shannon 理想的代数族途径. 迄今为止, 发现这种代数族 $\{\boldsymbol{\sigma}_i\}$ 的更好结构, 并由它导出 Shannon 好码渐近序列 $\{[n_i, k_i, d_i]\}$ 仍是一个尚未彻底解决的挑战性难题和持续不断的努力目标. 衡量这种代数族的好坏, 除了看 $\{\boldsymbol{\sigma}_i\}$ 的构造是否有利于通信工程实现 (构造简明, 执行复杂度低) 之外, 最重要的一个基本标准是看 $\{\boldsymbol{\sigma}_i\}$ 导出的序列 $\{[n_i, k_i, d_i]\}$ 诸参数的渐近极限结果是否不至于衰减到渐近 Gilbert-Varshamov (GV) 界之下, 该问题吸引了许多数学工作者的关注. 本文从矩阵映射的观点给出一种生成任意有限域 $\mathbb{F}_q$ 上代数族 $\{\boldsymbol{\sigma}_i\}$ 的新方法, 并表明由 $\{\boldsymbol{\sigma}_i\}$ 导出的渐近码序列 $\{[n_i, k_i, d_i]\}$ 可达渐近 GV 界之上. 这种新的代数族生成途径对于信息编码理论及其工程应用都具有很重要的意义.

关键词　线性映射族　代数构造　渐近 Gilbert-Varshamov 界

MSC (2010) 主题分类　11T71, 94A24

1　引言

设 $\mathbb{F}_q$ 是有限域 (素数幂 $q \geqslant 2$), 任意给定正整数 n 和 k ($n > k$), 考察线性映射 (单射)

$$\boldsymbol{\sigma} : \mathbb{F}_q^k \to \mathbb{F}_q^n,$$

它将 $\mathbb{F}_q^k$ 中全体向量映射到 $\mathbb{F}_q^n$ 的 k 维子空间 Ω (用信息论的语言, 也即将信息空间中向量映射到码矢空间), $\boldsymbol{\sigma}$ 在信息编码理论中也称为一个代数构造. 特别地, $\boldsymbol{\sigma}$ 可以是 $\mathbb{F}_q$ 上的一个 n 行 k 列的列满

英文引用格式: Wang X J, Peng X Y. A method of constructing linear mapping families to achieve the asymptotic GV bound (in Chinese). Sci Sin Math, 2021, 51: 225–238, doi: 10.1360/SSM-2019-0321

© 2020《中国科学》杂志社

秩矩阵 $\boldsymbol{G}_{n\times k}$ (也称为一个生成矩阵), 于是对任意向量 $\boldsymbol{\alpha}\in\mathbb{F}_q^k$ (本文一般指列向量), 通过映射 $\boldsymbol{\sigma}$, 有

$$\boldsymbol{\sigma}:\mathbb{F}_q^k\to\mathbb{F}_q^n,\quad \boldsymbol{\alpha}\mapsto\boldsymbol{\beta}=\boldsymbol{G}_{n\times k}\cdot\boldsymbol{\alpha}. \tag{1.1}$$

而 $\boldsymbol{\beta}$ 向量的全体构成 $\mathbb{F}_q^n$ 的 k 维子空间 Ω, Ω 的距离指标 d 则指 Ω 中任意两个向量间 Hamming 距离的最小值 (也即 Ω 中非零向量的最小 Hamming 重量, 它是一个正整数). 本文也用 $[n,k,d]$ 表示 Ω, 以指明它是 n 维向量空间的一个距离指标为 d 的 k 维子空间. 用 $\Omega:=[n,k,d]$ 表明它也是一个码矢线性空间 1). 信息编码理论中已证明, 3 个参数 n、k 和 d 之间恒有如下关系 [1]:

$$k+d\leqslant n+1. \tag{1.2}$$

编码理论的一个中心问题是, 在任意给定的信息符号有限域 (特别是尽可能小的有限域, 亦即尽可能细粒度的符号集) $\mathbb{F}_q$ 上如何实现下述目标: 对任意给定的正整数 n 和 k ($n>k$), 找到上述线性映射 $\boldsymbol{\sigma}$ (或生成矩阵 $\boldsymbol{G}_{n\times k}$) 使得 $\Omega:=[n,k,d]$ 的距离指标 d 尽可能大; 或者, 对任意给定的正整数 n 和 d ($n>d$), 找到上述线性映射 $\boldsymbol{\sigma}$ 使得 $\Omega:=[n,k,d]$ 的势 $|\Omega|=q^k$ 尽可能大. 其中 3 个参数 n、k 和 d 自然受限于不等式 (1.2), 也即有约束关系

$$\frac{k}{n}+\frac{d}{n}\leqslant 1+\frac{1}{n}, \tag{1.3}$$

故两个比值 k/n 与 d/n 总是此长彼消的. 对于 $\mathbb{F}_q$ 上一族线性映射序列 $\{\boldsymbol{\sigma}_i\}$ 及其参数分别为 n_i、k_i 和 d_i 的象空间序列 (码矢空间序列) $\{\Omega_i\}$ ($i\to\infty$), 记渐近参数

$$\delta=\lim_{i\to\infty}\frac{d_i}{n_i},\quad R=\lim_{i\to\infty}\frac{k_i}{n_i}.$$

如果能同时保持这两个参数不衰减到 0, 即在渐近情形下有 $\delta>0$ 且 $R>0$, 则称 $\{\boldsymbol{\sigma}_i\}$ 是实现 Shannon 理想的一个代数族, 称其象空间序列

$$\{\Omega_i\}:=\{[n_i,k_i,d_i]\}\quad(i\to\infty)$$

是一个 Shannon 好码渐近序列 [2]. 事实上, 迄今已知码类的编码方法大多数都不能导出 Shannon 好码渐近序列 (不能保持 δ 与 R 不同时衰减到 0), 能实现 Shannon 理想的编码方法仍是少数. 目前, 在细粒度的信息符号集所构成的有限域 $\mathbb{F}_q$ ($q<46$) 上, 特别是在最小的信息符号有限域 $\mathbb{F}_2$ 上, 对于任意编码尺度 n 和 k ($n>k$), 寻求更好的代数族 $\{\boldsymbol{\sigma}_i\}$ 来获得参数更佳的 Shannon 好码渐近序列 $\{[n_i,k_i,d_i]\}$ 仍然是一个有吸引力的基本挑战问题 (参见文献 [3]). 进一步, 让这些代数族 $\{\boldsymbol{\sigma}_i\}$ 都具有明确的生成矩阵形式 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$ (即可构造性地实现 $\{\boldsymbol{\sigma}_i\}$), 也是信息编码理论中一个未解决的非平凡问题 (参见文献 [4]).

两个参数 δ 和 R 在理论上可能达到的相对最好上界已有诸多结论 (参见文献 [4]), 在此不一一列举. 然而实际可达的相对最好的 δ 和 R 并不清楚. 于是寻求相对情形下 δ 和 R 尽可能好的 Shannon 好码渐近序列 $\{[n_i,k_i,d_i]\}$ 及其代数族 $\{\boldsymbol{\sigma}_i\}$ 方法成为了不断持续的热点工作, 而两个参数 δ 和 R 的可达下界往往是由实际构造的代数族 (一类编码方法) $\{\boldsymbol{\sigma}_i\}$ 具体给出的. 已知的最著名下界是渐近 GV

1) 在信息理论中, $\Omega:=[n,k,d]$ 通常称为一种线性编码, n 指明码矢长度, k 指明码矢空间 Ω 的维数 (即向量空间 $\mathbb{F}_q^k$ 的维数). k/n 越大意味着编码后传输的信息率越高, 而 d/n 越大则意味着编码传输的信息容错能力 (纠错分辨能力) 越强. 由此, 上述线性映射 $\boldsymbol{\sigma}$ 被视为一种编码方法. 特别地, $\boldsymbol{\sigma}$ 可以是一个生成矩阵 $\boldsymbol{G}_{n\times k}$.

