关于 t-Lee纠错码的数量

Nadja Willenborg[1], 、Anna-Lena Horlemann[1],和 Violetta Weger[2]

[1]瑞士圣加仑大学[2]德国慕尼黑工业大学

摘要

我们研究残数环 $\mathbb{Z}_m$ 上长度为 n 的 t-Lee纠错码，并确定 t-Lee纠错码数量的上界和下界。我们采用两种不同的方法，即估算二分图中的孤立节点，以及图容器方法。前者给出固定大小码的密度结果，后者则适用于任意大小的码。这证实了近期关于线性 Lee 度量码的一些密度结果，并为非线性码提供了新的密度结果。为应用图容器算法的一种变体，我们还研究了 Lee 度量中球的一些几何性质。

1 引言

编码理论中的一个经典研究方向是研究随机码的性质，并计算相对于某些界而言最优码的密度。对于 $\mathbb{F}_q$ 上的汉明度量码，我们已经有若干著名结果，例如 [8, 31], ，其中作者证明，当我们令长度 n 增大时，随机码以高概率达到吉尔伯特–瓦尔沙莫夫界[19, 39]。另一方面，众所周知，当我们令 q 增大时，随机码以高概率是最大距离可分（MDS）码，即达到 Singleton 界。在秩度量中也得到了类似结果，即当 n 增大时，随机秩度量码达到秩度量吉尔伯特–瓦尔沙莫夫界 [28] ；我们还知道，最大秩距码（MRD 码）的密度取决于它们是 $\mathbb{F}_{q^m}$-线性的还是 $\mathbb{F}_q$-线性的。对于前者， [29] 中证明了 MRD 码是稠密的；而对于后者，已证明 MRD 码既不稠密也不稀疏 [3, 12, 20, 23]。在本文中，我们将在一个新的框架下研究这类问题：赋予 Lee 度量的整数剩余环上的模。Lee 度量最初是为处理相位调制、受限存储器中的纠错或密码学应用而提出的（例如参见 [32]）。关于 $\mathbb{Z}_{p^s}^n$ 中这类 Lee 度量码的密度问题已经在 [11, 13] 中进行了研究。特别地，研究表明，当 n 增大时，随机码以高概率达到相应的吉尔伯特–瓦尔沙莫夫界，并且相对于 Lee 度量 Singleton 界[35, 2] 的最优线性码是稀疏的，无论 n， s 还是 p 增大。对于相对于 Lee 度量 Plotkin 界的最优线性码，也已证明其是稀疏的。在本文中，我们将确认这些结果，并运用图论中的技术获得关于非线性码的新结果。

我们考虑两种不同的技术：二分图和容器方法。前一种技术基于对某些二分图中非孤立节点数量的界进行估计，这些二分图的右侧节点集由 $\mathbb{Z}_m^n$ 中基数为 S 的码组成，左侧节点集则包含来自 $\mathbb{Z}_m^n$ 的元素，且其最小重量有上界。通过这种方法，我们首先推导出 Lee 度量码密度的上界和下界。随后，这些界给出了非线性情形下的渐近结果，而这一情形此前尚未得到研究。

第二种技术使用图 $G = (V, E)$，其节点集为 $V = \mathbb{Z}_m^n$ ，边集为 $E = \{(x, y) \in \mathbb{Z}_m^n \times \mathbb{Z}_m^n : x \neq y, d^{\mathrm{L}}(x, y) \leq 2t\}$，其中 $d^{\mathrm{L}}(x, y)$ 是 x 与 y 之间的 Lee 距离。注意， G 也是笛卡尔积 $C_m \square C_m \square \cdots \square C_m$ 的 $2t$ 图幂，其中

C_m 是长度为 m的环。该笛卡尔积的节点集为 $\mathbb{Z}_m^n$ ，当且仅当 x， $y \in \mathbb{Z}_m^n$ 之间的 Lee 距离为 1 时，它们之间存在一条边，另见 [1, 25]。我们证明，对于固定的 m，长度为 n 的 t-Lee 纠错码的数量至多为$2^{(1+o(1))H_m(n,\ t)}$，对所有 $t \le 10\sqrt{\theta_m n}$均成立。对于汉明度量码，这个问题已在 [18] 和 [7] 中研究过；对于赋予 Enomoto-Katona 距离（也称为运输距离）的码， [7] 也对此进行了研究。估计 t-纠错码的关键工具是所谓的“容器结果”，它指出，图的独立集仅包含在节点集的少数几个子集中，而这些子集是“近似独立集”。距离为 $2t+1$ 的 t-纠错码的估计，等价于估计我们图中的独立集。尽管我们的图不具备 Sapozhenko 所要求的性质，即图近乎正则且为扩展图，但我们可以将 [18] 中的饱和估计推广到 Lee 度量，再应用 [7]中的容器结果。为此，我们首先推导 Lee 度量下不同半径的球的体积估计。我们还刻画了半径相同、相应中心之间距离为 ℓ的两个球的交集。特别地，我们证明，这些交集的大小随 ℓ单调递减。随后，我们给出这些量的一个上界，其中仅包含 Lee 体积，而其显式公式早在 1982 [6]中就已为人所知。据我们所知，所有这些结果都是新的。研究球的交集对于编码理论的若干基本问题具有重要意义。我们的交集结果确定了 Lee 度量码的打包性质和覆盖性质，这些性质对于这类码的译码和性能分析都很重要。正如 [30], 近期指出的那样，若能找到可快速计算的两个球交集大小的上界和下界，将有助于研究码的覆盖性质。因此，我们认为这些技巧在这一背景下也可能具有参考价值。

本文的结构如下。我们首先在第2节介绍预备知识，包括李重量、李体积以及一些有用的界或渐近关系。在预备知识的第二部分，我们考察某些李体积的比值，并研究李球的交集。第3节从超饱和估计开始，随后将其用于容器算法。我们还将说明如何利用这一方法估计基数固定的 t-纠错码。 [22] 已经针对汉明度量、秩度量和和秩度量中的码研究过这一问题。在那里，计数问题被建模为满足某些正则性条件的二分图，并通过图中孤立节点的数量来估计码的数量。我们对李度量稍作修改后采用这一方法，并在第4节再次介绍。最后，我们在第5节总结本文。

2 预备知识

本文中，令 $\mathbb{N}$ 为正整数集合， $\mathbb{Z}_m := \{0,\ 1,\ \ldots\ldots,\ m-1\}$表示模 m 整数环；这里略去记号上的区别，将每个剩余类 $i + m\mathbb{Z}$ 记为其代表元 $0 \le i \le m-1$。用 P表示素数集合，用 $[n]$ 表示不超过 n的正整数集合。书写 $p \to +\infty$时，我们省略“$p \in P$”。对于依赖于 n的非负量，若存在某个正常数 C，使得对所有充分大的 n都有 $f(n) \le Cg(n)$，则记作 $f(n) \lesssim g(n)$。我们用 $[n]$ 表示不超过 n的正整数集合。给定有限集合X，用$\binom{X}{t}$ 表示 X的 t元子集所组成的集合族，用 $\binom{X}{\le t}$ 表示 X 中至多含有 t 个元素的子集族。以下恒等式以及关于二项式系数的上界都是众所周知的，且在后文中会用到。

引理 2.1. （参见 [21, 第 5]章）设 $n \in \mathbb{N}$, $k \ge 0$ 为整数。那么

1. $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$,
2. $\binom{n-1}{k} = \frac{n-k}{n}\binom{n}{k}$,
3. $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$,

4. $\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le \left(\frac{en}{k}\right)^k$.

2.1 李度量码

我们简要回顾 Lee 度量及其球体积。

定义 2.2. 对于 $x \in \mathbb{Z}_m$，我们将李重量 定义为

$$w^{\mathrm{L}} : \mathbb{Z}_m \to \left\{0, \ldots, \left\lfloor \frac{m}{2} \right\rfloor\right\}, \quad x \mapsto \min\{x, m-x\}.$$

我们用 θ_m 表示 $\mathbb{Z}_m$ 上的平均Lee重量，并将重量加法扩展到 $\mathbb{Z}_m^n$，因此 $x \in \mathbb{Z}_m^n$ 的李重量为

$$w^{\mathrm{L}}(x) := \sum_{i=1}^{n} w^{\mathrm{L}}(x_i).$$

我们将 $x, y \in \mathbb{Z}_m^n$ 的*Lee* 距离 定义为

$$d^{\mathrm{L}}(x, y) := w^{\mathrm{L}}(x - y).$$

一个 （*Lee* 度量）码是一个子集 $\mathscr{C} \subseteq \mathbb{Z}_m^n$。当 $|\mathscr{C}| \ge 2$ 其最小 *Lee* 距离为

$$d^{\mathrm{L}}(\mathscr{C}) := \min\{d^{\mathrm{L}}(x, y) \colon x, y \in \mathscr{C},\, x \ne y\}.$$

若码 $\mathscr{C}$ 是线性的，则它是 $\mathbb{Z}_m^n$ 的有限生成子模。生成 $\mathscr{C}$ 作为 $\mathbb{Z}_m$-模所需的 $\mathscr{C}$ 中元素的最少数目，称为 $\mathscr{C}$ 的秩。由于在线性情形中我们仅考虑 $\mathbb{Z}_p^n$，因此所考虑的所有线性码都是自由的，也就是说，$\mathscr{C}$ 的任意生成集的大小都决定了 $\mathscr{C}$ 的秩。

注意，根据定义，对于 $m = 2$ 和 $m = 3$，汉明距离与 Lee 距离相同。

定义 2.3。在 $\mathbb{Z}_m^n$ 中，以 $c \in \mathbb{Z}_m^n$ 为中心、半径为 $0 \le r \le \lfloor m/2 \rfloor$ 的李度量球为

$$\mathbf{B}_m^{\mathrm{L}}(n, r, c) := \{y \in \mathbb{Z}_m^n : d^{\mathrm{L}}(x, y) \le r\}.$$

其体积与中心无关，记作 $\mathbf{v}_m^{\mathrm{L}}(n,\ r)$。

定义 2.4。对于任意向量 $z \in \mathbb{Z}_m^n$，定义其*Lee* 组成 $\ell(z)$ 为

$$\ell(z) := (\ell_0(z), \ell_1(z), \ldots, \ell_{\lfloor m/2 \rfloor}(z)),$$

其中

$$\ell_i(z) := |\{j \in [n] : w^{\mathrm{L}}(z_j) = i\}|.$$

显然，$\sum_{i=0}^{\lfloor m/2 \rfloor} \ell_i(z) = n$ 和 $\sum_{i=0}^{\lfloor m/2 \rfloor} i\ell_i(z) = w^{\mathrm{L}}(z)$。我们用 $\mathscr{L}_m^n := \{\ell_0,\ \ldots\ldots,\ \ell_\alpha\} = \{\ell(z) : z \in \mathbb{Z}_m^n\}$ 表示所有 Lee 组成的集合，其中 $\alpha + 1$ 是 $\mathbb{Z}_m^n$ 中不同 Lee 组成的数量，且 $\ell_{\mathbf{0}} = \ell(0) = (n,\ 0,\ \ldots\ldots,\ 0)$。接着定义 *Lee* 关联方案，使得 $R = (R_{\ell_0},\ \ldots\ldots,\ R_{\ell_\alpha})$ 在 $\mathbb{Z}_m^n \times \mathbb{Z}_m^n$ 上构成一个划分，具体如下：

$$(x, y) \in R_{\ell_{\mathbf{i}}} \Leftrightarrow \ell(x - y) = \ell_{\mathbf{i}},$$

同时满足公理 $1. - 4.$，参见 [36, 第 2.1] 节：

1. $R_{\ell_{\mathbf{0}}} = \{(x, x) \in \mathbb{Z}_m^n \times \mathbb{Z}_m^n : x \in \mathbb{Z}_m^n\}$. 2. $R_{\ell_{\mathbf{i}}}^{-1} = \{(y, x) \in \mathbb{Z}_m^n \times \mathbb{Z}_m^n : (x,$ $y) \in R_{\ell_{\mathbf{i}}}\} = R_{\ell_{\mathbf{j}}}$ 对于某个$\mathbf{j} \in \{\mathbf{0}, \ldots, \alpha\}$。

3. $\{z \in \mathbb{Z}_m^n : (x,z) \in R_{\ell_{\mathbf{i}}}$和$(z,y) \in R_{\ell_{\mathbf{j}}}\}$的大小由一个数$p_{i,j}^k$描述，该数取决于 k，但不取决于$(x,y) \in R_{\ell_{\mathbf{k}}}$.

4. 对所有 $i, \ j, \ k \in \{0, \ \ldots, \ \alpha\}$ 我们有 $p_{i,j}^k = p_{j,i}^k$.

