擦除信道中的译码错误概率和 r -次支撑重量分布

献给冯克勤教授 80 华诞

熊茂胜

香港科技大学数学系, 香港

E-mail: mamsxiong@ust.hk

收稿日期: 2021-01-26; 接受日期: 2021-04-01; 网络出版日期: 2021-09-22

香港优配研究金 RGC (批准号: IRS21SC42) 资助项目

摘要 受近期 Shen 和 Fu 的文章启发, 本文研究在三种不同译码原则下, 线性码在擦除信道中传播的译码错误概率. 首先简化 Shen 和 Fu 所得到的确切公式, 结果显示译码错误概率与线性码的 r -次支撑重量分布有更加直接的联系. 然后对于 $[n, k]_q$ 线性码, 计算 r -次支撑重量分布的均值; 并且, 对于 Shen 和 Fu 文章中所遗留的公开问题, 即在最大似然译码原则下, 随机 $[n, nR]_q$ 线性码在擦除信道中的非成功译码概率的错误指数, 本文给出解答. 最后, 在列表译码的原则下, 本文计算出随机 $[n, nr]_q$ 线性码在擦除信道中的非成功译码概率的错误指数.

关键词 擦除信道 线性码 非成功译码概率 错误指数

MSC (2020) 主题分类 94B05, 94B70

1 引言

1.1 背景

在数字通信中, 信息传递于有噪声的信道时常发生扭曲. 纠错码的理论正是研究如何处理这个问题. 这是一个重要的研究领域, 对于现代生活有很多应用场景. 例如, 纠错码在手机通信中应用广泛, 用于纠正在高频无线电传输过程中由于衰落噪声所产生的错误. 构造拥有良好性质的纠错码和研究译码、编码算法仍然是编码理论中一个重要的具有挑战性的问题.

在二元的擦除信道 (binary erasure channel, BEC) 中, 接收到的二元信号要么是是正确的, 要么以概率 ϵ 被完全擦除. 擦除信道的概念首先由 Elias 提出 (参见文献 [1]). 擦除信道频繁出现于编码理论和信息论中, 因为它是最简单的信道模型之一, 而且很多通信问题都可以转化为擦除信道中的问题. 本文考虑更一般的 q -元的擦除信道, 在此信道中, 一个 q -元信号要么传递正确, 要么以概率 ϵ 被擦除.

英文引用格式: Xiong M S. Decoding error probability in the erasure channel and the r -th support weight distribution (in Chinese). Sci Sin Math, 2021, 51: 1685–1698, doi: 10.1360/SSM-2021-0019

在网络和分布式存储系统中, 擦除信道中的线性码广泛应用于分析估计随机数据包的丢失问题 (参见文献 [2–4]) 中, 因而线性码在擦除信道中的译码问题受到很多学者的关注. 在最近几年, 擦除信道的线性码的三大重要译码原则, 即明确译码、最大似然译码和列表译码, 已经被提出并得到发展; 相应的译码错误概率问题, 即按照译码原则对于从擦除信道中传来的信息进行错误译码的概率问题, 已经被众多学者研究, 相应的引人注目的结果可参见文献 [5–8].

特别地, 2019 年, Shen 和 Fu^[7] 运用他们新近提出的线性码的 “ q^ℓ - 不可修正集” 的概念并且改进文献 [6, 8] 中的研究结果, 详尽地研究了擦除信道中的线性码的译码错误概率问题. 在众多解决的问题以外, 他们得到了线性码在擦除信道中基于以上三大译码原则下的译码错误概率的显式表达式. 这些公式第一次明确而直接地展示了线性码在擦除信道中的译码错误概率与线性码的 r - 次支撑重量分布的关系. 线性码的 r - 次支撑重量分布类似于线性码的重量分布但是比线性码的重量分布更广, 是关于线性码的一族基本参数. 这些关系中的一部分已经隐含于一些文献之中 (参见文献 [5, 6, 8]). 这些公式的显式表达式有实际的应用, 例如, 它们可以用于计算当使用二元 Golay 码、拓展的二元 Golay 码和一些别的线性码于擦除信道时的译码错误概率^[7], 这些线性码的 r - 次支撑重量分布是已知的. 另外, 这些公式和背后的思想可以用于推导关于随机 $[n, k]_q$ 线性码在擦除信道中的译码错误概率. 更多细节, 可参见文献 [7].

1.2 主要结果陈述

我们需要指出, 尽管文献 [7] 中的公式的显式表达非常有用, 但是, 这些公式看起来相当复杂, 它们与 r - 次支撑重量分布的关系是非直接的. 基于对 r - 次支撑重量分布进行以二项式系数为首的线性组合, 这些量称为线性码的 r - 阶广义二项式的动差. 其实通过细致的代数变换, 以及运用二项式系数 $\binom{n}{m}$ 和 Gauss 二项式系数 $\begin{bmatrix} n \\ m \end{bmatrix}_q$ 的性质, 以上的公式可以大大简化. 我们的第一个结果如下.

定理 1.1 设 C 为一个 $[n, k]_q$ 线性码, $\{A_i^{(r)}\}_{i=1}^n$ 是其 r - 次支撑重量分布, 其中 $1 \leq r \leq k$, 则

(1) 基于 q^ℓ - 列表译码原则, 我们得到 C 的非成功译码概率 $P_d(C, \ell, \epsilon)$ 为

$$P_d(C, \ell, \epsilon) = \sum_{r=\ell+1}^k \sum_{j=r-\ell}^r (-1)^{j-1} q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q W^{(r)}(\epsilon); \quad (1.1)$$

(2) 基于最大似然译码原则, 我们得到 C 的译码错误概率 $P_{\text{mld}}(C, \epsilon)$ 为

$$P_{\text{mld}}(C, \epsilon) = \sum_{r=1}^k (-1)^{r-1} (T)_r q^{r(r-1)/2} W^{(r)}(\epsilon); \quad (1.2)$$