界[5,6], 即对于任意 $0<\delta\leqslant(q-1)/q$, 一定存在 $\mathbb{F}_q$ 上某种代数族 $\{\boldsymbol{\sigma}_i\}$ 可导出线性码序列 $\{[n_i,k_i,d_i]\}$ (或 $\{\Omega_i\}$) $(i\to\infty)$, 使得其渐近参数 R 位于渐近 GV 界曲线

$$R_{\mathrm{GV}}(\delta)=1-H_q(\delta) \tag{1.4}$$

上方, 其中

$$H_q(x):=x\log_q(q-1)-x\log_q x-(1-x)\log_q(1-x)$$

是 q 元信息熵函数.

因此, 找到能达到渐近 GV 界的代数族 (一类编码方法) $\{\boldsymbol{\sigma}_i\}$ 成为了一个基本目标. 然而, 渐近 GV 界却并未提供生成 $\{\boldsymbol{\sigma}_i\}$ 的实际有效办法. 事实上, 要找到实际有效且又能达到渐近 GV 界的具体渐近序列 $\{[n_i,k_i,d_i]\}$ 及其代数族 $\{\boldsymbol{\sigma}_i\}$ 构造方法是颇为不易的, 长期以来进展较为缓慢. 尤其是在更小的信息符号域 $\mathbb{F}_q$ $(q<46)$ 上, 对于任意给定的码长 n 和信息率 k/n (或一定区间内的相对距离 d/n), 是否都能够找到这样的线性映射 $\boldsymbol{\sigma}$, 使得其象空间 $\Omega:=[n,k,d]$ 的参数都能在渐近 GV 界曲线之上? 这成为了 Shannon 好码渐近序列研究的聚焦点, 也是信息编码理论的一大挑战 (参见文献 [4]). 以上问题在文献中也称 "渐近问题"[2].

在寻求 Shannon 理想的代数族 (Shannon 好码渐近序列) 的进程中, Justesen[7] 于 1972 年用级联映射的思想首次给出了一类 Shannon 好码渐近序列 $\{\Omega_i\}$ $(i\to\infty)$ 的构造实例, 具有里程碑的意义. 不过这种序列距离渐近 GV 界还有一定距离. 其后, Goppa 引入的代数几何方法成为 "渐近问题" 最引人注目的研究途径, 称为代数几何码 (AG (algebraic geometry) 码)[8–10], 被寄予了厚望.

约 1980 年前后, Goppa 在一条亏格为 g 的光滑射影曲线 $\mathcal{X}$ 上选择了 n 个不同的有理点 $P_1,P_2,\ldots,P_n$, 记除子

$$D=P_1+P_2+\cdots+P_n,$$

并选择除子 G 满足 $\deg(G)<n$ 且 G 在 $P_1,P_2,\ldots,P_n$ 点的系数均为 0 (即与除子 D 支座不相交), 可获得线性赋值映射

$$ev_D:\mathscr{L}(G)\to\mathbb{F}_q^n,\quad f\mapsto(f(P_1),f(P_2),\ldots,f(P_n)), \tag{1.5}$$

其中

$$\mathscr{L}(G):=\{f\in\mathbb{F}_q[X]\backslash\{0\}\mid(f)+G\geqslant 0\}\cup\{0\}$$

是除子 G 的 Riemann-Roch 空间, 它是 $\mathbb{F}_q$ 上的有限维向量空间, 映射 (1.5) 的象为码矢空间

$$\Omega:=[n,k,d].$$

而 $\deg(G)<n$ 保证了该映射为单射, 由 Riemann-Roch 定理可得

$$k\geqslant\deg(G)-g+1$$

2) 在 "渐近问题" 中, 显然, 符号有限域 $\mathbb{F}_q$ 越大, 则能使用的代数工具及其技巧越多, 问题越容易解决; 而 $\mathbb{F}_q$ 越小, 则在通信工程中的实现复杂度和技术成本越低, 但解决上述问题的难度就更大. 因此, 在尽可能小的符号域 $\mathbb{F}_q$ 上解决 "渐近问题" 成为了自 20 世纪 50 年代初 Shannon 创立信息理论以来的一个亟待解决的严峻问题 (参见文献 [2]) 和持续不断的努力目标. 特别是要想在 Shannon 最关注的二元域 $\mathbb{F}_2$ 上构造一族达到渐近 GV 界的线性码族 $\{[n_i,k_i,d_i]\}$ 异常困难, 已知的代数构造凤毛麟角. 在此基础上能够进一步明确给出 $\{\Omega_i\}$ 的生成矩阵形式的代数族 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$ 更加不易. 此外, 对于任给的码长 n (而非仅仅特殊整数类) 与任意信息率 k/n (而非仅仅个别信息率) 均能使 δ 至少达到渐近 GV 界的线性码构造也是一个待解的难题.

(其中等号在 $\deg(G) > 2g-2$ 时取得), $d \geqslant n - \deg(G)$, 故

$$k + d \geqslant n + 1 - g.$$

以上参数称为 AG 码的设计参数, 注意到 Goppa 的构造中并没有给出明确的生成矩阵结构, 还需具体给出特定的曲线并选择恰当的除子, 才能通过构造向量空间 $\mathscr{L}(G)$ 的具体基底确定生成矩阵.

显然, 这种 $\mathbb{F}_q$ 上 AG 码 $[n,k,d]$ 的设计参数取值必然受到曲线上有理点个数与曲线亏格大小的比例的限制. 于是对于给定的亏格 g, 找到有理点个数尽可能多的曲线族成为构造 AG 码的主要任务. 后继者先后找到了 Unitary 曲线 (Hermite 曲线)、Suzuki 曲线和 Ree 曲线等曲线族 (参见文献 [11,12]), 它们对于特定的亏格都有最多数量的有理点. 但是这些特定的曲线族往往只能在某些特定的有限域 $\mathbb{F}_q$ 上才能构造出 AG 码, 其码参数 $[n,k,d]$ 也比较特殊 (参见文献 [12–14]).

更一般地, 记 $N_q(g)$ 为 $\mathbb{F}_q$ 上亏格为 g 的曲线上有理点个数,

$$A(q) := \lim_{g\to\infty} \sup \frac{N_q(g)}{g}, \tag{1.6}$$

且素数幂 q ($q \geqslant 2$) 恒满足 [15]

$$A(q) \leqslant \sqrt{q} - 1.$$

因为当 q 是平方数时, 能够有结论 [16]

$$A(q) \geqslant \sqrt{q} - 1,$$

故依靠 Goppa 的巧妙构造和模曲线理论, 在 $q \geqslant 49$ 且为平方数条件下, 渐近 GV 界于 1982 年被 Tsfasman 等 [17] 刷新: 当平方数 $q \geqslant 49$ 时, $\mathbb{F}_q$ 上的 Shannon 好码渐近序列可以达到 Tsfasman-Vlăduţ-Zink (TVZ) 界曲线

$$R_{\mathrm{TVZ}}(\delta) = 1 - A(q)^{-1} - \delta = 1 - (\sqrt{q}-1)^{-1} - \delta \tag{1.7}$$

之上, 其中当 δ 在一个非空开区间上时, TVZ 界曲线优于渐近 GV 界曲线.

然而对于 q 为非平方数的情形, $A(q)$ 的精确下界依然未知. 后续研究的最基本思路是构造 $\mathbb{F}_q$ 上无限域扩张下的 “函数域塔” [18], 通过构造优秀的 “函数域塔” 去优化更多 q 为非平方数时 $A(q)$ 的下界. 2014 年, 文献 [19] 给出了一种 q 的幂次为 2 以上的奇数情形下的 “函数域塔” 构造, 并证明了对于所有非素数的素数幂 $q \geqslant 49$ ($q = 125$ 除外), 存在渐近参数超过渐近 GV 界的 Shannon 好码渐近序列. 在该 “函数域塔” 基础上, 文献 [20,21] 通过取多点除子和广义 Hermite 曲线找到了 Riemann-Roch 空间基底的具体构造方法, 并在 $\mathbb{F}_{27}$ 等域上构造了优秀参数的码.