备注 1。 如果 $(x, \ y) \in R_{\ell_{\mathbf{i}}}$，那么 x 与 y 之间的 Lee 距离为

$$d^{\mathrm{L}}(x,y) = \ell_{\mathbf{i},1}(x-y) + 2\ell_{\mathbf{i},2}(x-y) + \cdots + \left\lfloor \frac{m}{2} \right\rfloor \ell_{\mathbf{i},\lfloor m/2 \rfloor}(x-y).$$

这直接意味着 Lee 度量在该方案的各个类上为常数。将满足 $d^{\mathrm{L}}(x,y) = j$的数对 (x,y) 的各个类记为 $R_{\ell_{\mathbf{j_1}}}, \ldots, R_{\ell_{\mathbf{j_{s(j)}}}}$，其中 $\mathbf{s(j)}$ 是重量为 j的不同组合的数量。这个数 $\mathbf{s(j)}$ 对应于 j 分成 n 部分且每部分至多为 $\lfloor m/2 \rfloor$. 的弱组合数。这个数可以计算为

$$\mathbf{s}(\mathbf{j}) = \sum_{\substack{(r,s) \in \mathbb{N}^2 \\ r+s\lfloor m/2 \rfloor = j}} (-1)^s \binom{n}{s} \binom{n+r-1}{r},$$

参见例如 [37,第 1] 章。因此，

$$|\mathscr{L}_m^n| = \alpha + 1 = \sum_{j=0}^{n\lfloor m/2 \rfloor} \mathbf{s}(\mathbf{j}).$$

由公理 3。 我们得到：

引理 2.5. 令 $(x,y) \in \mathbb{Z}_m^n \times \mathbb{Z}_m^n$ 使得 $d^{\mathrm{L}}(x,y) = k$。则满足 $d^{\mathrm{L}}(x,z) \leq r$ 且 $d^{\mathrm{L}}(y,z) \leq r$ 的向量 $z \in \mathbb{Z}_m^n$的数量等于

$$\sum_{i=0}^{r} \sum_{j=1}^{\mathbf{s(i)}} \sum_{\ell=1}^{\mathbf{s(i)}} p_{i_j,i_\ell}^k,$$

其中 $p_{i, \ j}^k := |\{z \in \mathbb{Z}_m^n : (x, \ z) \in R_{\ell_{\mathbf{i}}} \wedge (y, \ z) \in R_{\ell_{\mathbf{j}}}\}|$ 它取决于 k，但不取决于这一对 $(x, \ y) \in R_{\ell_{\mathbf{k}}}$。

定义2.6。长度为 n 的 t-*Lee*纠错码是 $\mathbb{Z}_m^n$ 中最小 Lee 距离至少为 $2t+1$ 的一个码。其最大大小记为 $A_m(n, \ 2t+1)$。

简单的计数论证表明：

定理2.7。设 $A_m(n, \ 2t+1)$ 表示 t-Lee纠错码的最大大小$\mathscr{C} \subseteq \mathbb{Z}_m^n$ 并且

$$H_m(n,t) := \frac{m^n}{\mathbf{v}_m^{\mathrm{L}}(n,t)}, \tag{2.1}$$

then

$$A_m(n, 2t+1) \leq H_m(n,t).$$

这个上界称为球填充界（或汉明界）。达到这个上界等号的码称为完美码。

此外，针对 Lee 度量码已知许多类 Singleton 界（关于这些界的概述，见 [13] ）。然而，关于 $\mathbb{Z}_{p^s}$ 上自由线性码的最小 Lee 距离，目前已知的最小界可以通过类 Plotkin 论证得到，即对 $\mathbb{Z}_{p^s}$ 上的重量取平均。

定理 2.8。 （类 Plotkin 界，见 [13, 定理 26]）设 $\mathscr{C} \subseteq \mathbb{Z}_{p^s}^n$ 是一个自由线性 t-Lee-纠错码。对于 $p \geq 3$，我们有

$$|\mathscr{C}| \leq p^{s(n - \frac{8t+4}{p^s+1} + 1)}.$$

2.2 Lee度量体积的交集与估计

李度量球的体积已知：

引理 2.9. [5, 第 6 章。3]

$$\mathbf{v}_m^{\mathrm{L}}(n,r)=\begin{cases}\displaystyle\sum_{i=0}^{\lfloor 2r/m\rfloor}(-1)^i\binom{n}{i}\sum_{j=0}^{r-(m/2)i}2^j\binom{n}{j}\binom{r-(m/2)i}{j} & \text{if } m \text{ is even},\\ \displaystyle\sum_{i=0}^{r}\binom{n+1}{i}\sum_{j=0}^{\lfloor 2r/m\rfloor}(-2)^j\binom{n}{j}\binom{n-j}{r-j(\lfloor m/2\rfloor+1)-i} & \text{if } m \text{ is odd}.\end{cases}$$

由此得到以下界：

引理 2.10. 设 $n\in\mathbb{N}$ 和 $1\le r\le n\lfloor\frac{m}{2}\rfloor$。则

1. $\mathbf{v}_m^{\mathrm{L}}(n,r)\le\sum_{i=0}^{n}2^i\binom{n}{i}\binom{r}{i}$,
2. $\mathbf{v}_m^{\mathrm{L}}(n,r)\ge\begin{cases}\binom{n}{r}2^r & \text{if } r<n,\\ 2^n & \text{if } r\ge n.\end{cases}$

证明。上界见 [33, 第 10] 节。下界由 [40] 得知。事实上，若 $r<n$，$\mathbf{v}_m^{\mathrm{L}}(n,r)$ 包含 $\mathbb{Z}_m^n$ 中所有在 $\{1,m-1\}$ 里有 r 个非零项、其余位置为零的向量。若 $r\ge n$，$\mathbf{v}_m^{\mathrm{L}}(n,r)$ 包含所有 $\{1,m-1\}^n$。□

我们得到体积的以下渐近行为：

引理 2.11. 设 $n\in\mathbb{N},C>0$ 为常数，且 $1\le r\le n\lfloor\frac{m}{2}\rfloor$。则

1. $\mathbf{v}_m^{\mathrm{L}}(n,r)\in\omega(1)$，当 $n\to+\infty$.2 时。2. $\mathbf{v}_m^{\mathrm{L}}(n,r)\in O(1)$，当 $m\to+\infty$.3 时。3. 若 $r\lesssim n^{a/b}$，其中 $a<b$，则 $\mathbf{v}_m^{\mathrm{L}}(n,r)\in o\left(\frac{C^n}{n^{(b+1)/b}}\right)$，当 $n\to+\infty$.

Proof. 前两条结论直接由引理 2.10 得出。对于 $r\le n^{a/b}$，我们有

$$\mathbf{v}_m^{\mathrm{L}}(n,r)\le\sum_{i=0}^{n^{a/b}}2^i\binom{n}{i}\binom{n^{a/b}}{i}\sim(2e^2n^{a/b})^{n^{a/b}}$$

对于 $n\to+\infty$（由引理 2.1 和 2.10 得出）。此外

$$\frac{n^{(b+1)/b}(2e^2n^{a/b})^{n^{a/b}}}{C^n}=\frac{\exp\left(\frac{b+1}{b}\log(n)+n^{a/b}(\log(2)+2+\log(n^{a/b}))\right)}{\exp(n\log(C))}\overset{n\to+\infty}{\to}0,$$

因为分母的指数随 n 线性增长，而分子的指数仅增长 $n^{a/b}$.

□

在研究两个 Lee 球的交集之前，我们先推导不同半径的球的体积估计。证明见附录。

引理 2.12. 设 $1 \le t \le n\lfloor \frac{m}{2} \rfloor$ 和 C_m 为充分大的常数。则对于任意 $1 \le i$

$$\mathbf{v}_m^{\mathrm{L}}(n,t) \le \begin{cases} \left(\frac{t+i}{2(n+i)}\right)^i \mathbf{v}_m^{\mathrm{L}}(n+i,t+i) & \text{if } m \text{ is even,} \\ \left(\frac{C_m}{n+i}\right)^i \mathbf{v}_m^{\mathrm{L}}(n+i,t+i) & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \left(\frac{t+i}{n+i}\right)^i \mathbf{v}_m^{\mathrm{L}}(n+i,t+i) & \text{else,} \end{cases}$$

且对于 $1 \le i \le n\lfloor \frac{m}{2} \rfloor - t$

$$\mathbf{v}_m^{\mathrm{L}}(n,t) \le \begin{cases} \left(\frac{t+i}{2n}\right)^i \left(\frac{n-i+1}{n-i+1-t}\right)^i \mathbf{v}_m^{\mathrm{L}}(n,t+i) & \text{if } m \text{ is even,} \\ \left(\frac{C_m}{n}\right)^i \left(\frac{n-i+1}{n-i+1-t}\right)^i \mathbf{v}_m^{\mathrm{L}}(n,t+i) & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \left(\frac{t+i}{n}\right)^i \left(\frac{n-i+1}{n-i+1-t}\right)^i \mathbf{v}_m^{\mathrm{L}}(n,t+i) & \text{else.} \end{cases}$$

接下来，我们研究具有相同 Lee 半径的两个球的交集。

引理 2.13. 令 $0 \le t \le n\lfloor \frac{m}{2} \rfloor$ 和 $c_1, c_2 \in \mathbb{Z}_m^n$，则 $\mathbf{B}_m^{\mathrm{L}}(n,r,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,r,c_2)$ 的大小仅通过 $d^{\mathrm{L}}(c_1, c_2)$.依赖于 c_1, c_2

证明。 这直接由引理 2.5 得出。 □

因此，对于 $0 \le t \le n\lfloor m/2 \rfloor$，我们将 $\mathbb{Z}_m^n$ 中半径为 t 且中心之间的 Lee 距离为 ℓ 的两个球的交集的基数记为 $W(m,n,t,\ell)$。当所考虑的环境空间明确时，我们简记为 $W(t,\ell)$。显然，当$\ell > 2t$时， $W(t,\ell) = 0$。因此，我们只关注 $1 \le \ell \le 2t \le nm,$ ，因为 $t \le n\lfloor m/2 \rfloor$.

下面我们证明，随着 ℓ 增大，数值 $W(t, \ell)$ 会递减 .

引理 2.14. 设 $1 \le \ell \le$ 最小$\{2t, n\lfloor m/2 \rfloor - 1\}$，则

$$W(t,\ell+1) \le W(t,\ell).$$

证明。我们定义如下记号

$$(1^\ell 0^{n-\ell}) := (\underbrace{1,1,\ldots,1}_{\ell},\underbrace{0,0,\ldots,0}_{n-\ell}).$$

根据引理 2.13，只需确定以 $c_1 = (0^n)$ 和 $c_2 = (1^\ell 0^{n-\ell})$ 为中心、半径为 t 的 Lee 球的交集，其中 $W(t, \ell)$；以及以 c_1 和 $c_3 = (1^{\ell+1}0^{n-\ell-1})$ 为中心、半径为 W 的球的交集，其中 $t(, \ell+1)$。定义

$X := \mathbf{B}_m^{\mathrm{L}}(n,t,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_3) \backslash \mathbf{B}_m^{\mathrm{L}}(n,t,c_2)$ 和 $Y := \mathbf{B}_m^{\mathrm{L}}(n,t,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_2) \backslash \mathbf{B}_m^{\mathrm{L}}(n,t,c_3$).