(3) 基于明确译码原则, 我们得到 C 的非成功译码概率 $P_{\text{ud}}(C, \epsilon)$ 为

$$P_{\text{ud}}(C, \epsilon) = \sum_{r=1}^k (-1)^{r-1} q^{r(r-1)/2} W^{(r)}(\epsilon). \quad (1.3)$$

这里 $T := q^{-1}$,

$$(T)_r := \prod_{i=1}^r (1 - T^i), \quad (1.4)$$

且 $W^{(r)}(x)$ 是 C 的 r - 次支撑重量单项式, 表达式为

$$W^{(r)}(x) = \sum_{i=1}^n A_i^{(r)} x^i. \quad (1.5)$$

与文献 [7, 定理, 第 6194 和 6195 页] 做比较, (1.1)–(1.3) 不仅看起来更为简洁, 而且显示了与 C 的 r -次支撑重量更为直接和自然的关系, 不需要通过复杂的 C 的“ r -阶广义二项式的动差”. 这表明对于 C 在三种译码原则下于擦除信道中的译码表现, 其 r -次支撑重量分布扮演了关键性的角色. 这种情形非常类似于经典情形, 即在最大似然译码原则下二元对称信道中, 线性码的重量分布对于其译码表现扮演了关键性的角色 (参见文献 [9, 第 1 章]).

除了一些零散的例子, 计算线性码的 r -次支撑重量分布非常困难, 这甚至要远难于计算更为常见的线性码的重量分布. $[n, k]_q$ 线性码的 r -次支撑重量分布的均值是多少? 对于这个问题, 设 $\mathcal{C}$ 为所有 $[n, k]_q$ 线性码的集合, 我们使用如下符号:

$$A_i^{(r)}(\mathcal{C}) = \frac{1}{\#\mathcal{C}} \sum_{C \in \mathcal{C}} A_i^{(r)}(C), \quad (1.6)$$

其中 $\#\mathcal{C}$ 代表集合 $\mathcal{C}$ 的元素的个数. 我们得到如下定理:

定理 1.2 设 $\mathcal{C}$ 为所有 $[n, k]_q$ 线性码的集合. 对于任意的 $1 \leq r \leq k$, 有

$$\sum_{i=1}^n A_i^{(r)}(\mathcal{C}) x^i = \frac{\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \sum_{s=r}^n \begin{bmatrix} s \\ r \end{bmatrix}_q \binom{n}{s} x^s (1-x)^{n-s}.$$

另外, 文献 [7] 对于随机的 $[n, nR]_q$ 线性码, 计算了其基于明确译码原则下非成功译码概率的错误指数, 但是留下一个公开问题, 即其基于最大似然译码原则下译码错误概率的错误指数的计算. 我们解决了这个问题, 结论如下:

定理 1.3 设 $0 < R < 1$, $\mathcal{C}_n$ 是所有 $[n, nR]_q$ 线性码的集合. 我们得到 $\mathcal{C}_n$ 基于最大似然译码原则下平均译码错误概率的错误指数为

$$T(\epsilon) = \begin{cases} 0, & R \geq 1 - \epsilon, \\ (1-R) \log_q \frac{1-R}{\epsilon} + R \log_q \frac{R}{1-\epsilon}, & \frac{1-\epsilon}{1-\epsilon+q\epsilon} < R < 1 - \epsilon, \\ 1-R - \log_q(1-\epsilon+q\epsilon), & 0 < R \leq \frac{1-\epsilon}{1-\epsilon+q\epsilon}. \end{cases}$$

需要指出的是, 定理 1.3 中的错误指数 $T(\epsilon)$ 与文献 [7, 定理 3] 中完全一样, 即随机的 $[n, nR]_q$ 线性码基于最大似然译码原则下译码错误概率的错误指数恒等于其基于明确译码原则下非成功译码概率的错误指数.

最后, 在付方伟教授的建议下, 我们也计算并得到了随机 $[n, nR]_q$ 线性码的基于列表译码原则下的非成功译码概率的错误指数, 结论如下:

定理 1.4 设 $0 < R < 1$, $\mathcal{C}_n$ 是所有 $[n, nR]_q$ 线性码的集合. 对任意固定的非负整数 $\ell \geq 0$, 我们得到 $\mathcal{C}_n$ 的基于 q^ℓ -列表译码下的平均非成功译码概率的错误指数为

$$T(\epsilon) = \begin{cases} 0, & R \geq 1 - \epsilon, \\ (1-R) \log_q \frac{1-R}{\epsilon} + R \log_q \frac{R}{1-\epsilon}, & \frac{1-\epsilon}{1-\epsilon+q^{\ell+1}\epsilon} < R < 1 - \epsilon, \\ (\ell+1)(1-R) - \log_q(1-\epsilon+q^{\ell+1}\epsilon), & 0 < R \leq \frac{1-\epsilon}{1-\epsilon+q^{\ell+1}\epsilon}. \end{cases}$$

本文余下内容的结构如下: 第 2 节简要介绍将要在后面几节用到的符号与结果, 第 3 节证明定理 1.1, 第 4 节证明定理 1.2, 第 5 节证明定理 1.3, 第 6 节证明定理 1.4, 第 7 节总结全文.

2 预备知识

关于明确译码、最大似然译码和列表译码这三大译码原则, 三个相关函数 $P_d(C, \ell, \epsilon)$ 、 $P_{\text{mld}}(C, \epsilon)$ 和 $P_{\text{ud}}(C, \epsilon)$ 的计算, 以及它们与线性码的 q^ℓ -不可纠错集的概念之间的联系等, 文献 [7, II. 引言] 给出了非常详尽的介绍, 在此不再赘述. 我们关注于介绍与本文中的证明推导直接相关的一些结果.