特别地, 对于构造在更小有限域 $\mathbb{F}_q$ (无论 q 是否为平方数) 上的 AG 码, 该问题通常更为困难. 2005 年, 文献 [22] 指出 Goppa 的构造对于所有的 $q \geqslant 2$, 理论上可以达到渐近 GV 界, 但要想具体构造还有一定困难. 事实上, Goppa 之后还有一些对 AG 码构造的推广, 包括通过选取特殊除子 [23]、考虑高次点而非有理点上的赋值 [24,25]、选取函数域的有限维子空间而非除子 G 的 Riemann-Roch 空间 [26] 等途径. 在这之中的很多构造也被证明实质上与 Goppa 的构造等价 [27], 或者不够简洁明确, 并且要从曲线推广到高维簇情形的构造, 还需要更多的研究和结论, 详见文献 [28,29].

除了 AG 码之外, 近些年还有基于图论方法的渐近码序列能够达到渐近 GV 界. 该理论从 $\mathbb{F}_2$ 上的非线性映射序列推广到线性映射序列, 但由线性映射序列得到的渐近码序列参数较为特殊, 且未给出具有明确生成矩阵形式 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$ 的代数族 $\{\boldsymbol{\sigma}_i\}$. 最新的研究结果参见文献 [30–32].

综上可知, 当 q 较大时, 由于可使用的代数技巧较多, 故以 AG 码为代表的一些线性映射族 $\{\boldsymbol{\sigma}_i\}$ 构造方法能在一定的区间上构造出达到或超过渐近 GV 界的 Shannon 好码渐近序列; 当 q 较小 ($q<46$) 时, 特别是 $q=2$ 的情形下, 达到渐近 GV 界的线性映射族 $\{\boldsymbol{\sigma}_i\}$ 及生成的码矢空间序列 $\{\Omega_i\}$ 的明确构造依然稀缺, 一些 AG 码即便达到了 TVZ 界曲线之上也并非万事大吉, 因为 TVZ 界曲线在 q 较小时离渐近 GV 界曲线尚有一定差距 (仅在 q 较大时能在部分区间上更优). 值得注意的是, Goppa [33] 曾断言, $q=2$ 情形下的渐近 GV 界是确切的 (即既是下界又是上界). 此外, 注意到渐近 GV 界的参数具有连续性, 而 AG 码在具体构造的过程中由于受到特定曲线限制, 码参数尚不够连续, 其生成矩阵结构尚也不够清晰, 利用图论等新近的方法依然如此. 因此, 能让码矢空间序列参数 n 和 k 摆脱特定整数限制, 且具有清晰生成矩阵 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$形式的代数族 $\{\boldsymbol{\sigma}_i\}$ 仍然匮乏.

基于新的途径, 本文给出一种具有清晰生成矩阵形式的线性映射渐近代数族 $\{\boldsymbol{\sigma}_i\}$, 它能在较小的信息符号域 $\mathbb{F}_q$ (特别是 $q=2$ 的二元域) 上, 对于任意指定的正整数 n 和 k ($n>k$), 皆生成达到渐近 GV 界的 Shannon 好码渐近序列

$$\{\Omega_i\}:=\{[n_i,k_i,d_i]\}\quad (i\to\infty).$$

以下将进一步介绍这种代数族 $\{\boldsymbol{\sigma}_i\}$ 的构造方法, 并表明它生成的 Shannon 好码渐近序列可达渐近 GV 界.

2 预备知识

2.1 生成矩阵的标准形式

这里首先给出本文所指的生成矩阵, 它是一切生成矩阵的标准形式.

定义 2.1 对于有限域 $\mathbb{F}_q$ ($q\geqslant 2$) 上 n 行 k 列 ($n>k$) 的列满秩生成矩阵 $\boldsymbol{G}_{n\times k}$, 在信息编码理论中, 这种生成矩阵 $\boldsymbol{G}_{n\times k}$ 都等价于标准形式

$$\boldsymbol{G}_{n\times k}=\left[\frac{\boldsymbol{I}_{k\times k}}{\boldsymbol{P}_{(n-k)\times k}}\right]_{n\times k},\tag{2.1}$$

其中 $\boldsymbol{I}_{k\times k}$ 是 k 阶单位矩阵, $\boldsymbol{P}_{(n-k)\times k}$ 是 $n-k$ 行 k 列矩阵.

容易知道, 标准形式下的线性映射 $\boldsymbol{\sigma}$ 将 k 维信息空间 $\mathbb{F}_q^k$ 中的向量, 映射到向量空间 $\mathbb{F}_q^n$ 中 (注意对比映射 (1.1)), 即对任意向量 $\boldsymbol{\alpha}\in\mathbb{F}_q^k$, 有

$$\boldsymbol{\sigma}:\mathbb{F}_q^k\to\mathbb{F}_q^k\oplus\mathbb{F}_q^{n-k},\quad \boldsymbol{\alpha}\mapsto\boldsymbol{\beta}=\boldsymbol{\alpha}\oplus\boldsymbol{P}_{(n-k)\times k}\cdot\boldsymbol{\alpha}.\tag{2.2}$$

同时关于该线性映射可以定义两个向量集合如下:

定义 2.2 记 $D_{\leqslant d-1}^k$ 是向量空间 (k 维信息空间) $\mathbb{F}_q^k\backslash\{\boldsymbol{0}\}$ 中所有 Hamming 重量不超过 $d-1$ 的向量集合, $D_{\leqslant d-1}^n$ 是向量空间 $\mathbb{F}_q^n\backslash\{\boldsymbol{0}\}$ 中所有 Hamming 重量不超过 $d-1$ 的向量集合.

2.2 原始 GV 界和渐近 GV 界

本小节首先引入从非渐近情形下的 GV 界 (原始 GV 界) 到渐近 GV 界的具体转换, 随后给出原始 GV 界在线性映射下的等价判定形式, 首先记变量

$$V_q(n,t):=\sum_{i=0}^{t}C_n^i(q-1)^i.\tag{2.3}$$

则有关于信息熵函数的如下引理.

引理 2.1 (参见文献 [1, 引理 5.1.6]) 令 $q \geqslant 2$, $0 \leqslant \lambda \leqslant (q-1)/q$, 有

$$\lim_{n\to\infty} n^{-1}\log_q V_q(n, \lfloor \lambda n \rfloor) = H_q(\lambda). \tag{2.4}$$

原始 GV 界 (无论线性映射还是非线性映射) 最早由如下定理给出:

定理 2.1 [5] 在有限域 $\mathbb{F}_q$ 上任意给定正整数 n 和 d ($n > d$), 设 $|\Omega|$ 为码矢空间 Ω 集合的势, 原始 GV 界断言

$$|\Omega| \geqslant \frac{q^n}{\sum_{i=0}^{d-1} C_n^i (q-1)^i}. \tag{2.5}$$

通过下面的定理可以将原始 GV 界在渐近情形下转换为渐近 GV 界.

定理 2.2 (参见文献 [1, 定理 5.1.9]) 若 $0 < \delta \leqslant (q-1)/q$, 则

$$R_{\mathrm{GV}}(\delta) \geqslant 1 - H_q(\delta). \tag{2.6}$$

证明 由引理 2.1 和定理 2.1, 有

$$\begin{aligned} R_{\mathrm{GV}}(\delta) &= \lim_{n\to\infty} \sup\, n^{-1}\log_q|\Omega| \\ &\geqslant \lim_{n\to\infty} \{1 - n^{-1}\log_q V_q(n, \delta n)\} \\ &= 1 - H_q(\delta), \end{aligned} \tag{2.7}$$

故结论成立. □

对有限域 $\mathbb{F}_q$ 上的线性映射 $\boldsymbol{\sigma}$ 而言有 $|\Omega| = q^k$, 故得原始 GV 界在线性映射下的等价判定形式如下:

定理 2.3 (参见文献 [1, 定理 5.1.8]) 在有限域 $\mathbb{F}_q$ 上任意给定正整数 n 和 k ($n > k$), 若正整数 d 满足

$$\sum_{i=0}^{d-1} C_n^i (q-1)^i < q^{n-k+1}, \tag{2.8}$$

则存在码矢空间 $\Omega := [n, k, d]$.