设 $x \in X$。由于 $x \in \mathbf{B}_m^{\mathrm{L}}(n,t,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_3)$，我们有 $d^{\mathrm{L}}(c_1,x) \le t$ 且 $d^{\mathrm{L}}(c_3,x) \le t$。由于$x \notin \mathbf{B}_m^{\mathrm{L}}(n,t,c_2)$，我们还得到 $d^{\mathrm{L}}(c_2,x) > t$。由此得到

$$w^{\mathrm{L}}(x_1-1,\ldots,x_{\ell+1}-1,x_{\ell+2},\ldots,x_n) \le t \tag{2.2}$$

$$w^{\mathrm{L}}(x_1-1,\ldots,x_{\ell}-1,x_{\ell+1},\ldots,x_n) > t. \tag{2.3}$$

由于 $(x_1-1,$ ……， $x_{\ell+1}-1,$ $x_{\ell+2},$ ……， $x_n)$ 和 $(x_1-1,$ ……， $x_{\ell}-1,$ $x_{\ell+1},$ ……， $x_n)$ 仅在第 $(\ell+1)^{th}$ 个坐标上相差恰好 1，由 (2.2) 和 (2.3) 可得

$$w^{\mathrm{L}}(x_1-1,\ldots,x_{\ell+1}-1,x_{\ell+2},\ldots,x_n) = t \tag{2.4}$$

$$w^{\mathrm{L}}(x_1-1,\ldots,x_{\ell}-1,x_{\ell+1},\ldots,x_n) = t+1. \tag{2.5}$$

因此， $d^{\mathrm{L}}(x,\ c_2) = t+1$ 且 $d^{\mathrm{L}}(x,\ c_3) = t$. 此外，用 (2.5) 减去 (2.4) 得到 $w^{\mathrm{L}}(x_{\ell+1}) - w^{\mathrm{L}}(x_{\ell+1}-1) = 1$，由此可推出 $x_{\ell+1} \in \{1,\ \ldots\ldots,\ \lfloor m/2 \rfloor\}$，否则 $w^{\mathrm{L}}(x_{\ell+1}) - w^{\mathrm{L}}(x_{\ell+1}-1) = -1$，特别是 $d^{\mathrm{L}}(x,\ c_2) < d^{\mathrm{L}}(x,\ c_3)$，这是不可能的。

为证明 $|X| \le |Y|$，我们定义一个单射 $\phi\colon X \to Y$，如下：

$$\phi(x)_i := \begin{cases} x_i & \text{if } i \in [n] \setminus \{\ell+1\}, \\ m - x_i + 1 & \text{if } i = \ell+1. \end{cases}$$

接下来我们证明此映射是良定义的。为此，我们将证明对于每个$x \in X$，都有

$$d^{\mathrm{L}}(\phi(x), c_1) < d^{\mathrm{L}}(x, c_1) \le t, \quad d^{\mathrm{L}}(\phi(x), c_3) = t+1, \quad d^{\mathrm{L}}(\phi(x), c_2) = t.$$

第一个观察结果源于以下事实： $x_{\ell+1} \in \{1, \ldots, \lfloor m/2 \rfloor\}$，因此

$$w^{\mathrm{L}}(\phi(x)_{\ell+1}) = x_{\ell+1} - 1 < x_{\ell+1} = w^{\mathrm{L}}(x_{\ell+1}).$$

对于第二个观察结果，回想一下， $d^{\mathrm{L}}(c_3, x) = t$。由此可推得

$$w^{\mathrm{L}}(\phi(x)_{\ell+1} - 1) = w^{\mathrm{L}}(m - x_{\ell+1}) = x_{\ell+1} = (x_{\ell+1}-1) + 1 = w^{\mathrm{L}}(x_{\ell+1}-1) + 1,$$

这给出 $d^{\mathrm{L}}(\phi(x)\ c_3) = t+1.$。最后一个观察结果可类似地得出，因此 $\phi(x) \in Y$。由于没有两个不同的元素映射到同一个像，我们有 $|X| \le |Y|$，从而

$$|\mathbf{B}_m^{\mathrm{L}}(n,t,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_3)| = |X \sqcup Z| \le |Y \sqcup Z| = |\mathbf{B}_m^{\mathrm{L}}(n,t,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_2)|$$

其中 $Z = \mathbf{B}_m^{\mathrm{L}}(n,t,c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_2) \cap \mathbf{B}_m^{\mathrm{L}}(n,t,c_3)$。 □

为了得到数值 $W(t,\ \ell)$ 之间的关系（这对第 3 节给出的饱和估计很重要），我们首先给出 $W(t,\ 1)$ 的显式公式，以及一般情况下 $\ell \in \{1,\ \ldots,\ n\lfloor m/2 \rfloor\}$ 的 $W(t,\ \ell)$ 上界。

引理 2.15。设 $1 \le \ell \le \min\{2t,\ n\lfloor m/2 \rfloor - 1\}$。

1. 对于 $\ell = 1$，有

$$W(t,1) = \begin{cases} 2\sum_{i=1}^{m/2} \mathbf{v}_m^{\mathrm{L}}(n-1, t-i) & \text{if } m \text{ is even}, \\ 2\sum_{i=1}^{(m-1)/2} \mathbf{v}_m^{\mathrm{L}}(n-1,t-i) + \mathbf{v}_m^{\mathrm{L}}(n-1, t-\frac{m-1}{2}) & \text{if } m \text{ is odd}. \end{cases}$$

2. 对于 $\ell \ge 1$，有 $W(t,\ \ell) \le m^{\ell} \mathbf{v}_m^{\mathrm{L}}(n - \lceil \ell/2 \rceil,\ t - \lceil \ell/2 \rceil)$。

证明。 设 $\ell = 1$，假设两个球的中心分别为 $c_1 := (0^n)$ 和 $c_2 := (10^{n-1})$，并设 $x \in \mathbf{B}_m^{\mathrm{L}}(n,\ t,\ c_1) \cap \mathbf{B}_m^{\mathrm{L}}(n,\ t,\ c_2)$。这给出 $w^{\mathrm{L}}(x_1) \le t$，并且根据平移不变性，其余 $n-1$ 个坐标的李重量至多为

$$t - \max\{w^{\mathrm{L}}(x_1), w^{\mathrm{L}}(x_1 - 1)\}.$$

注意到

$$\max\{w^{\mathrm{L}}(x_1), w^{\mathrm{L}}(x_1-1)\} = \begin{cases} 1 & \text{if } x_1 = 0, \\ x_1 & \text{if } 1 \le x_1 \le \lfloor m/2 \rfloor, \\ m - x_1 & \text{if } x_1 = \lfloor m/2 \rfloor + 1 \text{ and } m \text{ is odd}, \\ m - x_1 + 1 & \text{in all other cases.} \end{cases}$$

因此，对于固定的

- $x_1 = 0$ 剩余的 $n-1$ 个坐标有 $\mathbf{v}_{\mathrm{L}m}(n-1, t-1)$ 种选择可供 x 使用，
- $x_1 \in \{1、2、\ldots\ldots、\lfloor m/2 \rfloor\}$ 剩余的 $n-1$ 个坐标有 $\mathbf{v}_{\mathrm{L}m}(n-1,\ t-x_1)$ 种选择，
- $x_1 \in \{\lfloor (m+1)/2 \rfloor + 1、\ldots\ldots、\ m-1\}$ 剩余的 $n-1$ 个坐标有 $\mathbf{v}_{\mathrm{L}m}(n-1,\ t-m+x_1-1)$ 种选择，
- $x_1 = (m+1)/2$ 且 m 为奇数时，剩余的$n-1$ 个坐标有 $\mathbf{v}_{\mathrm{L}m}(n-1,\ t-(m-1)/2)$ 种选择。

对于第二个结论，假设这两个球分别以 $c_1 = (0^n)$ 和 $c_2 = (1^\ell 0^{n-\ell})$ 为中心。对于 $x \in \mathbf{B}^{\mathrm{L}}_m(n,\ t,\ c_1) \cap \mathbf{B}^{\mathrm{L}}_m(n,\ t,\ c_2)$，我们有最后 $n-\ell$ 个坐标的李重量至多为 $t - \max\{\sum_{i=1}^{\ell} w^{\mathrm{L}}(x_i),\ \sum_{i=1}^{\ell} w^{\mathrm{L}}(x_i - 1)\}$。此外，我们注意到

$$\max\left\{\sum_{i=1}^{\ell} w^{\mathrm{L}}(x_i), \sum_{i=1}^{\ell} w^{\mathrm{L}}(x_i - 1)\right\} \geq \lceil \ell/2 \rceil . \tag{2.6}$$

令 s 为 x 的前 ℓ 个坐标的支撑大小。若 $s \geq \lceil \ell/2 \rceil$，则 (2.6) 可直接由前 ℓ 个坐标的李重量至少等于其支撑大小这一事实推出。若 $s < \lceil \ell/2 \rceil$，则 x 至少有 $\lceil \ell/2 \rceil$ 个坐标为零，因此 $\sum_{i=1}^{\ell} w^{\mathrm{L}}(x_i - 1) \geq \lceil \ell/2 \rceil$。现在可以利用李体积关于两个参数的单调性得到上界。

□

利用引理 2.15 可知，中心间距离为 ℓ 的两个球的交集，显著小于中心间距离为 1 的两个球的交集。此外，应用引理 2.12 可得 $W(t,\ 1)$ 的一个上界，其中只包含体积 $\mathbf{v}^{\mathrm{L}}_m(n,\ t)$。

Lemm引理 2.16。令 $0 \leq \ell < \min\{t,\ n\lfloor m/4 \rfloor\}$，并设 C_m 为一个充分大的常数，则

$$W(t, 2\ell+1) \leq \begin{cases} \left(\frac{mt}{2n}\right)^{\ell} W(t,1) \leq \left(\frac{mt}{2n}\right)^{\ell+1} \mathbf{v}^{\mathrm{L}}_m(n,t) & \text{if } m \text{ is even,} \\ \left(\frac{mC_m}{n}\right)^{\ell} W(t,1) \leq \left(\frac{mC_m}{n}\right)^{\ell+1} \mathbf{v}^{\mathrm{L}}_m(n,t) & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \left(\frac{mt}{n}\right)^{\ell} W(t,1) \leq \left(\frac{mt}{n}\right)^{\ell+1} \mathbf{v}^{\mathrm{L}}_m(n,t) & \text{in all other cases.} \end{cases}$$

证明。我们只证明 m 为偶数的情形，其他情形可通过类似论证得出。结合引理 2.15 的两个结论以及引理 2.12，我们可以推导出第一个结论，即，

$$\frac{W(t, 2\ell+1)}{W(t,1)} \leq \frac{m^{\ell} \mathbf{v}^{\mathrm{L}}_m(n-\ell-1, t-\ell-1)}{\mathbf{v}^{\mathrm{L}}_m(n-1, t-1)} \leq m^{\ell} \left(\frac{t}{2n}\right)^{\ell},$$

这就证明了第一个不等式。为证明第二个不等式，再次应用引理 2.12，得到

$$\frac{W(t,1)}{\mathbf{v}^{\mathrm{L}}_m(n,t)} \leq \frac{m \mathbf{v}^{\mathrm{L}}_m(n-1, t-1)}{\mathbf{v}^{\mathrm{L}}_m(n,t)} \leq m \left(\frac{t}{2n}\right).$$

□

3 Lee纠错码的数量

本节给出 t-Lee纠错码数量的一个上界，其中不对码的基数作任何规定。本节中，除非另有说明，我们允许 t 为 n中的一个函数。更确切地说，我们令 $\lim_{n\to+\infty} t(n)/(10\sqrt{\theta_m n}) = T$，其中

$T \in [0,1]$ 和 θ_m 表示 $\mathbb{Z}_m$上的平均Lee重量。不过，我们通常用 t 作为 $t(n)$的简写。

为了得到 t纠错码数量的上界，我们使用与 [7]中类似的容器算法。为了应用该算法，我们将首先推导出必要的超饱和估计。

在本节中， $G = (V, E)$是一个没有自环的简单无向图，包含节点$V = \mathbb{Z}_m^n$和边 $E = \{(x, y) \in V^2 \colon d^{\mathrm{L}}(x, y) \le 2t\}$。任何不包含边的集合 $I \subseteq V$称为独立集，并对应一个 tLee纠错码。此外，我们用 $\Delta(G)$表示 G 的最大度，用 $i(G)$表示 G中的独立集数量。我们用 $N_G(u)$表示节点 u的邻域，即与 u相邻的节点子集。因此，

$$\Delta(G) = \max\{|\, N_G(u) \,| \colon u \in V\}.$$

容器算法基于一个动态图（G_i）$_{i\ge 0}$（初始化为 $G_0 = G$），并通过迭代至少移除一个节点来缩减其节点集 V（G_i）。更确切地说，在算法的每次迭代中，都会从图中移除度最大的节点（以及可能的其邻域）。

设 $\mathscr{C} \subseteq \mathbb{Z}_m^n$ 是一个码， $G[\mathscr{C}] = (\mathscr{C}, E[\mathscr{C}])$ 是 G 的对应诱导子图。对于每个 $1 \le r \le 2t$，我们定义

$$E_r := \{(x, y) \in E[\mathscr{C}] : d^{\mathrm{L}}(x, y) = r\}$$

并且对于 $v \in \mathscr{C}$，将 E_r 中与 v 关联的边数定义为

$$\deg_r(v) := |\{u \in \mathscr{C} : d^{\mathrm{L}}(u, v) = r\}|.$$

引理 3.1. 设 $v \in \mathscr{C}$ 和 $r \le n/2$。则

$$\deg_r(v) \le 3^r \binom{n}{r}$$

因此

$$|E_r| \le \frac{3^r}{2} \binom{n}{r} |\mathscr{C}|.$$

证明。由二项式定理可得 $\deg_r(v) \le \mathbf{v}_m^{\mathrm{L}}(n, r) \le \sum_{i=0}^{n} 2^i \binom{n}{i}\binom{r}{i} = \sum_{i=0}^{r} 2^i \binom{n}{i}\binom{r}{i}$
$\le \binom{n}{r} \sum_{i=0}^{r} 2^i \binom{r}{i} = 3^r \binom{n}{r}$，这证明了第一个结论。第二个结论则由对 $\mathscr{C}$ 中所有码字对求和得到。