2.1 Gauss 二项式系数

对任意整数 $n \geq k \geq 0$, Gauss 二项式系数 $\begin{bmatrix} n \\ k \end{bmatrix}_q$ 定义为

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q)_n}{(q)_k (q)_{n-k}},$$

其中 $(q)_n := \prod_{i=1}^n (1 - q^i)$. 我们约定: 如果 $n \geq 0$, 则 $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$; 如果 $k < 0$ 或者 $k > n$, 则 $\begin{bmatrix} n \\ k \end{bmatrix}_q = 0$. 已知 $\begin{bmatrix} n \\ k \end{bmatrix}_q$ 有如下的组合解释 (参见文献 [9, 第 444 页]):

引理 2.1 $\begin{bmatrix} n \\ k \end{bmatrix}_q$ 是 $\mathbb{F}_q$ 上一个 n -维的向量空间所包含的所有 k -维子空间的个数.

Gauss 二项式系数满足如下的性质:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q, \quad \forall n \geq k \geq 0$$

以及恒等式 (参见文献 [9, 第 444 页])

$$\prod_{i=0}^{n-1} (1 + q^i x) = \sum_{i=0}^n \begin{bmatrix} n \\ i \end{bmatrix}_q q^{i(i-1)/2} x^i, \quad \forall n \geq 1. \quad (2.1)$$

2.2 r -次支撑重量分布

设 C 为一个 $[n, k]_q$ 线性码. 对于一个码字 $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$, $\mathbf{c}$ 的支撑定义为如下集合:

$$\text{supp}(\mathbf{c}) = \{i \in [n] : c_i \neq 0\},$$

其中 $[n]$ 代表集合 $\{1, 2, \dots, n\}$. 对于 C 的任意子集 D , 其支撑定义为

$$\text{supp}(D) = \bigcup_{\mathbf{c} \in D} \text{supp}(\mathbf{c}).$$

D 的支撑重量 $\text{wt}(D)$ 定义为 $\#(\text{supp}(D))$, 即集合 $\text{supp}(D)$ 的元素个数.

对任意的 $r = 1, 2, \dots, k$, 设 $A_i^{(r)}$ 为 C 的支撑重量为 i 的所有 r -维线性子码的数量. 相应的单项式 $W^{(r)}(x)$ (见 (1.5)) 被称为 C 的 r -次支撑重量单项式, 集合 $\{A_i^{(r)}\}_{i=1}^n$ 被称为 C 的 r -次支撑重量分布.

C 的 r -次支撑重量分布是线性码 C 的一族基本参数, 非常重要. 特别地, C 的 r -次广义 Hamming 重量定义为 $d_r = \min\{i > 0 : A_i^{(r)} \neq 0\}$, 集合 $\{d_1, d_2, \dots, d_r\}$ 被称为 C 的重量阶层集 (weight hierarchy). 众所周知, d_1 是 C 的极小 Hamming 距离, C 的广义 Hamming 重量满足关系 $d_1 < d_2 < \dots < d_k$ (参见文献 [10]). 因为它们在密码中有重要应用, 所以在文献中可以找到很多关于线性码的 r -次广义 Hamming 重量和重量阶层集的研究结果 (参见文献 [10–16]).

3 定理 1.1 的证明

设 C 是一个 $[n, k]_q$ 线性码, $\{A_i^{(r)}\}_{i=1}^n$ 是其 r -次支撑重量分布, 其中 $1 \leq r \leq k$. 对于 $r \geq 1$, 为了行文方便, 定义 $A_0^{(r)} = 0$. 设 $\{I_i^\ell\}_{i=1}^n$ 为 C 的 q^ℓ -不可纠正集分布, 且 $\{I_i\}_{i=1}^n$ 为 C 的不可纠正集分布. 文献 [7] 证明了如下结果:

$$I_i^\ell = \sum_{r=\ell+1}^k \sum_{j=r-\ell}^r (-1)^{j-1} q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q F_i^{(r)}, \quad (3.1)$$

$$I_i = \sum_{r=1}^k (-1)^{r-1} q^{r(r-1)/2} F_i^{(r)}, \quad (3.2)$$

其中 $F_i^{(r)}$ 是 C 的 r -阶广义二项式的动差, 定义为

$$F_i^{(r)} = \sum_{j=0}^n \binom{n-j}{n-i} A_j^{(r)}.$$

另外, 文献 [7] 显示这三个译码错误概率函数 $P_{\text{ud}}(C, \epsilon)$ 、 $P_{\text{ld}}(C, \ell, \epsilon)$ 和 $P_{\text{mld}}(C, \epsilon)$ 都可以用 I_i^ℓ 和 I_i 表达:

$$P_{\text{ud}}(C, \epsilon) = \sum_{i=1}^n I_i \epsilon^i (1 - \epsilon)^{n-i}, \quad (3.3)$$

$$P_{\text{ld}}(C, \ell, \epsilon) = \sum_{i=1}^n I_i^\ell \epsilon^i (1 - \epsilon)^{n-i}, \quad (3.4)$$

$$P_{\text{mld}}(C, \epsilon) = \sum_{i=1}^n \sum_{\ell=1}^k (I_i^{\ell-1} - I_i^\ell) (1 - q^{-\ell}) \epsilon^i (1 - \epsilon)^{n-i}. \quad (3.5)$$

将以上 (3.1) 和 (3.2) 代入 (3.3)–(3.5) 中, 即可得到文献 [7] 的一个主要结果 (参见文献 [7, 定理 1]). 这里用同样的策略, 只是计算更为仔细.

3.1 $P_{\text{ud}}(C, \epsilon)$ 和 $P_{\text{ld}}(C, \ell, \epsilon)$ 的计算

由 (3.2) 和二项式定理 $(1+x)^n = \sum_{i=0}^n \binom{n}{i} x^i$, 可以得到 C 的不可纠错集分布如下:

$$\sum_{i=1}^n I_i x^i = \sum_{r=1}^k (-1)^{r-1} q^{r(r-1)/2} \sum_{j=1}^n A_j^{(r)} x^j (1+x)^{n-j}.$$

这个结果由 (1.3) 可以很快得到.