由该定理容易得到以下推论.

推论 2.1 在有限域 $\mathbb{F}_q$ 上任意给定正整数 n 和 k ($n > k$), 若正整数 d 和 ε 满足

$$\sum_{i=1}^{d-1} C_n^i (q-1)^i < q^{n-(k+\varepsilon)+1} - 1, \tag{2.9}$$

则存在码矢空间 $\Omega := [n, k, d]$.

证明 若不等式 (2.9) 成立, 即不等式 (2.8) 中 k 取 $k+\varepsilon$ 时成立. 由定理 2.3 知, 存在码矢空间 $\Omega := [n, k+\varepsilon, d]$; 又由 ε 是正整数知, 存在码矢空间 $\Omega := [n, k, d]$. □

特别地, 对于 $\varepsilon = 1$ 的情形, 有以下推论.

推论 2.2 在有限域 $\mathbb{F}_q$ 上任意给定正整数 n 和 k $(n>k)$, 若正整数 d 满足

$$\sum_{i=1}^{d-1} C_n^i (q-1)^i < q^{n-k}-1, \tag{2.10}$$

则存在码矢空间 $\Omega := [n,k,d]$.

证明 在推论 2.1 中代入 $\varepsilon=1$ 可得推论成立. □

2.3 伴随矩阵及相关映射性质

本小节将引入伴随矩阵及相关映射性质, 它是本文代数族构造的重要工具. 首先给出伴随矩阵的定义如下:

定义 2.3 [34] 系数在有限域 $\mathbb{F}_q$ 上的 m 次首一多项式

$$f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m \tag{2.11}$$

的伴随矩阵定义为

$$\boldsymbol{M} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{m-1} \end{bmatrix}_{m\times m}. \tag{2.12}$$

显然, 伴随矩阵 $\boldsymbol{M}$ 的特征多项式是 $f(x)$, 由 Cayley-Hamilton 定理可知, $\boldsymbol{M}$ 为方程 $f(\boldsymbol{M})=\boldsymbol{0}$ 矩阵形式的根, 即有

$$f(\boldsymbol{M}) = a_0\boldsymbol{I} + a_1\boldsymbol{M} + \cdots + a_{m-1}\boldsymbol{M}^{m-1} + \boldsymbol{M}^m = \boldsymbol{0}, \tag{2.13}$$

其中 $\boldsymbol{I}$ 为 m 阶单位矩阵, 进一步得到以下定理:

定理 2.4 [34] 令 $f(x)$ 为系数在有限域 $\mathbb{F}_q$ 上的 m 次首一本原多项式, 其伴随矩阵 $\boldsymbol{M}$ 满足方程

$$f(\boldsymbol{M}) = \boldsymbol{0},$$

则 $\boldsymbol{M}$ 具备本原多项式 $f(x)$ 根的性质, 它作为 q^m-1 阶循环群的生成元 (有限域中的本原元) 能生成有限域 $\mathbb{F}_{q^m}$ 中所有非零域元, 即有矩阵集合

$$\mathscr{M} = \{\boldsymbol{0}, \boldsymbol{M}^1, \boldsymbol{M}^2, \ldots, \boldsymbol{M}^{q^m-1} = \boldsymbol{I}\} \tag{2.14}$$

同构于有限域 $\mathbb{F}_{q^m}$, 其中 $\mathscr{M}$ 中零元对应到 $\mathbb{F}_{q^m}$ 中零元.

该定理给出了矩阵集合 $\mathscr{M}$ 与有限域 $\mathbb{F}_{q^m}$ 的一一对应. 下面的定理则给出了矩阵集合 $\mathscr{M}$ 与向量空间 $\mathbb{F}_q^m$ 的一一对应.

定理 2.5 令 $f(x)$ 为系数在有限域 $\mathbb{F}_q$ 上的 m 次首一本原多项式, $\boldsymbol{M}$ 是其伴随矩阵, 即有矩阵集合

$$\mathscr{M} = \{\boldsymbol{0}, \boldsymbol{M}^1, \boldsymbol{M}^2, \ldots, \boldsymbol{M}^{q^m-1} = \boldsymbol{I}\}$$

同构于有限域 $\mathbb{F}_{q^m}$, 则以下性质成立:

(1) 伴随矩阵 $\boldsymbol{M}$ 可逆;

(2) 任意给定向量 $\boldsymbol{\zeta} \in \mathbb{F}_q^m \backslash \{\boldsymbol{0}\}$, 对任意两个矩阵 $\boldsymbol{M}^i \in \mathscr{M} \backslash \{\boldsymbol{0}\}$ 和 $\boldsymbol{M}^j \in \mathscr{M} \backslash \{\boldsymbol{0}\}$, 若 $\boldsymbol{M}^i \neq \boldsymbol{M}^j$, 则有

$$\boldsymbol{M}^i \boldsymbol{\zeta} \neq \boldsymbol{M}^j \boldsymbol{\zeta},$$

即有矩阵集合

$$\mathscr{M}\boldsymbol{\zeta} = \{\boldsymbol{0}, \boldsymbol{M}^1\boldsymbol{\zeta}, \boldsymbol{M}^2\boldsymbol{\zeta}, \ldots, \boldsymbol{M}^{q^m-1}\boldsymbol{\zeta} = \boldsymbol{\zeta}\} = \mathscr{M} \tag{2.15}$$

同构于向量空间 $\mathbb{F}_q^m$, 其中 $\mathscr{M}$ 中零元对应到 $\mathbb{F}_q^m$ 中零元;

(3) 任意给定两个向量 $\boldsymbol{\nu} \in \mathbb{F}_q^m \backslash \{\boldsymbol{0}\}$ 和 $\boldsymbol{\mu} \in \mathbb{F}_q^m \backslash \{\boldsymbol{0}\}$ (可重复), 存在且仅存在唯一矩阵

$$\boldsymbol{M}^x \in \mathscr{M} \backslash \{\boldsymbol{0}\},$$

使得 $\boldsymbol{M}^x \boldsymbol{\nu} = \boldsymbol{\mu}$;

(4) 任意给定向量空间 $\mathbb{F}_q^m \backslash \{\boldsymbol{0}\}$ 中 4 个向量 $\boldsymbol{\nu}_1$、$\boldsymbol{\nu}_2$、$\boldsymbol{\mu}_1$ 和 $\boldsymbol{\mu}_2$ (可重复), 在某些取值情形下, 可能存在同一个矩阵 $\boldsymbol{M}^y \in \mathscr{M} \backslash \{\boldsymbol{0}\}$, 使得 $\boldsymbol{M}^y \boldsymbol{\nu}_1 = \boldsymbol{\mu}_1$ 和 $\boldsymbol{M}^y \boldsymbol{\nu}_2 = \boldsymbol{\mu}_2$ 同时成立.

证明 (1) 由定理 2.4 知 $\boldsymbol{M}^{q^m-1} = \boldsymbol{I}$, 又由 $\boldsymbol{M}$ 是方阵且行列式 $|\boldsymbol{M}^{q^m-1}| \neq 0$, 可知行列式 $|\boldsymbol{M}| \neq 0$, 故伴随矩阵 $\boldsymbol{M}$ 可逆.