□

我们对 Lee度量 有如下估计。

引理 3.2。设 $\mathscr{C} \subseteq \mathbb{Z}_m^n$ 是一个 t-Lee纠错码，且 C_m 是一个充分大的常数。如果 $|\mathscr{C}| \ge 2H_m(n, t)$，则

$$\sum_{r=1}^{2t} W(t, r)|E_r| \ge \frac{|\mathscr{C}|^2 \mathbf{v}_m^{\mathrm{L}}(n, t)^2}{10m^n} \quad \text{and} \quad |E[\mathscr{C}]| \ge \begin{cases} \frac{n|\mathscr{C}|^2}{5mtH_m(n,t)} & \text{if } m \text{ is even,} \\ \frac{n|\mathscr{C}|^2}{10mC_mH_m(n,t)} & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \frac{n|\mathscr{C}|^2}{10mtH_m(n,t)} & \text{in all other cases.} \end{cases}$$

证明。与 [7, 引理 5.3], 类似，我们使用引理 2.14 和引理 2.16 得到该结果。为完整起见，我们在附录中给出证明。 □

容器方法通过表明，图的独立集仅落在节点集的少数几个子集中，而这些子集是“几乎独立集”，从而估计图的独立集数量。在建立所需的饱和估计后，我们将研究更为详细的关系。我们的第一个超饱和结果给出了节点集大小的限制，以确保诱导子图的最大度超过某个界。

命题 3.3。（超饱和 1）设 $t \le 10\sqrt{\theta_m n}$、$C_m$ 为充分大的常数，且 $\mathscr{C} \subseteq \mathbb{Z}_m^n$ 是一个 t-Lee纠错码。若 $|\mathscr{C}| \ge n^4 H_m(n,\ t)$，则

$$\Delta(G[\mathscr{C}]) \gtrsim \begin{cases} \frac{n^3|\mathscr{C}|}{C_m H_m(n,t)} & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \frac{n^3|\mathscr{C}|}{t^3 H_m(n,t)} & \text{in all other cases,} \end{cases}$$

关于 n 渐近成立。

证明。我们将证明 m 为偶数时的情形；当 m 为奇数时，证明类似。由于 $|\mathscr{C}| \ge n^4 H_m(n,\ t)$，由引理 3.2 可得

$$|E[\mathscr{C}]| \ge \frac{|\mathscr{C}|^2 n}{5mtH_m(n,t)} \ge |\mathscr{C}| \frac{n^5}{5mt}.$$

结合 $|E_1| + |E_2| \lesssim n^2|\mathscr{C}|$ 和 $|E_3| + |E_4| \lesssim n^4|\mathscr{C}|$（由引理 3.1 可得），得到 $|E_1| + |E_2| \lesssim \frac{t|E[\mathscr{C}]|}{n^3}$ 和 $|E_3| + |E_4| \lesssim \frac{t|E[\mathscr{C}]|}{n}$.。此外，由引理 2.16 可得

$$\begin{aligned} W(t,2) &\le W(t,1), \\ W(t,4) \le W(t,3) &\lesssim \frac{tW(t,1)}{n}, \\ W(t,r) \le W(t,5) &\lesssim \frac{t^2 W(t,1)}{n^2} \quad \forall r \ge 5, \end{aligned}$$

由此得到

$$\sum_{r=1}^{2t} W(t,r)|E_r| \lesssim \left(\frac{t}{n^3} + \frac{t^2}{n^2} + \frac{t^2}{n^2} \right) |E[\mathscr{C}]| W(t,1) \lesssim \frac{t^2}{n^2} W(t,1)|E[\mathscr{C}]|.$$

由引理 3.2 可得

$$\frac{|\mathscr{C}|^2 \mathbf{v}_m^{\mathrm{L}}(n,t)^2}{m^n} \lesssim \sum_{r=1}^{2t} W(t,r)|E_r| \lesssim \frac{t^2}{n^2} W(t,1)|E[\mathscr{C}]|.$$

利用引理 2.16 中的 $W(t,\ 1)$. $(t/n)\mathbf{v}_m^{\mathrm{L}}(n,\ t)$，我们得到

$$|E[\mathscr{C}]| \gtrsim \frac{n^2|\mathscr{C}|^2 \mathbf{v}_m^{\mathrm{L}}(n,t)^2}{t^2 m^n W(t,1)} \gtrsim \frac{n^3|\mathscr{C}|^2}{t^3 H_m(n,t)}.$$

因此，$G[\mathscr{C}]$ 中的平均度为 $\gtrsim \frac{n^3|\mathscr{C}|}{t^3 H_m\ n}(.\ \ t)$，因此 $\Delta(G[\mathscr{C}]) \gtrsim \frac{n^3|\mathscr{C}|}{t^3 H_m\ n}(.\ \ t)$· ——— □

接下来我们将给出一个最大度的估计，以证明 $i(G[\mathscr{C}])$ 小于 $2^{(1+\varepsilon)H_{m(n,t)}}$。为了得到这个估计，我们根据邻居数量来考察 $G[\mathscr{C}]$ 中的节点，使得它们之间的 Lee 距离至多为 20。通过考察半径为 t 的球，并证明它们的重叠可以忽略不计，我们可以估计 $60 \le t \le 10\sqrt{\theta_m n}$ 的 t-Lee-纠错码的数量。在引理 3.5 中，使用小于 20 的数无法得到合适的估计。因此，我们选择这个数。我们定义这些集合。

$$\mathscr{C}_1 := \left\{ v \in \mathscr{C} : \deg_r(v) \le \varepsilon n^{\lceil r/2 \rceil / 2} \quad \forall r \in \{1, \dots, 20\} \right\}, \tag{3.1}$$

$$\mathscr{C}_2 := \left\{ v \in \mathscr{C} : \sum_{r=1}^{20} \deg_r(v) \ge \frac{\log(n)}{\varepsilon} \right\} \tag{3.2}$$

并计算 $i(G[\mathscr{C}_i])$，对于 $i=1,2$，假设 $G[\mathscr{C}_i]$ 的最大度不太大。注意，对于 $v\in\mathscr{C}$，若 $n\to+\infty$，则有 $\sum_{r=1}^{20}\deg_r(v)\in o(n^5)$，因此当 n 足够大时，$\mathscr{C}=\mathscr{C}_1\cup\mathscr{C}_2$。由于当 n 足够大时，$G[\mathscr{C}]$ 的每个独立集都可能是 $G[\mathscr{C}_1]$ 的一个独立集与 $G[\mathscr{C}_2]$ 的并集，我们利用$i(G[\mathscr{C}])\le i(G[\mathscr{C}_1])i(G[\mathscr{C}_2])$ 得到总体估计。

引理 3.4。设 $t\le 10\sqrt{\theta_m n}$, $\mathscr{C}\subseteq\mathbb{Z}_m^n$ 是一个 t-Lee纠错码，$\Delta(G[\mathscr{C}])\le n^5$ 并固定$\varepsilon>0$。设 $\mathscr{C}_1$ 如(3.1)中所定义。

则当 n充分大时，$|\mathscr{C}_1|\le(1+O(\varepsilon))H_m(n,t)$。

证明。 证明见附录。 □

引理 3.5。设 $60\le t\le 10\sqrt{\theta_m n}$, $\mathscr{C}\subseteq\mathbb{Z}_m^n$ 是一个 t-Lee纠错码，且 $\Delta(G[\mathscr{C}])\le n^5$。固定 $0<\varepsilon$，令 n 充分大，并设 $\mathscr{C}_2$ 如(3.2)中所定义。则 $\mathscr{C}_2$ 的独立子集数量满足

$$i(G[\mathscr{C}_2])\le 2^{O(\varepsilon H_m(n,t))}.$$

证明。 证明见附录。 □

命题 3.6。（超饱和性 2）设 $0<\varepsilon$, $60\le t\le 10\sqrt{\theta_m n}$，$\mathscr{C}\subseteq\mathbb{Z}_m^n$ 是一个 t-Lee纠错码，并令 n 充分大。若 $\Delta(G[\mathscr{C}])\le n^5$，则

$$i(G[\mathscr{C}])\le 2^{(1+\varepsilon)H_m(n,t)}.$$

证明。 按照 (3.1) 和 (3.2) 定义 $\mathscr{C}_1$ 和 $\mathscr{C}_2$，得到

$$i(G[\mathscr{C}])\le i(G[\mathscr{C}_1])i(G[\mathscr{C}_2])\le 2^{|\mathscr{C}_1|}i(G[\mathscr{C}_2])\le 2^{(1+O(\varepsilon))H_m(n,t)}.$$

□

为了证明容器引理也适用于较小的 t，即 $1\le t\le 60$，我们使用来自 [7] 的饱和估计。

引理 3.7。设 $\mathscr{C}\subseteq\mathbb{Z}_m^n$ 和 C_m 为充分大的常数。如果 $|\mathscr{C}|\ge H_m(n,t)+\gamma$，那么至少有超碰在线

$$\begin{cases}\frac{\gamma 2n}{mt} & \text{if } m \text{ is even},\\ \frac{\gamma n}{mC_m} & \text{if } m \text{ is odd and } t=\lceil\frac{m}{2}\rceil,\\ \frac{\gamma n}{mt} & \text{in all other cases},\end{cases}$$

满足 Lee 距离至多为 $2t$ 的数对 $v,w\in\mathscr{C}$。

证明。 利用引理 2.16，证明与 [7, 引理 5.2] 的证明类似，详见附录。

□

假设这些饱和性结果成立，我们可以对容器引理 [18,Lemma 2.3]，进行修改，从而直接推出主定理。为完整起见，我们给出证明。不过，我们将首先介绍容器算法及其性质。

引理 3.8。令$1\le t\le 10\sqrt{\theta_m n}$，$0<\varepsilon$ 和 n 足够大。则存在一个集合族$\mathscr{F}$，其为 $\mathbb{Z}_m^n$ 的子集，并具有以下性质

(i) $|\mathscr{F}|\le 2^{\varepsilon H_m(n,t)}$.

(ii) 每个 t-Lee纠错码 $\mathscr{C}\subseteq\mathbb{Z}_m^n$ 都包含于某个 $F\in\mathscr{F}$ 中。

(iii) 每个 $F\in\mathscr{F}$ 都有 $i(G[F])\le 2^{(1+\varepsilon)H_m(n,t)}$。

回想一下， $G=(V,E)$ 描述了一个具有 $V=\mathbb{Z}_m^n$ 和 $E=\{(x,y)\in V^2\colon d^{\mathrm{L}}(x,y)\leq 2t\}$ 的图。为证明引理 3.8，我们将应用 Kleitman 和Winston 的算法的以下版本 [26, 27]。

算法 1. 为 $v_1,\ldots,v_{m^n}$ 中的元素任意固定一个顺序。令 I 为 G中的一个独立集。初始化 $G_0:=G$ 和 $P:=\emptyset$。如果 m 为偶数，则设 $\Delta:=\varepsilon n/(mt)$；如果 m 为奇数且 $t=\lceil m/2\rceil$，则选取足够大的 C_m，使引理 3.7 成立，并设 $\Delta:=\varepsilon n/(mC_m)$。其他情况下，设 $\Delta:=\varepsilon n/(2mt)$。在算法的每一步 i 中，通过以下过程将节点加入 P。

i) 令 u 为 $V(G_{i-1})$中度最大的节点。如果有两个节点的度最大，则选择排序中靠前的节点。

ii) 如果 $u\notin I$，定义 $V(G_i):=V(G_{i-1})\setminus\{u\}$，并继续执行步骤 $i+1$。

iii) 如果 $u\in I$ 且 $\deg_{G_{i-1}}(u)\geq\Delta$，则将 u 加入 P，定义 $V(G_i):=V(G_{i-1})\setminus(\{u\}\cup N_G(u))$，并继续执行步骤 $i+1$。

iv) If $u\in I$ 且 $\deg_{G_{i-1}}(u)<\Delta$ 定义 $f(P):=V(G_i)$，终止并输出 P和 $f(P)$.

引理 3.9。 设 $0<\varepsilon,1\leq t<60$ 且设 n 充分大。那么存在一个函数

$$f:\binom{V(G)}{\leq\frac{\varepsilon H_m(n,t)\log(n)}{n}}\to\binom{V(G)}{\leq(1+\varepsilon)\,H_m(n,t)},$$

使得对于 G 中的每个独立集 I，都存在某个子集 $P\subseteq I$ 满足 s

(i) $|P|\leq\varepsilon H_m(n,t)\log(n)\,n$, (ii) $I\subseteq P\cup f(P)$. iii) $i(G[P\cup f(P)])\leq 2^{(1+\varepsilon)H_m(n,t)}$.