类似地, 由 (3.1) 可以得到

$$\sum_{i=1}^n I_i^\ell x^i = \sum_{r=\ell+1}^k \sum_{j=r-\ell}^r (-1)^{j-1} q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q \sum_{t=1}^n A_t^{(r)} x^t (1+x)^{n-t}.$$

这个结果由 (1.1) 也可以很快得到.

3.2 $P_{\text{mld}}(C, \epsilon)$

由 (3.5) 可以得到

$$P_{\text{mld}}(C, \epsilon) = \sum_{\ell=1}^k (1 - q^{-\ell})(P_{\text{ld}}(C, \ell - 1, \epsilon) - P_{\text{ld}}(C, \ell, \epsilon)). \quad (3.6)$$

定义 $a_{\ell} := P_{\text{ld}}(C, \ell - 1, \epsilon) - P_{\text{ld}}(C, \ell, \epsilon)$ 以及利用 (1.1), 可以得到

$$\begin{aligned} a_{\ell} &= \sum_{r=\ell}^k \sum_{j=r-\ell+1}^r (-1)^{j-1} q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q W^{(r)}(\epsilon) - \sum_{r=\ell+1}^k \sum_{j=r-\ell}^r (-1)^{j-1} q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q W^{(r)}(\epsilon) \\ &= \sum_{j=1}^{\ell} (-1)^{j-1} q^{j(j-1)/2} \begin{bmatrix} \ell \\ j \end{bmatrix}_q W^{(\ell)}(\epsilon) + \sum_{r=\ell+1}^k (-1)^{r-\ell} q^{(r-\ell)(r-\ell-1)/2} \begin{bmatrix} r \\ \ell \end{bmatrix}_q W^{(r)}(\epsilon). \end{aligned} \quad (3.7)$$

运用恒等式

$$\sum_{j=0}^n (-1)^j q^{j(j-1)/2} \begin{bmatrix} n \\ j \end{bmatrix}_q = 0, \quad \forall n \geq 0 \quad (3.8)$$

于 (3.7) 的右边的第一项 (这个恒等式可以通过将 $x = -1$ 代入 (2.1) 中而得到), 得到

$$a_{\ell} = \sum_{r=\ell}^k (-1)^{r-\ell} q^{(r-\ell)(r-\ell-1)/2} \begin{bmatrix} r \\ r-\ell \end{bmatrix}_q W^{(r)}(\epsilon).$$

将上式代入 (3.6), 可得

$$P_{\text{mld}}(C, \epsilon) = \sum_{r=1}^k W^{(r)}(\epsilon) \sum_{\ell=0}^r (1 - q^{-\ell})(-1)^{r-\ell} q^{(r-\ell)(r-\ell-1)/2} \begin{bmatrix} r \\ r-\ell \end{bmatrix}_q.$$

注意在此添加了一项对应于 $\ell = 0$, 这是没有问题的, 因为对应的因子 $1 - q^{-\ell} = 0$. 再一次利用 (3.8) 和恒等式

$$\sum_{\ell=0}^r q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q (-q)^j = (q)_r = \prod_{i=1}^r (1 - q^i)$$

(这个恒等式可以通过将 $x = -q$ 代入 (2.1) 中得到), 于是可得

$$\begin{aligned} P_{\text{mld}}(C, \epsilon) &= \sum_{r=1}^k W^{(r)}(\epsilon) \sum_{\ell=0}^r q^{-\ell} (-1)^{r-\ell+1} q^{(r-\ell)(r-\ell-1)/2} \begin{bmatrix} r \\ r-\ell \end{bmatrix}_q \\ &= \sum_{r=1}^k W^{(r)}(\epsilon) q^{-r} (-1) \sum_{\ell=0}^r q^{j(j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix}_q (-q)^j \\ &= - \sum_{r=1}^k W^{(r)}(\epsilon) q^{-r} (q)_r. \end{aligned}$$

注意到 $(q)_r = (-1)^r q^{r(r+1)/2} (T)_r$, 由此可以得到定理 1.1 中的 (1.2). 至此完成了定理 1.1 的证明.

4 定理 1.2 的证明

为了证明定理 1.2, 我们直接计算 $A_i^{(r)}(\mathcal{C})$. 回顾引理 2.1 提到 $[n]_q$ 是 $\mathbb{F}_q$ 上一个 n -维向量空间中包含的所有 k -维子空间的数目. 对于任意的 $1 \leq t \leq n$, 定义

$$h_r := \begin{bmatrix} n \\ k \end{bmatrix}_q \cdot A_t^{(r)}(\mathcal{C}), \quad (4.1)$$

由此得到

$$h_r = \sum_{C \in \mathcal{C}} \sum_{\substack{V \subset C \\ \dim V = r \\ \text{wt}(V) = t}} 1 = \sum_{\substack{V \subset \mathbb{F}_q^n \\ \dim V = r \\ \text{wt}(V) = t}} \sum_{\substack{V \subset C \subset \mathbb{F}_q^n \\ \dim C = k}} 1.$$

注意在上式中, $V \subset C \subset \mathbb{F}_q^n$ 当且仅当 $C/V \subset \mathbb{F}_q^n/V$, 其中 $\dim C/V = k - r$, $\dim \mathbb{F}_q^n/V = n - r$, 于是由引理 2.1 得到

$$h_r = \begin{bmatrix} n - r \\ k - r \end{bmatrix}_q \sum_{\substack{V \subset \mathbb{F}_q^n \\ \dim V = r \\ \text{wt}(V) = t}} 1 = \begin{bmatrix} n - r \\ k - r \end{bmatrix}_q \sum_{\substack{T \subset [n] \\ \#T = t}} \sum_{\substack{V \subset \mathbb{F}_q^n \\ \dim V = r \\ \text{supp}(V) = T}} 1.$$

对于任意的子空间 $V \subset \mathbb{F}_q^n$, 条件 $\text{supp}(V) = T$ 意味着对任意的 $\mathbf{v} = (v_1, v_2, \dots, v_n) \in V$, 它满足如下性质: 对任意的 $i \in [n] \setminus T$, 有 $v_i = 0$. 所以为计算所有如此的子空间的数目, 我们可以忽略包含于集合 T 中的坐标而仅计算包含于 $\mathbb{F}_q^t$ 中的如此的子空间. 因此我们得到

$$\sum_{\substack{V \subset \mathbb{F}_q^n \\ \dim V = r \\ \text{supp}(V) = T}} 1 = \sum_{\substack{V \subset \mathbb{F}_q^t \\ \dim V = r \\ \text{wt}(V) = t}} 1 = \begin{bmatrix} t \\ r \end{bmatrix}_q - \sum_{\substack{V \subset \mathbb{F}_q^t \\ \dim V = r \\ \text{wt}(V) \leq t-1}} 1. \quad (4.2)$$

我们可以用容斥原理 (4.2) 来计算上式的第二项.