(2) 用反证法, 假设当 $\boldsymbol{M}^i \neq \boldsymbol{M}^j$ 时,

$$\boldsymbol{M}^i \boldsymbol{\zeta} = \boldsymbol{M}^j \boldsymbol{\zeta}$$

成立. 由条件知 $i \neq j$, 不失一般性可设 $1 \leqslant i < j \leqslant q^m - 1$. 由 (1) 知矩阵 $\boldsymbol{M}$ 可逆, 可记 $\boldsymbol{M}$ 的逆为 $\boldsymbol{M}^-$, 将 $\boldsymbol{M}^i \boldsymbol{\zeta} = \boldsymbol{M}^j \boldsymbol{\zeta}$ 两边同时左乘 $(\boldsymbol{M}^-)^i$ 得 $\boldsymbol{\zeta} = \boldsymbol{M}^{j-i} \boldsymbol{\zeta}$, 因为 $\boldsymbol{\zeta} \neq \boldsymbol{0}$, 所以 $\boldsymbol{M}^{j-i} = \boldsymbol{I}$. 又由 $1 \leqslant i < j \leqslant q^m - 1$ 知 $0 < j - i < q^m - 1$, 故伴随矩阵 $\boldsymbol{M}$ 生成的循环群阶数不超过 $q^m - 1$, 这与伴随矩阵 $\boldsymbol{M}$ 生成的循环群阶数为 $q^m - 1$ 相矛盾, 则当 $\boldsymbol{M}^i \neq \boldsymbol{M}^j$ 时, $\boldsymbol{M}^i \boldsymbol{\zeta} \neq \boldsymbol{M}^j \boldsymbol{\zeta}$ 成立, 余下的结论是显然的.

(3) 由 (2) 和定理 2.4 可得.

(4) 结论是显然的. □

由定理 2.5(2) 可知, 对于任意给定的向量 $\boldsymbol{\zeta} \in \mathbb{F}_q^m \backslash \{\boldsymbol{0}\}$, 从矩阵集合 $\mathscr{M}\boldsymbol{\zeta}$ 到向量空间 $\mathbb{F}_q^m$ 有重要的一一对应, 本质上依然是矩阵集合 $\mathscr{M}$ 到向量空间 $\mathbb{F}_q^m$ 的一一对应, 因为非零向量 $\boldsymbol{\zeta}$ 在 $\mathscr{M}$ 上的作用是 $\mathscr{M}$ 上的自同构作用. 另外不难发现, 在 $\boldsymbol{\zeta}\mathscr{M}$ 情形下也有类似的定义和结论.

3 主要结果和具体构造

3.1 本文主要结果

诸多文献已表明, 前述赋值映射 (1.5) 及其研究途径对线性映射及所生成的码矢空间参数自由度有较多的限制. 为摆脱这种局限, 本文另辟路径, 直接考虑具有明确生成矩阵 $\boldsymbol{G}$ 形式的线性映射 $\boldsymbol{\sigma}$, 即后文重点考虑形如 (2.1) 的生成矩阵 $\boldsymbol{G}_{n\times k}$, 并由此导出码矢空间 $\Omega := [n, k, d]$.

本文发现的主要结果是, 给定有限域 $\mathbb{F}_q$ (特别是 $\mathbb{F}_2$)、任意正整数 n 和 k $(n>k)$, 均能够获得线性映射 $\boldsymbol{\sigma}$ 的明确生成矩阵形式 (2.1), 而由该生成矩阵导出的码矢空间 $\Omega:=[n,k,d]$, 其距离指标 d 的最大取值主要由不等式

$$\sum_{i=0}^{d-1}C_n^i(q-1)^i-\sum_{i=1}^{d-1}C_k^i(q-1)^i-\sum_{i=1}^{d-1}C_{n-k}^i(q-1)^i-r<q^{n-k} \tag{3.1}$$

决定, 其中 $C_k^i=0$ (当 $i\geqslant k+1$ 时), r 是一个非负整数. 显然, 给定 n 和 k $(n>k)$ 之后, r 越小则 d 越小, d "最坏" 的情形莫过于 $r=0$. 本文证明了, 即使在 "最坏" 的情形下, 也能给出 (2.1) 形式的生成矩阵 $\boldsymbol{G}_{n\times k}$ 来导出码矢空间 $\Omega:=[n,k,d]$, 使得其 n、k、d 参数可在渐近情形下达到渐近 GV 界.

关于主要结果更完整的准确表述详见本文第 4 节定理 4.1 和注 4.1–4.4. 以下详细说明这种具有明确生成矩阵 $\boldsymbol{G}_{n\times k}$ 的线性映射 $\boldsymbol{\sigma}$ 的构造方法.

3.2 一种可达渐近 GV 界的构造途径

由定理 2.2 可知渐近 GV 界可由非渐近情形下的原始 GV 界直接导出, 故一个关键的想法是, 构造代数族 $\{\boldsymbol{\sigma}_i\}$, 使得该代数族中任何线性映射 $\boldsymbol{\sigma}_i$ 所生成的码矢空间 Ω_i 的参数下界, 也不能距离原始 GV 界 (定理 2.3) 太远 (参数之间的差距在渐近情形下趋于 0). 特别地, 本文选择推论 2.2 作为目标进行构造.

同时, 给定有限域 $\mathbb{F}_q$、任意正整数 n 和 k $(n>k)$, 为得到距离指标至少为 d 的码矢空间 Ω, 另一个关键的想法是, 找到一个线性映射 $\boldsymbol{\sigma}$ (或生成矩阵 $\boldsymbol{G}$), 使得它生成的码矢空间 Ω 中所有向量均不在向量集合 $D^n_{\leqslant d-1}$ (参见定义 2.2) 中. 为此, 考虑如下构造假设:

构造假设 3.1 给定有限域 $\mathbb{F}_q$、任意正整数 n 和 k $(n>k)$, 在 $\mathbb{F}_q$ 上构造生成矩阵集合

$$\mathscr{G}=\{\boldsymbol{G}_1,\boldsymbol{G}_2,\ldots,\boldsymbol{G}_{q^{n-k}-1}\}, \tag{3.2}$$

其中矩阵集合 $\mathscr{G}$ 中元素 $\boldsymbol{G}_i$ 均是 n 行 k 列的标准形式生成矩阵, 记 $\boldsymbol{G}_i$ 分别生成码矢空间 Ω_i, 对于想要得到的距离指标 d, 若以下条件成立:

(1) 任意给定向量 $\boldsymbol{\varphi}\in D^n_{\leqslant d-1}$, 至多存在一个 $\mathscr{G}$ 中生成矩阵 $\boldsymbol{G}_t$, 由它生成的码矢空间 Ω_t 使得 $\boldsymbol{\varphi}\in\Omega_t$ 成立;

(2) 矩阵集合 $\mathscr{G}$ 的势大于向量集合 $D^n_{\leqslant d-1}$ 的势;

则通过该构造可得码矢空间 Ω, 使得其距离指标性能不低于推论 2.2 中的界. 进一步, 如果满足

(3) 任意给定两个不同的向量 $\boldsymbol{\varphi}_1,\boldsymbol{\varphi}_2\in D^n_{\leqslant d-1}$, 可能存在同一个生成矩阵 $\boldsymbol{G}_j\in\mathscr{G}$, 由它生成的码矢空间 Ω_j 使得下式同时成立:

$$\boldsymbol{\varphi}_1\in\Omega_j \quad 和 \quad \boldsymbol{\varphi}_2\in\Omega_j,$$

则 Ω 的距离指标还可能更优.

证明 当上述条件 (1) 和 (2) 同时成立时, 由抽屉原理可知, 集合 $\mathscr{G}$ 中至少存在一个生成矩阵 $\boldsymbol{G}$, 使得 $\boldsymbol{G}$ 生成的码矢空间 Ω 与向量集合 $D^n_{\leqslant d-1}$ 交集为空, 即 Ω 的距离指标至少为 d. 注意到不等式 (2.10) 的左端正好等于向量集合 $D^n_{\leqslant d-1}$ 的势, 而右端正好为矩阵集合 $\mathscr{G}$ 的势, 故通过该构造假设至少能达到推论 2.2 中的界. 进一步, 易得若上述条件 (3) 中情形多次出现, 则 Ω 的实际距离指标 d 显然只可能更大. □

因此, 如果给出构造假设 3.1 中生成矩阵的具体结构, 那么便能给出距离性能不低于推论 2.2 的码矢空间, 由此便能够找到这样的生成矩阵, 由它导出的码矢空间参数的下限仅在 k 上距离原始 GV 界 (参见定理 2.3) 至多相差 1 (即推论 2.1 中 $\varepsilon = 1$ 的情形). 更进一步, 由此也找到了具有明确生成矩阵形式 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$ 的代数族 $\{\boldsymbol{\sigma}_i\}$ 途径, 使得所构造的 Shannon 好码渐近序列 $\{\Omega_i\}$ $(i\to\infty)$ 可达渐近 GV 界. 值得注意的是, 若构造假设 3.1(3) 的情形多次出现, 则通过该假设所构造出的 Shannon 好码渐近序列就有了超过渐近 GV 界的可能.