证明。 证明可在附录中找到。 □

为证明关于 $60\leq t\leq 10\sqrt{\theta_m n}$ 的结论，我们采用 Dong 等人 [18] 提出的算法 1 的以下变体。

算法 2。 为集合 V 的元素任意固定一个顺序 v_1，……，v_{m^n}。令 I 为 G 中的一个独立集。初始化 $G_0:=G$ 和 $P:=\emptyset$。在算法的每一步 i 中，按以下过程将节点加入 P。

i) 如果 $i(G_{i-1})\leq 2^{(1+\varepsilon)H_m(n,\,t)}$，则设 $f(P)=V(G_{i-1})$，终止并输出 P 和 $f(P)$.

ii) 令 u 为 $V(G_{i-1})$ 中度最大的节点。如果有两个节点的度均为最大度，则选择排序中靠前的节点。

iii) 如果 $u\notin I$，定义 $V(G_i):=V(G_{i-1})\setminus\{u\}$，并继续执行步骤 $i+1$。

iv) 若 $u\in I$，则将 u 加入 P，定义 $V(G_i):=V(G_{i-1})\setminus(\{u\}\cup N_G(u))$，并转到步骤 $i+1$。

算法 2 可验证下述函数定义良好。

引理 3.10。 设 $0<\varepsilon,0<C$ 为充分大的常数， $60\leq t\leq 10\sqrt{\theta_m n}$，并设 n 充分大。则存在一个函数

$$f:\binom{V}{\leq\frac{CH_m(n,t)\log(n)}{n}}\to 2^V,$$

使得对于 G 中的任意独立集 I，都存在某个子集 $P\subseteq I$ 满足以下三个条件：

i) $I \subseteq P \cup f(P)$,

ii) $|P| \leq \frac{CH_m(n,\ t)\ 对数(n)}{n}$,

iii) $i(G[P \cup f(P)]) \leq 2^{(1+\varepsilon)H_m(n,t)}$.

证明。第一个观察结论可通过结构归纳法得出。为了证明其余两个条件，我们根据 $V(G_i)$ 的大小，将算法分为两个阶段。

- 令 P_1 表示当 $|V(G_{i-1})| \geq n^4 H_m(n,\ t)$ 时添加到 P 的节点集合 $u \in P$。
- 令 P_2 表示当 $|V(G_{i-1})| < n^4 H_m(n,\ t)$。时添加到 P 的节点集合 $u \in P$。

也就是说，存在一个 $k > 0$，使得添加到 P 中的每个节点，直到第 k 步（包括该步）为止，都属于 P_1；而在第 k 步之后添加到 P 中的每个节点都属于 P_2。令 $\beta := \frac{n^{3/2}}{H_m(n,t)}$。随着我们向 P_1 中添加节点，根据引理 3.3，我们至少移除 G_{i-1} 中比例为 β 的节点，从而得到 G_i。因此，分别有 $(1-\beta)^k m^n \leq n^4 H_m(n,\ t)$ 和 $(1-\beta)^k \mathbf{v}_m^{\mathrm{L}}(n,\ t) \leq n^4$。根据引理 2.11，我们有 $\beta \to 0$，因为 $n \to +\infty$，因此当 n 足够大时，$\beta \leq \log\left(\frac{1}{1-\beta}\right)$，于是

$$
\begin{aligned}
|P_1| &\leq \frac{\log\left(\frac{n^4 H_m(n,t)}{m^n}\right)}{\log(1-\beta)} \leq \frac{\log\left(\frac{m^n}{n^4 H_m(n,t)}\right)}{\log\left(\frac{1}{1-\beta}\right)} \lesssim \frac{\log(\mathbf{v}_m^{\mathrm{L}}(n,t)) - 4\log(n)}{\beta} \overset{(*)}{\lesssim} \frac{t\log(n) H_m(n,t)}{n^{3/2}} \\
&\lesssim \frac{\log(n) H_m(n,t)}{n},
\end{aligned}
$$

其中 (*) 根据引理 2.1 和 2.10 得出。随着我们向 P_2 中添加节点，在相关迭代过程中，我们有 $i(G_{i-1}) \geq 2^{(1+\varepsilon)H_m(n,\ t)}$。根据引理 3.6，我们在每次迭代中至少移除 n^5 个节点，因此

$$
|P_2| \lesssim \frac{n^4 H_m(n,t)}{n^5} \leq \frac{H_m(n,t)}{n}.
$$

这给出了

$$
|P| = |P_1| + |P_2| \leq \frac{C\log(n) \cdot H_m(n,t)}{n},
$$

因此

$$
i(G[P \cup f(P)]) \leq 2^{|P|} \cdot i(f(P)) \leq 2^{(1+2\varepsilon)H_m(n,t)}.
$$

□

现在我们可以开始证明引理 3.8。

引理 3.8 的证明。令 $G = (V, E)$ 为具有 $V = \mathbb{Z}_m^n$ 和 $E = \{(x,y) \in V^2 : d^{\mathrm{L}}(x,y) \leq 2t\}$ 的图。假设 I 遍历 G 的所有独立集。如果 $1 \leq t \leq 60$，则令 $\mathscr{F}$ 为通过算法 1 得到的所有 $P \cup f(P)$ 的集合族，否则令 $\mathscr{F}$ 为通过算法 2 得到的所有 $P \cup f(P)$ 的集合族。由于 t-Lee纠错码恰好是 G 中的独立集，根据引理 3.9 和 3.10，我们得到每个 t-Lee纠错码都包含于某个 $F \in \mathscr{F}$ 中。引理 3.9 和 3.10 中的第三个条件给出，对于每个 $F \in \mathscr{F}$，有 $i(G[F]) \leq 2^{(1+2\varepsilon)H_m(n,t)}$。根据引理 2.1，$\log\binom{n}{m} \leq m\log(O(n)/m)$。由此得到 $1 \leq t < 60$

$$
\begin{aligned}
\log|\mathscr{F}| &\leq \log\binom{m^n}{\leq \frac{\varepsilon H_m(n,t)\log(n)}{n}} \leq \frac{\varepsilon H_m(n,t)\log(n)}{n} \log\left(O\left(\frac{\mathbf{v}_m^{\mathrm{L}}(n,t)n}{\varepsilon\log(n)}\right)\right) \\
&\lesssim \frac{\varepsilon H_m(n,t)\log(n)}{n} \log\left(O\left(\frac{(2en)^t n}{t^t \varepsilon\log(n)}\right)\right)
\end{aligned}
$$

类似地，对于 $60 \leq t \leq 10\sqrt{\theta_m n}$ 以及充分大的 C，有

$$\log|\mathscr{F}| \le \log\left(\le \frac{C\log(n)}{n} H_m(n,t)\right) \lesssim \frac{C\log(n)}{n} H_m(n,t)\log\left(O\left(\frac{n^{t+1}(2e/t)^t}{C\log(n)}\right)\right)$$
$$\lesssim \frac{Ct(\log(n))^2}{n} H_m(n,t).$$

因此，$|\mathscr{F}| \le 2^{\varepsilon H_m(n,\ t)}$，当 n 充分大时成立。引理 3.8 的证明至此完成。 □

现在可以陈述关于 t-Lee纠错码数量的主要结果。

定理 3.11. 令 $1 \le n, 2 \le m, 1 \le t \le 10\sqrt{\theta_m n}$, 则当 n充分大时，$\mathbb{Z}_m^n$ 中的 t-Lee纠错码数量渐近地至多为 $2^{(1+o(1))H_m(n,t)}$, 。

证明。设 $0 < \varepsilon$ 和 $\mathscr{F}$ 如引理 3.8 中所述，则 $\mathbb{Z}_m^n$ 中的 t-Lee纠错码数量至多为

$$\sum_{F\in\mathscr{F}} i(G[F]) \le |\mathscr{F}| 2^{(1+\varepsilon)H_m(n,t)} = 2^{(1+2\varepsilon)H_m(n,t)},$$

由于 ε 可以任意小，结论得证。 □

下面我们给出给定大小的 t-Lee纠错码数量的一个上界。我们将使用这一结果在 Python 中进行实验，并将其与第4节中通过二分图得到的上界进行比较。

定理 3.12. 令 $2 \le m, 1 \le t \le 60,\ 0 < \varepsilon$，并设 $1 \le n$ 充分大，则 $\mathbb{Z}_m^n$ 中长度为 n 且大小为 S 的 t-Lee纠错码数量渐近地至多为

$$2^{\varepsilon H_m(n,t)} \binom{(1+\varepsilon)H_m(n,t)}{S}.$$

证明。对于 $1 \le t \le 60$，令 $\mathscr{F}$ 为通过算法 1 得到的所有 $P \cup f(P)$ 的集合族。由引理 3.9 可得

$$|P \cup f(P)| \le \frac{\varepsilon H_m(n,t)\log(n)}{n} + (1+\varepsilon)\, H_m(n,t) \lesssim (1+\varepsilon)\, H_m(n,t),$$

也就是说，这是每个容器大小的一个上界。由于任何 t-纠错码都包含在某个 $F \in \mathscr{F}$ 中，且 $|\mathscr{F}| \le 2^{\varepsilon H_m(n,\ t)}$，结论由此得出。 □

注 2。请注意，由于引理 2.11 在考察 m 趋于无穷时使用了依赖于 $H_m(n,\ t)$ 的超饱和估计，我们最终只能考虑平凡码 $\mathscr{C} = \mathbb{Z}_m^n$，从而得到平凡的计数结果。因此，容器方法不适用于考察递增的 m。在第4节中，我们将使用一种基于二分图的不同计数技术，以估计当 m 趋于无穷时具有给定距离的码的数量。

回顾一下，$A_m(n,\ d)$ 表示最小距离为 d 的码 $\mathscr{C} \subseteq \mathbb{Z}_m^n$ 的最大大小。我们首先证明，对于 $10\sqrt{\theta_m n} < t < n^{4/5}$，$A_m(n,\ 2t+1) = o(H_m(n,\ t)/n)$。本节中以下版本的 Elias 界将起关键作用。

定理 3.13。令 $1 \le d,\ n$ 为整数，且 θ_m 为 $\mathbb{Z}_m$ 上的平均Lee重量。对于满足以下条件的每个 $r \le \theta_m n$

$$0 < r^2 - 2\theta_m n r + \theta_m n d,$$

以下上界成立

$$A_m(n,d) \le \frac{\theta_m n d}{r^2 - 2\theta_m n r + \theta_m n d} \cdot \frac{m^n}{\mathbf{v}_m^{\mathrm{L}}(n,r)}.$$

证明。 与汉明度量中的情况类似，见 [38, 定理 5.2。11]。 □

命题 3.14. 设 θ_m 为 $\mathbb{Z}_m$上的平均李重量。若 $10\sqrt{\theta_m n} < t < n^{4/5}$，则有 e

$$A_m(n, 2t+1) = o\left(\frac{H_m(n,t)}{n}\right).$$

证明。 我们在 $r = t + \alpha$ 的条件下应用 Elias界，其中 $\alpha = 7$。当 $10\sqrt{\theta_m n} < t$ 时，我们满足条件

$$r^2 \lesssim r^2 - \theta_m(2\alpha - 1)n = r^2 - 2\theta_m nr + \theta_m n(2t+1). \tag{3.3}$$

事实上，当 $10\sqrt{\theta_m n} < t < n^{4/5}$ 时，我们有 $\theta_m(2\alpha - 1)n = 13 \cdot \theta_m n$，而 $100 \cdot \theta_m n < r^2$。应用定理 3.13，并结合引理 2.12 的第二部分，得到

$$\begin{aligned} A_m(n, 2t+1) &\le \frac{\theta_m n(2t+1)}{r^2 - 2\theta_m nr + \theta_m n(2t+1)} \cdot \frac{m^n}{\mathbf{v}_m^{\mathrm{L}}(n,r)} \\ &\overset{(3.3)}{\lesssim} \frac{nt}{(t+\alpha)^2} \cdot \frac{m^n}{\mathbf{v}_m^{\mathrm{L}}(n, t+\alpha)} \\ &\lesssim \begin{cases} \frac{n}{t}\left(\frac{(t+\alpha)(n-\alpha+1)}{2n(n-\alpha+1-t)}\right)^{\alpha} H_m(n,t) & \text{if } m \text{ is even} \\ \frac{n}{C_m}\left(\frac{(C_m+\alpha)(n-\alpha+1)}{n(n-\alpha+1-t)}\right)^{\alpha} H_m(n,t) & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \frac{n}{t}\left(\frac{(t+\alpha)(n-\alpha+1)}{n(n-\alpha+1-t)}\right)^{\alpha} H_m(n,t) & \text{in all other cases,} \end{cases} \end{aligned}$$

其中 $0 < C_m$ 是一个足够大的常数。采用与 [18, 命题 5.2] 中类似的计算，在这三种情况下均可得到 $A_m(n, 2t+1) = o(H_m(n, t)/n)$。 □