对任意坐标子集 $E \subset [t]$, 记 $H(E)$ 为所有满足如下条件的 r -维子空间 $V \subset \mathbb{F}_q^t$ 的集合:

$$\forall \mathbf{v} = (v_1, v_2, \dots, v_t) \in V \implies v_i = 0, \quad \forall i \in E.$$

记 $h(E)$ 为集合 $H(E)$ 的元素的个数. 容易看到, 如果 $\#E = \ell$, 那么 $h(E) = [t - \ell]_q$. 由容斥原理得到

$$\sum_{\substack{V \subset \mathbb{F}_q^t \\ \dim V = r \\ \text{wt}(V) \leq t-1}} 1 = \# \left(\bigcup_{i \in [t]} H(\{i\}) \right) = \sum_{\emptyset \neq E \subset [t]} (-1)^{\#E+1} h(E).$$

以上表明

$$\sum_{\substack{V \subset \mathbb{F}_q^t \\ \dim V = r \\ \text{wt}(V) \leq t-1}} 1 = \sum_{i=1}^t (-1)^{i+1} \begin{bmatrix} t \\ i \end{bmatrix}_q \begin{bmatrix} t-i \\ r \end{bmatrix}_q.$$

回到 (4.2) 和 (4.1), 可得

$$A_t^{(r)}(\mathcal{C}) = \frac{\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \binom{n}{t} \sum_{s=0}^t (-1)^s \binom{t}{s} \begin{bmatrix} t-s \\ r \end{bmatrix}_q.$$

由上式可以直接得到定理 1.2. 于是完成了定理 1.2 的证明.

5 定理 1.3 的证明

设 $\mathcal{C}_n$ 为所有 $[n, nR]_q$ 线性码的集合, 其中 $0 < R < 1$. 定义

$$P_{\text{mld}}(\mathcal{C}_n, \epsilon) := \frac{1}{\#\mathcal{C}_n} \sum_{C \in \mathcal{C}_n} P_{\text{mld}}(C, \epsilon),$$

其中 $P_{\text{mld}}(C, \epsilon)$ 是线性码 C 基于最大似然译码原则下的译码错误概率. 文献 [7, 定理 2] 表明

$$P_{\text{mld}}(\mathcal{C}_n, \epsilon) = \sum_{i=1}^n \sum_{\ell=1}^k \frac{q^{(i-\ell)(k-\ell)} \begin{bmatrix} i \\ \ell \end{bmatrix}_q \begin{bmatrix} n-i \\ k-\ell \end{bmatrix}_q (1-q^{-\ell})}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}.$$

其错误指数定义如下:

$$T(\epsilon) = \lim_{n \rightarrow \infty} -\frac{1}{n} \log_q P_{\text{mld}}(\mathcal{C}_n, \epsilon),$$

如果以上的极限存在 (参见文献 [7, 17, 18]). 现在计算上式中的极限.

定义

$$f_{i,\ell} := \frac{q^{(i-\ell)(k-\ell)} \begin{bmatrix} i \\ \ell \end{bmatrix}_q \begin{bmatrix} n-i \\ k-\ell \end{bmatrix}_q (1-q^{-\ell})}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}.$$

容易看出, 对于任意的整数 i 和 ℓ , $f_{i,\ell}$ 总是非负的; 另外, $f_{i,\ell} \neq 0$ 当且仅当 $1 \leq i \leq n$, $1 \leq \ell \leq k$ 以及 $k-\ell \leq n-i$, 即得到

$$P_{\text{mld}}(\mathcal{C}_n, \epsilon) = \sum_{i,\ell} f_{i,\ell},$$

其中下标 i 和 ℓ 代表满足以下性质的整数:

$$1 \leq i \leq n, \quad \max\{1, k+i-n\} \leq \ell \leq k. \quad (5.1)$$

设

$$F = \max_{i,\ell} f_{i,\ell} > 0,$$

其中下标 i 和 ℓ 总是代表满足条件 (5.1) 的整数, 我们可以得到

$$F \leq P_{\text{mld}}(\mathcal{C}_n, \epsilon) \leq nkF.$$

因为 $k = Rn$ 和 $\lim_{n \rightarrow \infty} \frac{\log_q(nk)}{n} = 0$, 所以可得

$$h_n(\epsilon) := \frac{1}{n} \log_q P_{\text{mld}}(\mathcal{C}_n, \epsilon) = o(1) + \frac{1}{n} \max_{i,\ell} \log_q f_{i,\ell}, \quad \text{当 } n \rightarrow \infty \text{ 时}. \quad (5.2)$$

现在研究 $f_{i,\ell}$. 设 $T = q^{-1}$, 于是 $0 < T < 1$. 对任意的整数 $m \geq j \geq 0$, 容易验证

$$\begin{bmatrix} m \\ j \end{bmatrix}_q = q^{j(m-j)} \begin{bmatrix} m \\ j \end{bmatrix}_T.$$

我们可以将 $f_{i,\ell}$ 写为

$$f_{i,\ell} = q^{-\ell(n-k-i+\ell)} \frac{(1-T^\ell)^{[i]_T} [k-\ell]_T^{[n-i]_T}}{[n]_T} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}.$$