3.3 运用伴随矩阵的具体构造

本小节给出满足构造假设 3.1 的 $\mathscr{G}$ 中生成矩阵的具体结构, 关键还在于所构造的 $\mathscr{G}$ 中生成矩阵需具备特殊映射性质. 故利用伴随矩阵及相关映射性质 (参见定理 2.5), 本小节给出 $\mathscr{G}$ 中具有标准形式的生成矩阵构造如下:

构造 3.1 给定有限域 $\mathbb{F}_q$、任意正整数 n 和 k $(n>k)$, 具体构造生成矩阵集合 (3.2) 为

$$\mathscr{G}=\left\{\left[\frac{\boldsymbol{I}}{\boldsymbol{M}^i\cdot\boldsymbol{B}_{(n-k)\times k}}\right]_{n\times k}\,\middle|\, i=1,2,\ldots,q^{n-k}-1\right\},\tag{3.3}$$

其中 $\boldsymbol{I}$ 是 k 阶单位矩阵, $n-k$ 阶方阵 $\boldsymbol{M}$ 是 $\mathbb{F}_q$ 上一个首一 $n-k$ 次本原多项式 $f(x)$ 的伴随矩阵 (参见定义 2.3), 而矩阵 $\boldsymbol{B}_{(n-k)\times k}$ 的构造分为以下两种情形:

(1) 当 $k/n\leqslant 1/2$ 时, 构造 $\boldsymbol{B}_{(n-k)\times k}$ 为任意列满秩矩阵;

(2) 当 $k/n>1/2$ 时, 若已知存在参数为 $n_0=k$、$k_0=2k-n$ 和 d_0 (其中 d_0 不小于想要通过构造得到的 d 的最大值) 的码矢空间 $\Omega_0:=[n_0,k_0,d_0]$, 它对应的生成矩阵记为 $\boldsymbol{H}_{k\times(2k-n)}$, 则构造 $\boldsymbol{B}_{(n-k)\times k}$ 为满足方程

$$\boldsymbol{B}_{(n-k)\times k}\boldsymbol{H}_{k\times(2k-n)}=\boldsymbol{0}\tag{3.4}$$

的行满秩矩阵, 也即 $\boldsymbol{B}_{(n-k)\times k}$ 可由方程

$$\boldsymbol{x}\boldsymbol{H}_{k\times(2k-n)}=\boldsymbol{0}\tag{3.5}$$

解空间的一组基底构造而成.

至此, 本小节明确给出了构造假设 3.1 中形如 $\mathscr{G}$ 的生成矩阵的具体结构. 至于该构造如何满足构造假设 3.1 中条件, 在下一节中将会体现得更加清晰.

4 达到渐近 GV 界的一种 Shannon 好码渐近序列

本节将具体证明构造 3.1 给出的码矢空间距离指标 d 的实际取值情形, 同时也说明这种具有明确生成矩阵形式 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$ 的代数族 $\{\boldsymbol{\sigma}_i\}$ 途径所构造的 Shannon 好码渐近序列 $\{\Omega_i\}$ $(i\to\infty)$ 可达渐近 GV 界.

4.1 构造 3.1 所得码矢空间的实际距离指标

首先通过构造 3.1 可以立即得到下面的定理.

定理 4.1 给定有限域 $\mathbb{F}_q$、任意正整数 n 和 k $(n>k)$, 结论分为以下两种情形:

(1) 当 $k/n\leqslant 1/2$ 时, 若正整数 d 满足不等式

$$\sum_{i=1}^{d-1}C_n^i(q-1)^i-\sum_{i=1}^{d-1}C_k^i(q-1)^i-\sum_{i=1}^{d-1}C_{n-k}^i(q-1)^i-r<q^{n-k}-1, \tag{4.1}$$

其中 $C_k^i=0$ (当 $i\geqslant k+1$ 时), 而非负整数 r 是一个表示重复的参数, 则通过构造 3.1 可得码矢空间 $\Omega:=[n,k,\geqslant d]$.

(2) 当 $k/n>1/2$ 时, 若正整数 d 同时满足不等式 (4.1) 和不等式 $d\leqslant d_0$ (即构造 3.1 中已知有码矢空间 $\Omega_0:=[n_0,k_0,d_0]$), 则通过构造 3.1 可得码矢空间 $\Omega:=[n,k,\geqslant d]$.

证明 由构造 3.1 中生成矩阵的具体结构可知, 对任意向量 $\boldsymbol{\gamma}\in\mathbb{F}_q^k$, 通过 $\mathscr{G}$ 中生成矩阵作用有

$$\left[\frac{\boldsymbol{I}}{\boldsymbol{M}^i\cdot\boldsymbol{B}_{(n-k)\times k}}\right]\cdot\boldsymbol{\gamma}=\left[\frac{\boldsymbol{\gamma}}{\boldsymbol{M}^i\cdot\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{\gamma}}\right]=\left[\frac{\boldsymbol{\gamma}}{\boldsymbol{\phi}}\right]=\boldsymbol{\varphi}. \tag{4.2}$$

若能证明存在某个正整数 $i\in\{1,2,\ldots,q^{n-k}-1\}$, 使得对任意向量 $\boldsymbol{\gamma}\in\mathbb{F}_q^k$, 经生成矩阵 $\boldsymbol{M}^i$ 作用 (4.2) 后得到的最终向量 $\boldsymbol{\varphi}$ 均不在集合 $D^n_{\leqslant d-1}$ (参见定义 2.2) 中, 则由生成矩阵 $\boldsymbol{M}^i$ 导出的码矢空间 Ω 的距离指标至少为 d.

当向量 $\boldsymbol{\gamma}=\boldsymbol{0}$ 时, 经 (4.2) 后恒有 $\boldsymbol{\varphi}=\boldsymbol{0}$. 由定义 2.2 知 $\boldsymbol{\varphi}$ 不在集合 $D^n_{\leqslant d-1}$ 中. 故我们只需就向量 $\boldsymbol{\gamma}\in\mathbb{F}_q^k\backslash\{\boldsymbol{0}\}$ 的情形进行证明.