由此可推出关于当 $10\sqrt{\theta_m n} < t < n^{4/5}$ 时 t-Lee纠错码数量的结果。

定理 3.15。 设 $2 \le m$，$10\sqrt{\theta_m n} < t < n^{4/5}$，则对于充分大的 n，在 $\mathbb{Z}_m^n$ 中长度为 n 的 t-Lee纠错码数量渐近至多为 $2^{o(H_m(n,\ t))}$，

证明。 根据命题 3.14， t-Lee纠错码的数量至多为

$$\binom{m^n}{\le A_m(n, 2t+1)} \le 2^{(\log_2(m)) \cdot n \cdot o(H_m(n,t)/n)} = 2^{o(H_m(n,t))}.$$

□

在定理 3.15 中，我们对 t 得出了与 Dong 等人在 [18, 定理 1.1 (b)] 中针对汉明度量所得不同的限制。在汉明度量下， t 的区域为 $10\sqrt{n} < t \le (1 - q^{-1})n - C_q\sqrt{n\log(n)}$，其中某个常数为 $C_q > 0$，使得 $\mathbb{F}_q^n$ 中的 t-Lee纠错码数量至多为 $2^{o(H_{q(n,\ t))}}$。对于 t，该区域略大于我们的区域。汉明度量码对 t 的限制较少，这是因为引理 3.1] 中给出的体积比估计也取决于环境空间的大小。

4 二分图上的码计数

本节通过估计二分图中的孤立节点，确定 t-Lee纠错码数量的上界和下界。具体而言，我们定义了给定基数的这类码在相同基数的码集合中的密度函数。利用二分图模型，我们还可以考察 $\mathbb{Z}_p$ 上的线性码（ p 为素数时）。我们确定了密度函数的渐近行为，并得到了关于 Lee

度量码的密度结果，这些码在各种界的意义下都是最优的。令 $1 \le t \le \lfloor \frac{nm-2}{4} \rfloor$，并考虑密度函数

$$\delta_m^L(\mathbb{Z}_m^n, S, t) := \frac{|\{\mathscr{C} \subseteq \mathbb{Z}_m^n : |\mathscr{C}| = S,\, d^{\mathrm{L}}(\mathscr{C}) \ge 2t+1\}|}{|\{\mathscr{C} \subseteq \mathbb{Z}_m^n : |\mathscr{C}| = S\}|} \tag{4.1}$$

（可能是） $\mathbb{Z}_m^n$ 中的非线性 t-Lee纠错码，以及$\mathbb{Z}_p^n$ 中最小 Lee 距离至少为 $2t+1$的线性 t-Lee 纠错码的密度函数，记作

$$\delta_p^L[\mathbb{Z}_p^n, S, t] := \frac{|\{\mathscr{C} \le \mathbb{Z}_p^n : |\mathscr{C}| = S,\, d^{\mathrm{L}}(\mathscr{C}) \ge 2t+1\}|}{|\{\mathscr{C} \le \mathbb{Z}_p^n : |\mathscr{C}| = S\}|}. \tag{4.2}$$

请注意，非线性 Lee 度量码的基数 $2 \le |\mathscr{C}| \le m^n$可以是任意值，而线性码的基数则是 p的幂。

为了给出密度（4.1）和（4.2）的上界与下界，我们采用计数论证，统计相对于定义在二分图左侧节点上的某些映射而言为正则的二分图中孤立节点的数量。这种方法最初由 [23] 提出，并在 [22]应用于不同的度量和不同类型的线性结构。

我们回顾有限非空集合 $\mathscr{V}$上的关联概念，该集合的幅度为 $r \ge 0$ （见[23]）。关联是一个函数 α: $\mathscr{V} \times \mathscr{V} \to \{0,\dots,r\}$，满足以下条件:

(i) $\alpha(V,V) = r$ 对所有 $V \in \mathscr{V}$均成立;

(ii) $\alpha(V,V\prime) = \alpha(V\prime V)$ 对所有 $V, V\prime \in \mathscr{V}$均成立。

给定有限二分图 $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ 及其上的关联 α，其幅度为 r。若对于所有 $(V, V\prime) \in \mathscr{V} \times \mathscr{V}$，满足 $(V,W) \in \mathscr{E}$且 $(V\prime W) \in \mathscr{E}$的节点 $W \in \mathscr{W}$的数量仅取决于 $\alpha(V, V\prime)$，则称其为 $\mathscr{B}$ α-正则图 。于是将该数量记为 $\mathscr{W}_\ell(\alpha)$，其中$\ell = \alpha(V, V\prime) \in \{0, \dots, r\}$。

命题 4.1. [23, 引理 3.2 和引理 3.5]
设 $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ 是一个二分 α-正则图，其中 α 是 $\mathscr{V}$上的关联，幅度为r。设 $\mathscr{F} \subseteq \mathscr{W}$为 $\mathscr{W}$的非孤立节点集合族。若 $\mathscr{W}_r(\alpha) > 0$，则

(i) $|\mathscr{F}| \le |\mathscr{V}|\, \mathscr{W}_r(\alpha)$.

(ii) $|\mathscr{F}| \ge \frac{\mathscr{W}_r(\alpha)^2\, |\mathscr{V}|^2}{\sum_{\ell=0}^{r} \mathscr{W}_\ell(\alpha)\, |\alpha^{-1}(\ell)|}$.

4.1 非线性 Lee 度量码

首先给出 $\mathbb{Z}_m^n$ 中（可能是）非线性李度量码数量的界，其最小距离不小于 $2t+1$。

定理 4.2. 设 $S \ge 1$ 和 $1 \le t < +\infty$ 为整数。定义以下量

$$\begin{aligned}
\beta^0 &:= \frac{1}{2} m^n (\mathbf{v}_m^{\mathrm{L}}(n, 2t) - 1) - 2\mathbf{v}_m^{\mathrm{L}}(n, 2t) + 3, \\
\beta^1 &:= 2\mathbf{v}_m^{\mathrm{L}}(n, 2t) - 4, \\
\Theta &:= 1 + \beta^1 \frac{S-2}{m^n - 2} + \beta^0 \frac{(S-2)(S-3)}{(m^n-2)(m^n-3)},
\end{aligned}$$

并令 $\mathscr{F} := \{\mathscr{C} \subseteq \mathbb{Z}_m^n :\ |\mathscr{C}| = S,\ \ d^{\mathrm{L}}(\mathscr{C}) \le 2t\}$。我们有

$$\frac{1}{2\Theta} m^n (\mathbf{v}_m^{\mathrm{L}}(n, 2t) - 1) \binom{m^n - 2}{S-2} \le |\mathscr{F}| \le \frac{1}{2} m^n (\mathbf{v}_m^{\mathrm{L}}(n, 2t) - 1) \binom{m^n - 2}{S-2}.$$

证明。 证明类似于 [22, 定理 2.1], , 使用命题 4.1 中的两个界。

□

根据定理 4.2，我们可以推导出 $\mathbb{Z}_m^n$ 中 Lee 度量码的密度函数的以下渐近行为。

定理 4.3。设 $1 \le t < +\infty$。

i) 设 $n \ge 3$ 为整数。考虑序列 $(H_m(n, 2t+1))_{m\ge 2}$，其中每个 $H_m(n, 2t+1)$ 按照 (2.1) 中的定义，且 $(S_m)_{m\ge 2}$ 为整数序列，其中 $S_m \ge 1$ 对所有 $m \ge 2$ 均成立。我们有

$$\lim_{m\to+\infty} \delta_m^L(\mathbb{Z}_m^n, S_m, 2t+1) = \begin{cases} 1 & \text{if } S_m \in o(\sqrt{H_m(n,2t+1)}) \text{ as } m \to +\infty, \\ 0 & \text{if } S_m \in \omega(\sqrt{H_m(n,2t+1)}) \text{ as } m \to +\infty. \end{cases}$$

ii) 令 $m \ge 2$。考虑序列 $(H_m(n, 2t+1))_{n\ge 1}$，其中每个 $H_m(n, 2t+1)$ 的定义同 (2.1)，且 $(S_n)_{n\ge 1}$ 是整数序列，其中 $S_n \ge 1$ 对所有 $n \ge 1$ 均成立。我们有

$$\lim_{n\to+\infty} \delta_m^L(\mathbb{Z}_m^n, S_n, 2t+1) = \begin{cases} 1 & \text{if } S_n \in o(\sqrt{H_m(n,2t+1)}) \text{ as } n \to +\infty, \\ 0 & \text{if } S_n \in \omega(\sqrt{H_m(n,2t+1)}) \text{ as } n \to +\infty. \end{cases}$$

由定理 4.3 可立即得到球覆盖界（分别为吉尔伯特–瓦尔沙莫夫界）的以下结果。

推论 4.4. 均匀随机选取的 Lee 度量码满足球覆盖界的概率，在 $\mathbb{Z}_m^n$ 中当 $m \to +\infty$ 和 $n \to +\infty$ 时均趋于 0。

4.2 线性 Lee 度量码

本节考虑维数为 $k \le n$ 的线性码 $\mathscr{C} \subseteq \mathbb{Z}_p^n$。同样，我们先给出在 $\mathbb{Z}_p^n$ 中最小距离不小于 $2t+1$ 的线性李度量码数量的界。我们考虑与定理 2.3], 的证明中相同的二分图 [22, ，但由于元素 $x \in \mathbb{Z}_p^n$ 的李重量可能在数乘后增加，我们考虑 $\mathbb{Z}_p^n$ 中 Lee 距离不超过 $2t$ 的所有元素（零元素除外），而不是像 [22] 中那样考虑一维向量空间。因此，我们令该图的左侧节点集为 $\mathbf{B}_p^{\mathrm{L}}(n, 2t, 0) \setminus \{0\}$。此外，我们只考虑定义在 $\mathbb{Z}_p$ 上的线性李度量码，即定义在素数阶域上的码。这样做的原因是，如果左侧节点集 $\mathscr{B}$ 中的元素具有不同的阶，图的正则性条件便无法满足；而当我们考虑定义在 $\mathbb{Z}_{p^s}$ 上的码时，情况正是如此，其中 $s > 1$.

定理 4.5。设 $1 \le k \le n$ 和 $1 \le t < +\infty$ 为整数，且 $\mathscr{F} := \{\mathscr{C} \subseteq \mathbb{Z}_p^n : \dim(\mathscr{C}) = k,\ d^{\mathrm{L}}(\mathscr{C}) \le 2t\}$。我们有

$$\frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p^2}{\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_p (\mathbf{v}_p^{\mathrm{L}}(n,2t)-p) + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p (p-1)} \le |\mathscr{F}| \le (\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p.$$

证明。我们考虑二分图 $\mathscr{B} = (\mathscr{V},\ \mathscr{W},\ \mathscr{E})$，其中 $\mathscr{V} = \mathbf{B}_p^{\mathrm{L}}(n,\ 2t,\ 0) \setminus \{0\}$，$\mathscr{W} = \{\mathscr{C} \subseteq \mathbb{Z}_p^n : \dim(\mathscr{C}) = k\}$ 和 $\mathscr{E} = \{(c,\ \mathscr{C}) \in \mathscr{V} \times \mathscr{W} :\ c \in \mathscr{C}\}$。我们有

$$|\mathscr{V}| = \mathbf{v}_p^{\mathrm{L}}(n,2t) - 1, \quad |\mathscr{W}| = \begin{bmatrix} n \\ k \end{bmatrix}_p.$$

很容易看出， $\mathscr{B}$ 是度为

$$\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p.$$

应用命题 4.1，我们得到 $|\mathscr{F}|$ 的一个上界。

为证明下界，我们考虑该关联

$$\alpha : \mathscr{V} \times \mathscr{V} \to \{0,1\}, \quad (V,V') \mapsto 2 - \dim\langle V, V'\rangle.$$

这里我们得到

$$|\alpha^{-1}(0)| = |\mathscr{V}|(|\mathscr{V}| - (p-1)), \quad |\alpha^{-1}(1)| = |\mathscr{V}|(p-1)$$

且 $\mathscr{B}$ 是 α-正则的。此外，我们有

$$\mathscr{W}_0(\alpha) = \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_p, \ \mathscr{W}_1(\alpha) = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p,$$

结合命题 4.1 后，可推出下界。 □

As 由此可立即得到密度函数的以下界。

推论 4.6。 设 $1 \le k \le n$ 和 $1 \le t < +\infty$ 为整数。我们有

$$1 - \frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p}{\begin{bmatrix} n \\ k \end{bmatrix}_p} \le \delta_p^L[\mathbb{Z}_p^n, p^k, 2t+1] \le 1 - \frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p}{\bar{\Theta}\begin{bmatrix} n \\ k \end{bmatrix}_p}, \tag{4.3}$$

其中

$$\bar{\Theta} = (p-1) + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p^{-1} (\mathbf{v}_p^{\mathrm{L}}(n,2t)-p)\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_p.$$

由推论 4.6，我们可以推导出 $\mathbb{Z}_p^n$ 中线性 Lee 度量码密度的以下渐近行为。

定理 4.7. 设 $1 \le t < +\infty$ 为整数。

1. 设 $1 \le k < n$ 为整数，则 $\lim_{p\to+\infty} \delta_p^L[\mathbb{Z}_p^n, p^k, 2t+1] = 1$.