注意无穷级数

$$(T)_\infty = \prod_{i=1}^{\infty} (1-T^i)$$

收敛于一个正实数, 这个数完全依赖于 q , 以及对任意的非负整数 m , 有

$$1 \geq (T)_m := \prod_{i=1}^m (1-T^i) > M = (T)_\infty.$$

因此对于任意的整数 $m \geq j \geq 0$, 有

$$M \leq \begin{bmatrix} m \\ j \end{bmatrix}_T = \frac{(T)_m}{(T)_j (T)_{m-j}} \leq \frac{1}{M^2}.$$

这表明对于任意的 $m \geq j \geq 0$, 量 $\log_q \begin{bmatrix} m \\ j \end{bmatrix}_T$ 是绝对有界的. 量 $\log_q(1-T^\ell)$ 也介于 0 与 $\log_q(1-T)$ 之间. 所以当 $n \rightarrow \infty$ 时,

$$\frac{1}{n} \log_q f_{i,\ell} = \frac{-\ell(n-k-i+\ell)}{n} + \frac{1}{n} \log_q \binom{n}{i} + \frac{1}{n} \log_q \epsilon^i (1-\epsilon)^{n-i} + o(1).$$

现在需要寻找到满足于条件 (5.1) 的 i 和 ℓ 使得上式取最大值. 我们的策略是先固定 i , 然后考虑什么样的满足条件 (5.1) 的 ℓ 使得 $\frac{1}{n} \log_q f_{i,\ell}$ 最大. 有两种情形:

情形 1 如果 $n-k-i \geq 0$, 显然可见, 应取 $\ell = 1$ 使得值 $\frac{1}{n} \log_q f_{i,\ell}$ 最大;

情形 2 如果 $n-k-i < 0$, 因为对于任意满足 (5.1) 的 ℓ 总有 $\ell(n-k-i+\ell) \geq 0$, 所以当 $\ell = k+i-n$ 时, 值 $\frac{1}{n} \log_q f_{i,\ell}$ 是最大的.

综合以上的考虑, 得到

$$\frac{1}{n} \max_{i,\ell} \log_q f_{i,\ell} = o(1) + \max \left\{ \max_{n-k-i \geq 0} \{F(i)\}, \max_{n-k-i < 0} \{G(i)\} \right\},$$

其中

$$F(i) = \frac{-(n-k-i)}{n} + \frac{1}{n} \log_q \binom{n}{i} + \frac{1}{n} \log_q \epsilon^i (1-\epsilon)^{n-i},$$

$$G(i) = \frac{1}{n} \log_q \binom{n}{i} + \frac{1}{n} \log_q \epsilon^i (1-\epsilon)^{n-i}.$$

将 $k = Rn$ 和 $i = tn$ (其中 $0 \leq t \leq 1$) 代入以上两式, 注意到 (参见文献 [7, 引理 3] 和 [9])

$$\frac{1}{n} \log_q \binom{n}{tn} = h(t) + o(1),$$

其中

$$h(t) = -t \log_q t - (1-t) \log_q (1-t)$$

是 q - 元熵函数, 我们得到

$$h_n(\epsilon) = o(1) + \max \left\{ \max_{0 < t \leq 1-R} (R-1+t+g(t)), \max_{1-R < t \leq 1} g(t) \right\}, \quad (5.3)$$

这里函数 $g(t)$ 定义为

$$g(t) = h(t) + t \log_q \epsilon + (1-t) \log_q (1-\epsilon).$$

余下的分析与文献 [7] 类似: 对函数取一阶导数, 我们可以发现函数 $g(t)$ 和 $t+g(t)$ 在区间 $[0, 1]$ 中取值表现非常简单: 函数 $g(t)$ 在区间 $(0, \epsilon]$ 严格递增, 然后在区间 $[\epsilon, 1)$ 严格递减; 函数 $t+g(t)$ 在区间 $(0, t_0]$ 严格递增, 然后在区间 $[t_0, 1)$ 严格递减, 其中 $t_0 := \frac{q\epsilon}{1-\epsilon+q\epsilon}$. 运用以上性质, 可以得到 (5.3) 右边的最大值.

事实上我们不需要如此做: 仔细阅读文献 [7] 我们发现, 这些函数与在文献 [7] 中出现的用于计算基于明确译码原则下随机 $[n, nR]_q$ 线性码的非成功译码概率的错误指数完全相同, 只是我们的符号稍微有些不一样. 感兴趣的读者可以对比式 (5.3) 与文献 [7, (74) 和 (75) 式], 特别需要注意

$$T(\epsilon) = - \lim_{n \rightarrow \infty} h_n(\epsilon).$$

这表明我们所需要计算的错误指数与已经得到的文献 [7, 定理 3] 是完全一样的. 如此便证明了定理 1.3.

6 定理 1.4 的证明

设 $\mathcal{C}_n$ 为所有 $[n, nR]_q$ 线性码的集合, 其中 $0 < R < 1$. 对任意的非负整数 ℓ , 定义

$$P_{\text{ld}}(\mathcal{C}_n, \ell, \epsilon) := \frac{1}{\#\mathcal{C}_n} \sum_{C \in \mathcal{C}_n} P_{\text{ld}}(C, \ell, \epsilon),$$

其中 $P_{\text{ld}}(C, \ell, \epsilon)$ 是线性码 C 基于 q^ℓ - 列表译码原则下的非成功译码概率, 其一般的表达式可以参见 (3.4). 记

$$I_i^\ell := \sum_{C \in \mathcal{C}_n} I_i^\ell(C)$$

以及

$$\lambda_\ell^{(i)} = I_i^{\ell-1} - I_i^\ell = \sum_{C \in \mathcal{C}_n} \sum_{\substack{E \subset [n] \\ \#E=i \\ \dim C(E)=\ell}} 1.$$