(1) 当 $k/n\leqslant 1/2$ 时, 由构造 3.1 中矩阵 $\boldsymbol{B}_{(n-k)\times k}$ 的秩为 k 知, 对任意向量 $\boldsymbol{\gamma}\in\mathbb{F}_q^k\backslash\{\boldsymbol{0}\}$, 有

$$\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{\gamma}\neq\boldsymbol{0},$$

进而由定理 2.5(2) 有

$$\boldsymbol{\phi}\neq\boldsymbol{0}.$$

记 $\bar{D}^n_{\leqslant d-1}$ 由向量集合 $D^n_{\leqslant d-1}$ 中 $\boldsymbol{\gamma}$ 和 $\boldsymbol{\phi}$ 均不为 $\boldsymbol{0}$ 的向量组成, 则由集合 $D^n_{\leqslant d-1}$ 易得集合 $\bar{D}^n_{\leqslant d-1}$ 的势为

$$\sum_{i=1}^{d-1}C_n^i(q-1)^i-\sum_{i=1}^{d-1}C_k^i(q-1)^i-\sum_{i=1}^{d-1}C_{n-k}^i(q-1)^i. \tag{4.3}$$

给定任意向量 $\boldsymbol{\varphi}\in\bar{D}^n_{\leqslant d-1}$, 由 $\boldsymbol{\varphi}=\boldsymbol{\gamma}\oplus\boldsymbol{\phi}$ 知, $\boldsymbol{\varphi}$ 对应的向量 $\boldsymbol{\gamma}$ 和 $\boldsymbol{\phi}$ 是确定的且均不为 $\boldsymbol{0}$, 进而向量 $\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{\gamma}$ 也随之确定且不为 $\boldsymbol{0}$. 由定理 2.5(3) 可知, 存在且仅存在唯一正整数 $j\in\{1,2,\ldots,q^{n-k}-1\}$, 使得向量 $\boldsymbol{\phi}=\boldsymbol{M}^j\cdot(\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{\gamma})$, 即存在且仅存在唯一生成矩阵 $\boldsymbol{G}_j\in\mathscr{G}$, 使得 $\boldsymbol{G}_j$ 生成的码矢空间 Ω_j 包含向量 $\boldsymbol{\varphi}$.

又由定理 2.5(4) 知, 可能存在集合 $\bar{D}^n_{\leqslant d-1}$ 中多个不同的向量, 使得它们均在同一个生成矩阵 $\boldsymbol{G}_t\in\mathscr{G}$ 所生成的码矢空间 Ω_t 中. 故要确定至多需要多少个集合 $\mathscr{G}$ 中生成矩阵, 来得到向量集合 $\bar{D}^n_{\leqslant d-1}$ 中所有向量, 还需减去一个表示重复的参数 r (非负整数), 即至多需要

$$\sum_{i=1}^{d-1}C_n^i(q-1)^i-\sum_{i=1}^{d-1}C_k^i(q-1)^i-\sum_{i=1}^{d-1}C_{n-k}^i(q-1)^i-r \tag{4.4}$$

个集合 $\mathscr{G}$ 中生成矩阵. 由集合 $\mathscr{G}$ 的势为 $q^{n-k}-1$ 知, 当不等式 (4.1) 成立时, 我们至少能得到一个 $\mathscr{G}$ 中生成矩阵 $\boldsymbol{G}_i$, 它生成的码矢空间 Ω_i 与向量集合 $\bar{D}^n_{\leqslant d-1}$ 交集为空; 进一步易知 Ω_i 与 $D^n_{\leqslant d-1}$ 交集也为空, 即通过构造 3.1 可给出码矢空间 $\Omega:=[n,k,\geqslant d]$.

(2) 当 $k/n > 1/2$ 时, 由构造 3.1 知, 矩阵 $\boldsymbol{B}_{(n-k)\times k}$ 是行满秩矩阵, 且方程 $\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{x}=\boldsymbol{0}$ 的解空间中向量的最小 Hamming 重量为 d_0. 也就是说, 对任意向量 $\boldsymbol{\gamma}\in D^k_{\leqslant d-1}$, 由 $d\leqslant d_0$ 知 (4.2) 中 $\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{\gamma}\neq\boldsymbol{0}$ (否则与构造 3.1 中 $\boldsymbol{H}_{k\times(2k-n)}$ 的最小 Hamming 重量为 d_0 相矛盾), 进而 $\boldsymbol{\phi}\neq\boldsymbol{0}$.

又由向量 $\boldsymbol{\gamma}$ 经 (4.2) 后得到的最终向量 $\boldsymbol{\varphi}=\boldsymbol{\gamma}\oplus\boldsymbol{\phi}$ 知, 对于满足不等式 $d\leqslant d_0$ 的距离指标 d, 仅需考虑向量 $\boldsymbol{\gamma}\in D^k_{\leqslant d-1}$ 的情形 (其余情形均不会影响构造所给出的码矢空间的距离指标), 而此时

$$\boldsymbol{B}_{(n-k)\times k}\cdot\boldsymbol{\gamma}\neq\boldsymbol{0}$$

且

$$\boldsymbol{\phi}\neq\boldsymbol{0},$$

故结论和 (1) 同理可证. □

4.2 几点注记

通过对定理 4.1 的证明, 既可知构造 3.1 的确满足构造假设 3.1 的条件, 也明确了通过构造 3.1 所给出的码矢空间中参数 n、k 和 d 的实际取值情形. 另外将不等式 (4.1) 稍作变换即有不等式

$$\sum_{i=0}^{d-1}C_n^i(q-1)^i-\sum_{i=1}^{d-1}C_k^i(q-1)^i-\sum_{i=1}^{d-1}C_{n-k}^i(q-1)^i-r<q^{n-k}. \tag{4.5}$$

注 4.1 在非渐近情形下, 对比不等式 (4.5) 和 (2.8) 可知, 给定有限域 $\mathbb{F}_q$、任意正整数 n 和 k $(n>k)$, 如果原始 GV 界 (参见定理 2.3) 保证了 $\mathbb{F}_q$ 上码矢空间 $\Omega:=[n,k,d]$ 的存在性, 则由定理 4.1 知, 即使在 "最坏" 情形 $r=0$ 时, 通过构造 3.1 也能在 $\mathbb{F}_q$ 上找到具有明确生成矩阵形式的线性映射来给出码矢空间

$$\Omega:=[n,k-1,\geqslant d].$$

而当 r 可能很大时, 通过构造 3.1 还可能给出具有更好距离指标的码矢空间 Ω.

注 4.2 在渐近情形下, 由注 4.1 更进一步可以得到, 通过构造 3.1 的代数族 $\{\boldsymbol{\sigma}_i\}$ 途径给出的 Shannon 好码渐近序列的渐近参数和渐近 GV 界的差距趋于 0. 故本文具有明确生成矩阵形式的代数族 $\{\boldsymbol{\sigma}_i\}$ 途径给出的 Shannon 好码渐近序列 $\{\Omega_i\}$ $(i\to\infty)$ 可达到渐近 GV 界.

注 4.3 需要特别注意的是, 若如 Goppa 所断言, 在有限域 $\mathbb{F}_2$ 上渐近 GV 界是渐近确切的 (即既是下界又是上界), 则构造 3.1 所给出的码矢空间距离指标 d 只会受到不等式 (4.5) 的约束. 这是因为在 $k/n>1/2$ 的情形下, 渐近 GV 界的存在保证了在构造 3.1 中, 总是能找到合适的矩阵 $\boldsymbol{B}_{(n-k)\times k}$ 使得 d_0 足够大, 即与不等式 (4.5) 相比, 不等式 $d\leqslant d_0$ 不会对所构造的 Shannon 好码渐近序列的距离指标产生约束.

注 4.4 显然非负整数 r 的取值还可进一步优化, 它与有限域的具体结构有关. 故在非渐近情形下, 通过构造 3.1 还可能给出达到或超过原始 GV 界的码矢空间的参数 n、k 和 d. 而在渐近情形下, 若在有限域 $\mathbb{F}_2$ 上渐近 GV 界不是渐近确切的 (即在 $\mathbb{F}_2$ 上, 通过优化 r, 还有改进渐近 GV 界的可能), 则通过构造 3.1 给出的 Shannon 好码渐近序列的距离指标 d, 还可能受到构造 3.1 中码矢空间

$$\Omega_0:=[n_0,k_0,d_0]$$

存在性的限制 (即距离指标 d 最大取值被不等式 $d\leqslant d_0$ 约束).

5 总结

至此, 本文从矩阵映射的观点给出了一种在任意有限域 $\mathbb{F}_q$ (特别是 $\mathbb{F}_2$) 上具有明确生成矩阵形式 $\{\boldsymbol{G}_{n\times k}^{\{i\}}\}$ 的代数族 $\{\boldsymbol{\sigma}_i\}$ 新方法, 并表明由 $\{\boldsymbol{\sigma}_i\}$ 导出的 Shannon 好码渐近序列 $\{\Omega_i\} := \{[n_i, k_i, d_i]\}$ $(i \to \infty)$ 可达到渐近 GV 界. 这种新的代数族生成途径在工程应用中, 不仅构造简洁、易于实现, 而且由于重复参数 r 的存在, 还可能获得更优的实际性能.