2. 设 $p \in P$，固定码率 $R \in [0,1)$，使得 $k(n) = Rn$. 于是 $\lim_{n\to+\infty} \delta_p^L[\mathbb{Z}_p^n, p^{k(n)}, 2t+1] = 1$.

证明。 考虑 4.3 中给出的下界，并利用q-二项式系数的渐近估计，我们得到

$$\frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p}{\begin{bmatrix} n \\ k \end{bmatrix}_p} \sim \frac{\mathbf{v}_p^{\mathrm{L}}(n,2t)p^k}{p^n},$$

b无论作为 $p \to +\infty$ 还是作为 $n \to +\infty$。现在，这两个结论可由引理 2.11 得出 . □

因此，当固定 n， k 和 t 时，线性 t-Lee 纠错码的比例会在 p 趋于无穷时趋近于 1。由上面的推论可知，大多数码都具有较大的距离。

然而，达到定理 2.8 中界的码在 $n \to +\infty$ 和 $p \to +\infty$中都很稀少。这一点在 [13]中已有观察。不过，由于这是目前已知关于线性码最小 Lee 距离的最紧界，我们将聚焦于此界，并用我们更一般的技术验证 [13] 中的结果。在经典情形下，Plotkin 界远比 Singleton 界宽松。达到最优的线性码是常重量码，而其非线性对应码称为等距码。它们有多种应用（例如，[14, 16, 34, 24], 它们与 Steiner系统密切相关（例如， [17, 10]），而且由于它们与极小码有关， [4] 也应用于秘密共享方案（例如，参见 [9]）。Lee度量下的情况则略有不同：Lee度量 Plotkin 界最初由 Wyner 和 Graham 提出， [42], 后来由 Chiang 和 Wolf 改进， [15] 最终由 Byrne 和 Weger 于 [13]进一步改进。因此，Lee度量 Plotkin 界比 Lee度量 Singleton 界得到更广泛的研究，且界限也紧得多。常数李重量码最早由 Wood 研究， [41] 其刻画和密度问题已在 [13]中得到完整研究。这类码的应用领域与经典码类似。

定理 4.8。 设 $1 \le t \le \lfloor \frac{nm-2}{4} \rfloor$ 为一个整数。

(i) 设 $1 \le n$为一个整数，则 $\lim_{p\to+\infty} \delta_p^L[\mathbb{Z}_p^n, p^{n-\frac{8t+4}{p+1}+1}, t] = 0.$

(ii) Let $p \in P$, then $\lim_{n\to+\infty} \delta_p^L[\mathbb{Z}_p^n, p^{n-\frac{8t+4}{p+1}+1}, t] = 0.$

证明。 回顾 [22, 引理 3.4] 中关于 q-项二项式系数的渐近估计，很容易看出，对于 (4.5) 中给出的上界，我们有

$$\frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p}{\bar{\Theta}\begin{bmatrix} n \\ k \end{bmatrix}_p} \sim \frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)}{p^{n-k}(p-1)+\mathbf{v}_p^{\mathrm{L}}(n,2t)-p},$$

当 $p \to +\infty$ 和 $n \to +\infty$ 时均成立。令 $k = n - \frac{8t+4}{p+1} + 1$，得到

$$\lim_{p\to+\infty} \frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)}{p^{\frac{8t+4}{p+1}-1}(p-1)+\mathbf{v}_p^{\mathrm{L}}(n,2t)-p} = 1,$$

and

$$\lim_{n\to+\infty} \frac{(\mathbf{v}_p^{\mathrm{L}}(n,2t)-1)}{p^{\frac{8t+4}{p+1}-1}(p-1)+\mathbf{v}_p^{\mathrm{L}}(n,2t)-p} = 1.$$

利用推论 4.6，即可得出该结论。 □

对于码率为 R 的线性码，我们可以将球覆盖 或*Gilbert-Varshamov (GV)* 界 重新表述为

$$R \ge 1 - \frac{1}{n}\log_p(\mathbf{v}_p^{\mathrm{L}}(n,2t)),$$

这等价于

$$\log_p(\mathbf{v}_p^{\mathrm{L}}(n,2t)) \ge n(1-R). \tag{4.4}$$

下文将研究达到界 (4.4)（关于 p 或 n）的码的渐近行为。

定理 4.9。 设 $1 \le t \le \lfloor \frac{nm-2}{4} \rfloor$ 为整数。设 $\mathscr{C} \subseteq \mathbb{Z}_p^n$ 为码率为$R = 1 - \frac{1}{n}\log_p(\mathrm{v}_p^{\mathrm{L}}(n, 2t))$的线性李度量码。那么， $\mathscr{C}$的最小距离至少为 $2t+1$（即该码满足吉尔伯特–瓦尔沙莫夫界）的概率趋近于 1，当 $p \to +\infty$ 时。

证明。 该结论由 $k(n) = Rn < n$ 和定理 4.7 得出。 □

若考虑 n 趋于无穷大，则均匀随机选取的线性李度量码达到吉尔伯特–瓦尔沙莫夫界的概率至多为 $\frac{p-2}{p-1}$，且下界为 0。然而，若加入一个 ε-环境，则可得：

定理 4.10。 设 $1 \le t \le \lfloor \frac{nm-2}{4} \rfloor$ 为整数， $0 < \varepsilon$，且 $\mathscr{C} \subseteq \mathbb{Z}_p^n$ 为一个码率为 $R = 1 - \frac{1}{n}\log_p(\mathrm{v}_p^{\mathrm{L}}(n, 2t)) - \varepsilon$的线性李度量码，且该码是均匀随机选取的。那么，对于 $n \to +\infty$， $\mathscr{C}$的最小距离至少为 $2t+1$ 的概率趋于 1。

证明。 令 $k := k(n) = Rn$，并考虑 4.3 中的下界，可得

$$\frac{(\mathrm{v}_p^{\mathrm{L}}(n, 2t) - 1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_p}{\begin{bmatrix} n \\ k \end{bmatrix}_p} \sim \frac{1}{p^{\varepsilon n}}.$$

对于 $n \to +\infty$，该陈述成立。 □

前述定理与 [11], 中关于 Gilbert–Varshamov 界的渐近行为结果相吻合；其中，对于由可加权产生的一般度量（包括汉明度量、齐次度量和 Lee度量），相应结论已得到证明。

5 结论

根据 Python 对小参数的计算结果，即 $m = 4$, 5, $t \le 3$ 和 $n \le 20$, 我们观察到，在所有情况下，通过图容器得到的 t-Lee纠错码数量上界都比通过二分图得到的上界更紧。然而，要证明更强的界 $2^{O(A_m(n,\ 2t+1)}$ 对任意固定的 $0 < c$ 在 $2t + 1 < (1 - m^{-1} - c)n$ 时成立，要困难得多，因为必须证明：大小远大于 $A_m(n,\ 2t+1)$ 的集合中，必然存在许多对距离不超过 $2t+1$ 的元素。在 H- 自由图的背景下，这个更强的界是 Kleitman 和 Winston 在 [27], 中提出的一个著名猜想，该猜想也促成了容器算法的发展。我们认为，对于研究达到某个给定界的码的数量而言，该算法仍然非常有趣。事实上，可以将这些结果推广并转换到其他界，即 Singleton 界或 Plotkin 界，并随后利用这些界作为码大小的替代指标，以寻找可用于容器算法的饱和估计。然而，这将超出本文的范围；我们最初感兴趣的是刻画具有相同 Lee 半径且其中心之间距离为 ℓ 的两个球的交集。由于我们关于两个李度量球交集大小的上界仅取决于李体积，而李体积已有显式公式，因此可以快速计算；我们建议利用这些结果来研究 Lee 度量码的覆盖性质。

6 致谢

Violetta Weger 获得欧盟“地平线2020”研究与创新计划资助，资助项目为玛丽·斯克沃多夫斯卡-居里资助协议，编号 899987。

参考文献

[1] A. Abiad 和 H. Koerts，图乘积的独立数，Discussiones Math- ematicae Graph Theory。[2] T. L. Alderson 和 S. Huntemann，最大 Lee 距离码，《Journal of Discrete Mathematics》2013 (2013)。[3] J. Antrobus 和 H. Gluesing-Luerssen，极大 Ferrers图码：构造与一般性考量，《IEEE信息论汇刊》65 (2019)，第 10 期，6204–6223。[4] A. Ashikhmin 和 A. Barg，线性码中的极小向量，《IEEE信息论汇刊》44 (1998)，第 5 期，2010–2017。[5] H. Astola，纠错码的代数与组合方法及其在容错逻辑中的应用，博士论文，坦佩雷理工大学，2015年。[6] J. Astola，Lee码理论，拉彭兰塔理工大学物理与数学系，研究报告 (1982年)。[7] J. Balogh、A. Treglown 和 A. Z. Wagner，图容器在布尔格中的应用，《Random Structures and Algorithms》49 (2016)，第 4 期，845–872。[8] A. Barg 和 G. D. Forney，随机码：最小距离与错误指数，《IEEE信息论汇刊》48 (2002)，第 9 期，2568–2573。[9] A. Beimel，秘密共享方案：综述，《编码与密码学：第三届国际研讨会 IWCC 2011》，中国青岛，2011年5月30日至6月3日。论文集 3，施普林格，2011年，第 11–46 页。.[10] M. Braun、T. Etzion、P. R. J. Osterg˚ard、A. Vardy 和 A. Wassermann，Steiner系统的类比形式的存在性，《Forum of Mathematics, Pi》，第 4 卷，剑桥大学出版社，2016年，第 e7 页。[11] E. Byrne、A.-L. Horlemann、K. Khathuria 和 V. Weger，有限链环上自由模的密度，《Linear Algebra and its Applications》651 (2022)，1–25。[12] E. Byrne 和 A. Ravagnani，划分平衡码族与编码理论中的渐近计数，《Journal of Combinatorial Theory, Series A》171 (2020)，105169。[13] E. Byrne 和 V. Weger，Lee度量中的界与最优码，《Finite Fields and Their Applications》87 (2023)，102151。[14] A. R. Calderbank、M. A. Herro 和 V. Telang，无直流分量线路码设计的多级方法，《IEEE信息论汇刊》35 (1989)，第 3 期，579–583。[15] J. C. Y. Chiang 和 J. K. Wolf，Lee度量的信道与码，《Information and Control》19 (1971)，第 2 期，159–173。[16] F. R. K. Chung、J. A. Salehi 和 V. K. Wei，光正交码：设计、分析与应用，《IEEE信息论汇刊》35 (1989)，第 3 期，595–604。[17] C. J. Colbourn 和 R. Mathon，Steiner系统，《组合设计手册》，Chapman and Hall/CRC，2006年，第 128–135 页。[18] D. Dong、N. Mani 和 Y. Zhao，纠错码的数量，arXiv 预印本 arXiv:2205.12363 (2022年)。