文献 [7, 定理 2] 的证明给出了以下的公式:

$$\lambda_\ell^{(i)} = q^{(i-\ell)(k-\ell)} \begin{bmatrix} i \\ \ell \end{bmatrix}_q \begin{bmatrix} n-i \\ k-\ell \end{bmatrix}_q, \quad \forall 0 \leq \ell \leq k.$$

由此可以得到

$$I_i^\ell = \sum_{j=\ell+1}^k \lambda_j^{(i)}, \quad \forall 0 \leq \ell \leq k.$$

如此, 我们得到

$$P_{\text{ld}}(\mathcal{C}_n, \ell, \epsilon) = \sum_{i=1}^n \sum_{j=\ell+1}^k \frac{q^{(i-j)(k-j)} \begin{bmatrix} i \\ j \end{bmatrix}_q \begin{bmatrix} n-i \\ k-j \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}.$$

其错误指数定义为

$$T(\epsilon) = \lim_{n \rightarrow \infty} -\frac{1}{n} \log_q P_{\text{mld}}(\mathcal{C}_n, \epsilon),$$

如果以上的极限存在 (参见文献 [7, 17, 18]). 现在计算上式中的极限. 证明的方法与第 5 节类似.

定义

$$f_{i,j} := \frac{q^{(i-j)(k-j)} \begin{bmatrix} i \\ j \end{bmatrix}_q \begin{bmatrix} n-i \\ k-j \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}.$$

容易看出, 对于任意的整数 i 和 j , $f_{i,j}$ 总是非负的; 另外, $f_{i,j} \neq 0$ 当且仅当 $1 \leq i \leq n$, $\ell+1 \leq j \leq k$, $0 \leq j \leq i$ 以及 $k+i-n \leq j \leq k$, 即得到

$$P_{\text{ld}}(\mathcal{C}_n, \ell, \epsilon) = \sum_{i,j} f_{i,j},$$

其中下标 i 和 j 代表满足以下性质的整数:

$$1 \leq i \leq n, \quad \max\{\ell+1, k+i-n\} \leq j \leq \min\{k, i\}. \quad (6.1)$$

设

$$F = \max_{i,j} f_{i,j} > 0,$$

其中下标 i 和 j 总是代表满足条件 (6.1) 的整数, 则可以得到

$$F \leq P_{\text{ld}}(\mathcal{C}_n, \ell, \epsilon) \leq nkF.$$

因为 $k = Rn$ 和 $\lim_{n \rightarrow \infty} \frac{\log_q(nk)}{n} = 0$, 所以可以得到

$$h_n(\epsilon) := \frac{1}{n} \log_q P_{\text{ld}}(\mathcal{C}_n, \ell, \epsilon) = o(1) + \frac{1}{n} \max_{i,j} \log_q f_{i,j}, \quad \text{当 } n \rightarrow \infty \text{ 时}. \quad (6.2)$$

类似地, 设 $T = q^{-1}$, 我们得到

$$f_{i,j} = q^{-j(n-k-i+j)} \frac{\begin{bmatrix} i \\ j \end{bmatrix}_T \begin{bmatrix} n-i \\ k-j \end{bmatrix}_T}{\begin{bmatrix} n \\ k \end{bmatrix}_T} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}.$$

注意到

$$\frac{1}{n} \log_q \frac{[j]_T [k-j]_T^{n-i}}{[k]_T} = o(1),$$

由此得到

$$\frac{1}{n} \log_q f_{i,j} = \frac{-j(n-k-i+j)}{n} + \frac{1}{n} \log_q \binom{n}{i} + \frac{1}{n} \log_q \epsilon^i (1-\epsilon)^{n-i} + o(1).$$

现在需要寻找到满足于条件 (6.1) 的 i 和 j 使得上式取最大值. 我们的策略仍然是先固定 i , 然后考虑什么样的满足条件 (6.1) 的 j 使得 $\frac{1}{n} \log_q f_{i,j}$ 最大. 有如下两种情形:

情形 1 如果 $n-k-i \geq 0$, 因为 $\ell+1 \leq j \leq \min\{k, i\}$, 显然可见, 我们应取 $j = \ell+1$ 使得值 $\frac{1}{n} \log_q f_{i,j}$ 最大.

情形 2 如果 $n-k-i < 0$, 因为 $\ell+1 \leq j \leq \min\{k, i\}$, 这里又分两种子情形. 如果 $j \geq \ell+1 > k$ 且 $j \geq \ell+1 > k$, 那么 $j = \ell+1$ 将使值 $\frac{1}{n} \log_q f_{i,\ell}$ 最大; 如果 $\ell+1 \leq k+i-n$, 那么取 $j = k+i-n$.

综合以上的考虑, 我们得到

$$h_n(\epsilon) = o(1) + \max \left\{ \max_{\substack{1 \leq i \leq n-k \\ \ell+1 \leq \min\{k, i\}}} G_1(i), \max_{\substack{n-k < i \leq n \\ \min\{k, i\} \geq \ell+1 > k+i-n}} G_1(i), \max_{\substack{n-k < i \leq n \\ \ell+1 \leq k+i-n \leq \min\{k, i\}}} G_2(i) \right\},$$

其中

$$G_1(i) = \frac{-(\ell+1)(n-k-i+\ell+1)}{n} + \frac{1}{n} \log_q \binom{n}{i} + \frac{1}{n} \log_q \epsilon^i (1-\epsilon)^{n-i},$$

$$G_2(i) = \frac{1}{n} \log_q \binom{n}{i} + \frac{1}{n} \log_q \epsilon^i (1-\epsilon)^{n-i}.$$

将 $k = Rn$ 和 $i = tn$ (其中 $0 \leq t \leq 1$) 代入以上两式, 注意到 (参见文献 [7, 引理 3] 和 [9])

$$\frac{1}{n} \log_q \binom{n}{tn} = h(t) + o(1),$$

其中

$$h(t) = -t \log_q t - (1-t) \log_q (1-t)$$

是 q - 元熵函数, $l \geq 0$ 是固定的, $n \rightarrow \infty$, 我们可以得到

$$h_n(\epsilon) = o(1) + \max \left\{ \max_{0 < t \leq 1-R} (-(\ell+1)(1-R-t) + g(t)), \max_{1-R < t \leq 1} g(t) \right\}, \quad (6.3)$$