致谢 特别感谢张景中院士曾对以下问题的关心和指导: 在固定的符号域上, 特别是 $\mathbb{F}_2$ 上, 能否以及如何构造任意规模的 "广义 Cauchy 高矩阵" (或 "广义 Vandermonde 高矩阵") $\boldsymbol{G}_{n\times k}$, 使得 $\boldsymbol{G}_{n\times k}$ 的任何 $k+\delta$ 行形成的子矩阵 $\boldsymbol{A}_{(k+\delta)\times k}$ 皆是列满秩的? 最节省的增量 δ 应是多少? 该问题数年前激励了作者进行相关研究, 本文的结果可以从一个侧面一定程度上回答该问题, 即 δ 至多等于 $(n-k)-(d-1)$ 就足够了, 其中 d 即为本文中的 "距离指标". 该问题更一般的详细结果将在我们的其他论文中给出. 特别感谢杨路教授长期以来对作者的鼓励和帮助. 同时感谢审稿人为本文提供的宝贵意见.

参考文献

1 van Lint J H. Introduction to Coding Theory. Heidelberg: Springer-Verlag, 1999
2 Shannon C E. A mathematical theory of communication. Bell Syst Tech J, 1948, 27: 379–423
3 Stichtenoth H. Algebraic Function Fields and Codes. Heidelberg: Springer-Verlag, 2009
4 Huffman W C, Pless V. Fundamentals of Error-Correcting Codes. Cambridge: Cambridge University Press, 2003
5 Gilbert E N. A comparison of signalling alphabets. Bell Syst Tech J, 1952, 31: 504–522
6 Varshamov R R. Estimate of the number of signals in error correcting codes (in Russian). Dokl Akad Nauk SSSR, 1957, 117: 739–741
7 Justesen J. Class of constructive asymptotically good algebraic codes. IEEE Trans Inform Theory, 1972, 18: 652–656
8 Goppa V D. Codes associated with divisors (in Russian). Probl Peredachi Inf, 1977, 13: 33–39
9 Goppa V D. Codes on algebraic curves (in Russian). Dokl Akad Nauk SSSR, 1981, 259: 1289–1290
10 Goppa V D. Algebraico-geometric codes. Math USSR Izv, 1983, 21: 75–91
11 Martínez-Moro E, Munuera C, Ruano D. Advances in Algebraic Geometry Codes. Singapore: World Scientific, 2008
12 Hurt N E. Many Rational Points. Dordrecht: Springer, 2003
13 Tiersma H. Remarks on codes from Hermitian curves (Corresp.). IEEE Trans Inform Theory, 1987, 33: 605–609
14 Park S. Minimum distance of Hermitian two-point codes. Des Codes Cryptogr, 2010, 57: 195–213
15 Vlăduţ S G, Drinfel'd V G. Number of points of an algebraic curve. Funct Anal Appl, 1983, 17: 53–54
16 Ihara Y. Congruence relations and Shimura curves. In: Automorphic Forms, Representations, and L-functions. Proceedings of Symposia in Mathematics. Providence: Amer Math Soc, 1979, 291–311
17 Tsfasman M A, Vlăduţ S G, Zink T. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. Math Nachr, 1982, 109: 21–28
18 Garcia A, Stichtenoth H. On the asymptotic behaviour of some towers of function fields over finite fields. J Number Theory, 1996, 61: 248–273
19 Bassa A, Beelen P, Garcia A, et al. An improvement of the Gilbert-Varshamov bound over nonprime fields. IEEE Trans Inform Theory, 2014, 60: 3859–3861
20 Hu C Q, Zhao C A. Multi-point codes from generalized Hermitian curves. IEEE Trans Inform Theory, 2016, 62: 2726–2736
21 Hu C Q. Explicit construction of AG codes from a curve in the tower of Bassa-Beelen-Garcia-Stichtenoth. IEEE Trans Inform Theory, 2017, 63: 7237–7246
22 Xing C P. Goppa geometric codes achieving the Gilbert-Varshamov bound. IEEE Trans Inform Theory, 2005, 51: 259–264
23 Xing C P, Niederreiter H, Lam K Y. Constructions of algebraic-geometry codes. IEEE Trans Inform Theory, 1999, 45: 1186–1193
24 Niederreiter H, Xing C P, Lam K Y. A new construction of algebraic geometry codes. Appl Algebra Engrg Comm Comput, 1999, 9: 373–381
25 Xing C P, Niederreiter H, Lam K Y. A generalization of algebraic-geometry codes. IEEE Trans Inform Theory, 1999, 45: 2498–2501
26 Xing C P, Ling S. A class of linear codes with good parameters from algebraic curves. IEEE Trans Inform Theory, 2000, 46: 1527–1532

27 Ozbudak F, Stichtenoth H. Constructing codes from algebraic curves. IEEE Trans Inform Theory, 1999, 45: 2502–2505
28 Tsfasman M A, Vlăduţ S G. Algebraic-Geometric Codes. Netherlands: Springer, 1991
29 Beelen P. The order bound for general algebraic geometric codes. Finite Fields Appl, 2007, 13: 665–680
30 Jiang T, Vardy A. Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes. IEEE Trans Inform Theory, 2004, 50: 1655–1664
31 Vu V, Wu L. Improving the Gilbert-Varshamov bound for q-ary codes. IEEE Trans Inform Theory, 2005, 51: 3200–3208
32 Gaborit P, Zemor G. Asymptotic improvement of the Gilbert-Varshamov bound for linear codes. IEEE Trans Inform Theory, 2008, 54: 3865–3872
33 Goppa V D. Bounds for codes (in Russian). Dokl Akad Nauk SSSR, 1993, 333: 423
34 Freedman H, Lidl R, Niederreiter H. Introduction to Finite Fields and Their Applications. Cambridge: Cambridge University Press, 1995

A method of constructing linear mapping families to achieve the asymptotic GV bound

Xiaojing Wang & Xingyi Peng

Abstract Given a finite field $\mathbb{F}_q$ ($q \geqslant 2$) and arbitrary positive integers n and k ($n > k$), the construction methods of linear mapping sequences (algebraic families) $\{\boldsymbol{\sigma}_i\}$ ($\boldsymbol{\sigma}_i : \mathbb{F}_q^k \to \mathbb{F}_q^n$ ($i \to \infty$)) over $\mathbb{F}_q$ have been a central problem of coding theory in information science, which is generally called the algebraic family approach to the Shannon ideal. Until now, finding a better structure of the algebraic family $\{\boldsymbol{\sigma}_i\}$, and using it to derive asymptotic sequences $\{[n_i, k_i, d_i]\}$ of the Shannon good codes, is still an unresolved challenge and ongoing goal. To measure the algebraic family, in addition to seeing whether the construction $\{\boldsymbol{\sigma}_i\}$ is convenient for implementation by communication engineering (simple construction, low complexity), a vital standard is to see if the asymptotic parameters of sequences $\{[n_i, k_i, d_i]\}$ derived by $\{\boldsymbol{\sigma}_i\}$ do not decrease under the asymptotic Gilbert-Varshamov bound (asymptotic GV bound), which has attracted the attention of many mathematicians. In this paper, we give a new method by the matrix mapping to generate the algebraic family $\{\boldsymbol{\sigma}_i\}$ over any finite field $\mathbb{F}_q$, and we indicate the asymptotic code sequences $\{[n_i, k_i, d_i]\}$ derived by $\{\boldsymbol{\sigma}_i\}$ are above the asymptotic GV bound. The new approach to construct algebraic families is of great significance to information coding theory and its engineering application.

Keywords **linear mapping families, algebraic construction, asymptotic Gilbert-Varshamov bound**

MSC(2010) **11T71, 94A24**

doi: 10.1360/SSM-2019-0321