这里函数 $g(t)$ 定义为

$$g(t) = h(t) + t \log_q \epsilon + (1-t) \log_q (1-\epsilon).$$

余下的分析与文献 [7, 定理 3] 的证明完全类似 (注意文献 [7, 定理 3] 和 (5.3) 所对应的是以上 $\ell = 0$ 的情形). 对函数取一阶导数, 我们可以发现函数 $g(t)$ 和 $-(\ell+1)(1-R-t) + g(t)$ 在区间 $[0, 1]$ 中取值表现

非常简单: 函数 $g(t)$ 在区间 $(0, \epsilon]$ 严格递增, 然后在区间 $[\epsilon, 1)$ 严格递减; 函数 $-(\ell+1)(1-R-t)+g(t)$ 在区间 $(0, t_0]$ 严格递增, 然后在区间 $[t_0, 1)$ 严格递减, 其中

$$t_0 := \frac{q^{\ell+1}\epsilon}{1-\epsilon+q^{\ell+1}\epsilon}.$$

运用以上性质, 我们可以得到 (6.3) 右边的最大值. 经过整理, 我们得到了定理 1.4. 如此完成了定理 1.4 的证明.

7 结论

本文研究了线性码在擦除信道中基于三种译码原则的译码错误概率, 得到如下新的结果:

- (1) 简化了文献 [7] 中所得到的显式表达式, 显示其与线性码的 r -次支撑重量分布的更为直接的关系;
- (2) 计算了 $[n, k]_q$ 线性码的 r -次支撑重量分布的平均值;
- (3) 计算了随机 $[n, nR]_q$ 线性码基于最大似然译码原则下的译码错误概率的错误指数. 这解决了文献 [7] 中遗留的一个公开问题.
- (4) 计算了随机 $[n, nR]_q$ 线性码基于列表译码原则下的非成功译码概率的错误指数.

参考文献

- 1 Cover T M, Thomas J A. Elements of Information Theory. New York: John Wiley & Sons, 1991
- 2 Byers J W, Luby M, Mitzenmacher M, et al. A digital fountain approach to reliable distribution of bulk data. In: ACM SIGCOMM (Special Interest Group on Data Communication) Computer Communication Review, vol. 28. 1998, 56–67
- 3 Luby M, Mitzenmacher M, Shokrollahi A, et al. Practical loss-resilient codes. In: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing. New York: ACM, 1997, 150–159
- 4 Lun D S, Médard M, Koetter R, et al. On coding for reliable communication over packet networks. Phys Commun, 2008, 1: 3–20
- 5 Didier F. A new upper bound on the block error probability after decoding over the erasure channel. IEEE Trans Inform Theory, 2006, 52: 4496–4503
- 6 Lemes L C, Firer M. Generalized weights and bounds for error probability over erasure channels. In: Proceedings of the 2014 Information Theory and Applications Workshop (ITA). San Diego: IEEE, 2014, 1–8
- 7 Shen L Z, Fu F W. The decoding error probability of linear codes over the erasure channel. IEEE Trans Inform Theory, 2019, 65: 6194–6203
- 8 Weber J H, Abdel-Ghaffar K A S. Results on parity-check matrices with optimal stopping and/or dead-end set enumerators. IEEE Trans Inform Theory, 2008, 54: 1368–1374
- 9 MacWilliams F J, Sloane J J A. The Theory of Error-Correcting Codes, I and II. North-Holland Mathematical Library, vol. 16. Amsterdam: Elsevier, 1988
- 10 Wei V K. Generalized Hamming weights for linear codes. IEEE Trans Inform Theory, 1991, 37: 1412–1418
- 11 Britz D, Britz T, Shiromoto K, et al. The higher weight enumerators of the doubly-even, self-dual $[48, 24, 12]$ code. IEEE Trans Inform Theory, 2007, 53: 2567–2571
- 12 Dougherty S T, Gulliver T A, Ours M. Higher weights and graded rings for binary self-dual codes. Discrete Appl Math, 2003, 128: 121–143
- 13 Li S. The weight hierarchy of a family of cyclic codes with arbitrary number of nonzeros. Finite Fields Appl, 2017, 45: 355–371
- 14 Ozarow L H, Wyner A D. Wire-tap channel II. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 209. Berlin: Springer, 1985, 33–50

- 15 Schaathun H G. The weight hierarchy of product codes. IEEE Trans Inform Theory, 2000, 46: 2648–2651
- 16 Xiong M, Li S, Ge G. The weight hierarchy of some reducible cyclic codes. IEEE Trans Inform Theory, 2016, 62: 4071–4080
- 17 Gallager R G. Information Theory and Reliable Communication. New York: John Wiley & Sons, 1968
- 18 Viterbi A J, Omura J K. Principles of Digital Communication and Coding. New York: McGraw-Hill, 1979

Decoding error probability in the erasure channel and the r -th support weight distribution

Maosheng Xiong

Abstract Inspired by a recent work of Shen and Fu (2019), we study the decoding error probability of linear codes over the erasure channel under three decoding principles. We first simplify the explicit formulas obtained by Shen and Fu (2019), showing a much more direct relation to the r -th support weight distribution of linear codes. Then we compute the average r -th support weight distribution of $[n, k]_q$ linear codes. We resolve an open question of Shen and Fu (2019) concerning the error exponent of the average unsuccessful decoding probability under maximum likelihood decoding for random $[n, nR]_q$ linear codes. We also obtain the error exponent of the average unsuccessful decoding probability for random $[n, nR]_q$ linear codes under list decoding.

Keywords erasure channel, linear code, unsuccessful decoding probability, error exponent

MSC(2020) 94B05, 94B70

doi: 10.1360/SSM-2021-0019