[19] E. N. Gilbert, 《信号字母表的比较》, 《贝尔系统技术期刊》31（1952年）, 第3期, 504–522页。[20] H. Gluesing-Luerssen, 《关于某些线性最大秩距码的稀疏性》, Linear Algebra and its Applications 596（2020年）, 145–168页。[21] R. L. Graham、D. E. Knuth、O. Patashnik 和 S. Liu, 《具体数学：计算机科学基础》, 《物理学中的计算机》3（1989年）, 第5期, 106–107页。[22] A. Gruica、A.-L. Horlemann、A. Ravagnani 和 N. Willenborg, 《平移不变度量空间中不同线性度码的密度》, arXiv预印本 arXiv:2208.10573（2022年）。[23] A. Gruica 和 A. Ravagnani, 《线性子空间的公共补空间与最大秩距码的稀疏性》, 《SIAM应用代数与几何杂志》6（2022年）, 第2期, 79–110页。[24] L. Gyorfi、J. L. Massey 等, 《二元恒重循环码与循环可置换码的构造》, IEEE信息论汇刊38（1992年）, 第3期, 940–949页。[25] J.-L. Kim 和 S.-J. Kim, 《使用最优李码对圈的笛卡尔积进行2-距离着色》, Discrete applied mathematics 159（2011年）, 第18期, 2222–2228页。[26] D. J. Kleitman 和 K. J. Winston, 《格的渐近数量》, 《组合数学、最优设计及其应用》（J. Srivastava 编）, 《离散数学年刊》6（1980年）, 243–249页。[27] ———, 《无4-圈图的数量》, 《离散数学》41（1982年）, 第2期, 167–172页。[28] P. Loidreau, 《有限域上秩度量码的渐近行为》, 《设计、编码与密码学》71（2014年）, 105–118页。[29] A. Neri、A.-L. Horlemann-Trautmann、T. Randrianarisoa 和 J. Rosenthal, 《关于最大秩距码和Gabidulin码的普遍性》, 《设计、编码与密码学》86（2018年）, 第2期, 341–363页。[30] C. Ott、H. Liu 和 A. Wachter-Zeh, 《和秩度量中球的几何性质》, arXiv预印本 arXiv:2303.11887 （ 2023 年）。[31] J. Pierce, 《随机线性码最小距离的极限分布》, IEEE信息论汇刊13（1967年）, 第4期, 595–599页。[32] S. Ritterhoff、G. Maringer、S. Bitzer、V. Weger、P. Karl、T. Schamberger、J. Schupp 和 A. Wachter-Zeh, 《FuLeeca：一种基于李度量的签名方案》, 密码学电子印刷档案（2023年）。[33] R. M. Roth, 《编码理论导论》, 《IET通信》47（2006年）, 第18–19期, 4页。[34] K. Schouhamer-Immink, 《数字录音机的编码技术》, Prentice Hall专业技术参考书, 1991年。[35] K. Shiromoto, 《有限环上码的Singleton界》, 《代数组合学杂志》12（2000年）, 95–99页。[36] P. Sol´e, 《关于李距离和模距离码的参数》, 《离散数学》89（1991年）, 第2期, 185–194页。

[37] R. P. Stanley, 《组合枚举学》，第2版，第1卷，剑桥大学出版社，2011年。[38] J. H. Van Lint, 《编码理论导论》，第86卷，施普林格科学与商业媒体，1998年。[39] R. R. Varshamov, 《纠错码中信号数量的估计》，《苏联科学院学报》**117**（1957年），739–741页。[40] V. Weger、P. Santini、M. Battaglioni 和A.-L. Horlemann, 《李度量码的*NP*完全问题》，arXiv预印本 arXiv:2002.12785（2020年）。[41] J. Wood, 《恒重线性码的结构》，《美国数学会汇刊》**354**（2002年），第3期，1007–1026页。[42] A. D. Wyner 和 R. L. Graham, 《关于最小距离的一个上界》 k元码，《Information and Control》**13** （1968年），第1期，47–52页。

A 附录

引理 A.1. 设 $1 \leq n, t,\ 2 \leq m, 0 \leq i \leq t$和 $0 \leq r \leq m-1$为满足$r = 2t - m\lfloor \frac{2t}{m} \rfloor$的整数。那么

1. $\left\lfloor \frac{2(t-1}{m} \right\rfloor = \left\lfloor \frac{2t}{m} \right\rfloor$)若 $r \geq 2$.

2. 若 m 是偶数 , r 也是偶数。

3. 若 m 是奇数且 $r \leq 1$，则有

$$\binom{n - \lfloor \frac{2t}{m} \rfloor}{t - \lfloor \frac{2t}{m} \rfloor (\lfloor \frac{m}{2} \rfloor + 1) - i} = \binom{n - \lfloor \frac{2t}{m} \rfloor}{-\frac{2t - r(m+1)}{2m} - i} = \begin{cases} 1 & \text{if } 2t = m+1 \text{ and } i = 0 \\ 0 & \text{else} \end{cases}.$$

证明。 不难看出

$$\left\lfloor \frac{2(t-1)}{m} \right\rfloor = \left\lfloor \frac{2t}{m} \right\rfloor \text{ if } r \geq 2.$$

此外，如果 m是偶数（且 $m' := m/2 \in \mathbb{N}$），则有 $r = 2t - 2m'\lfloor \frac{2t}{2m'} \rfloor = 2(t - m'\lfloor \frac{t}{m'} \rfloor)$，即 r也是偶数。对于 $r = 0$，我们得到$\frac{m}{2}\lfloor \frac{2t}{m} \rfloor = t$；对于 $r = 1$，我们得到 $\frac{m}{2}\lfloor \frac{2t}{m} \rfloor = t - \frac{1}{2}$。当 m为奇数且 $r < 2$ 时，有

$$\left\lfloor \frac{m+2}{2} \right\rfloor \left\lfloor \frac{2t}{m} \right\rfloor = \frac{m+1}{2} \left\lfloor \frac{2t}{m} \right\rfloor = \frac{(2t-r)(m+1)}{2m} = t + \frac{t}{m} - r\frac{m+1}{2m} \in \left\{ t + \frac{t}{m}, t + \frac{2t-m-1}{2m} \right\},$$

从而得证。 □

引理 *2.12* 的证明。 我们先求出参数 n和 t 均变化时体积的比值，并从 m 为偶数的情形开始。我们有

$$\begin{aligned} &\frac{\mathbf{v}_m^{\mathrm{L}}(n-1, t-1)}{\mathbf{v}_m^{\mathrm{L}}(n, t)} \\ &\leq \frac{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n-1}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)}{\sum_{i=0}^{\lfloor \frac{2t}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^{j+1} \binom{n}{j+1} \binom{t-\frac{mi}{2}}{j+1} \right)} \end{aligned}$$

$$
\begin{aligned}
&\leq \frac{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)}{\sum_{i=0}^{\lfloor \frac{2t}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^{j+1} \binom{n}{j+1} \binom{t-\frac{mi}{2}}{j+1} \right)} \\
&\overset{(*)}{\leq} \frac{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)}{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \cdot 2 \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \left(\frac{n}{j+1} \right) \binom{t-1-\frac{mi}{2}}{j} \left(\frac{t-\frac{mi}{2}}{j+1} \right) \right)} \\
&\leq \frac{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)}{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \left(\frac{2n}{t-\frac{mi}{2}} \right) \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)} \\
&\leq \frac{\sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)}{\left(\frac{2n}{t} \right) \sum_{i=0}^{\lfloor \frac{2(t-1)}{m} \rfloor} (-1)^i \binom{n}{i} \left(\sum_{j=0}^{t-1-\frac{mi}{2}} 2^j \binom{n-1}{j} \binom{t-1-\frac{mi}{2}}{j} \right)} \\
&\leq \left(\frac{t}{2n} \right),
\end{aligned}
$$

其中 **(*)** 可由引理 2.1 推得，因为要么 $\lfloor \frac{2t}{m} \rfloor = \lfloor {}^{2}{}_{(t-1)_m} \rfloor$，要么 $m \lfloor \frac{2t}{m} \rfloor = 2t$（见引理 A.1）。后一种情况下，分母中关于 $i = \lfloor 2t/m \rfloor$ 的被加数等于零。

迭代地，这给出了

$$
\frac{\mathbf{v}_m^{\mathrm{L}}(n,t)}{\mathbf{v}_m^{\mathrm{L}}(n+i,t+i)} \leq \left(\frac{t+i}{2(n+i)} \right) \cdot \left(\frac{t+i-1}{2(n+i-1)} \right) \cdot \cdots \cdot \left(\frac{t+1}{2(n+1)} \right) \leq \left(\frac{t+i}{2(n+i)} \right)^i.
$$

对于 m 为奇数且除 $2t = m+1$ 之外的所有情况，结合引理 A.1 可得

$$
\begin{aligned}
&\frac{\mathbf{v}_m^{\mathrm{L}}(n-1,t-1)}{\mathbf{v}_m^{\mathrm{L}}(n,t)} \\
&\leq \frac{\sum_{i=0}^{t-1} \binom{n}{i} \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n-1}{j} \binom{n-j-1}{t-j(\lfloor m/2 \rfloor+1)-i-1}}{\sum_{i=0}^{t} \binom{n+1}{i} \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i}} \\
&\overset{(*)}{=} \frac{\sum_{i=0}^{t-1} \binom{n+1}{i+1} \left(\frac{i+1}{n+1} \right) \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \left(\frac{n-j}{n} \right) \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i} \left(\frac{t-j(\lfloor m/2 \rfloor+1)-i}{n-j} \right)}{\sum_{i=0}^{t} \binom{n+1}{i+1} \left(\frac{i+1}{n+1-i} \right) \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i}} \\
&\leq \frac{\sum_{i=0}^{t-1} \binom{n+1}{i+1} \left(\frac{i+1}{n+1} \right) \left(\frac{t-i}{n} \right) \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i}}{\sum_{i=0}^{t-1} \binom{n+1}{i+1} \left(\frac{i+1}{n+1-i} \right) \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i}} \\
&\leq \frac{\sum_{i=0}^{t-1} \binom{n+1}{i+1} \left(\frac{i+1}{n+1} \right) \left(\frac{t}{n} \right) \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i}}{\sum_{i=0}^{t-1} \binom{n+1}{i+1} \left(\frac{i+1}{n+1} \right) \sum_{j=0}^{\lfloor 2(t-1)/m \rfloor} (-2)^j \binom{n}{j} \binom{n-j}{t-j(\lfloor m/2 \rfloor+1)-i}} \\
&= \frac{t}{n},
\end{aligned}
$$

其中，**(*)** 由引理 2.1 得出。迭代进行这一过程可得到

$$
\frac{\mathbf{v}_m^{\mathrm{L}}(n,t)}{\mathbf{v}_m^{\mathrm{L}}(n+i,t+i)} \leq \left(\frac{t+i}{n+i} \right) \cdot \left(\frac{t+i-1}{n+i-1} \right) \cdot \cdots \cdot \left(\frac{t+1}{n+1} \right) \leq \left(\frac{t+i}{n+i} \right)^i.
$$

对于 $2t = m+1$ 的情况，我们有

$$
\frac{\mathbf{v}_m^{\mathrm{L}}(n-1,t-1)}{\mathbf{v}_m^{\mathrm{L}}(n,t)}
$$

$$
\begin{aligned}
&\leq \frac{\sum_{i=0}^{t-1}\binom{n+1}{i}\binom{n-1}{t-i-1}}{\sum_{i=0}^{t-1}\binom{n+1}{i}\left(-2n+\left(\frac{n}{t-i}\right)\binom{n-1}{t-i-1}\right)+\binom{n+1}{t}(1-2n)} \\
&= \frac{\sum_{i=0}^{t-1}\binom{n+1}{i}\binom{n-1}{t-i-1}-2t\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)+\binom{n+1}{t}\left(\frac{t}{n}\right)+2t\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)-\binom{n+1}{t}\left(\frac{t}{n}\right)}{\left(\frac{n}{t}\right)\left(\sum_{i=0}^{t-1}\binom{n+1}{i}\binom{n-1}{t-i-1}-2t\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)+\binom{n+1}{t}\left(\frac{t}{n}\right)\right)} \\
&= \frac{t}{n}+\frac{\frac{2t^2}{n}\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)-\binom{n+1}{t}\left(\frac{t^2}{n^2}\right)}{\sum_{i=0}^{t-1}\binom{n+1}{i}\binom{n-1}{t-i-1}-2t\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)+\binom{n+1}{t}\left(\frac{t}{n}\right)}.
\end{aligned}
$$

此外

$$
\begin{aligned}
&\frac{\frac{2t^2}{n}\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)-\binom{n+1}{t}\left(\frac{t^2}{n^2}\right)}{\sum_{i=0}^{t-1}\binom{n+1}{i}\binom{n-1}{t-i-1}-2t\left(\sum_{i=0}^{t-1}\binom{n+1}{i}+\binom{n+1}{t}\right)+\binom{n+1}{t}\left(\frac{t}{n}\right)} \\
&\overset{(*)}{\leq} \frac{\frac{2t^2}{n}\left(\sum_{i=0}^{t-1}\left(\frac{e(n+1)}{i}\right)^i+\left(\frac{e(n+1)}{t}\right)^t\right)-\left(\frac{n+1}{t}\right)^t\left(\frac{t^2}{n^2}\right)}{\sum_{i=0}^{t-1}\left(\frac{n+1}{i}\right)^i\left(\frac{n-1}{t-i-1}\right)^{t-i-1}-2t\left(\sum_{i=0}^{t-1}\left(\frac{e(n+1)}{i}\right)^i+\left(\frac{e(n+1)}{t}\right)^t\right)+\left(\frac{n+1}{t}\right)^t\left(\frac{t}{n}\right)} \\
&\in O(n^{-1}),
\end{aligned}
$$

其中 (*) 用到了引理 2.1。因此

$$
\frac{\mathbf{v}_m^{\mathrm{L}}(n-1,t-1)}{\mathbf{v}_m^{\mathrm{L}}(n,t)} \leq \frac{C_m}{n},
$$

对于充分大的常数 C_m. 因此,

$$
\begin{aligned}
\frac{\mathbf{v}_m^{\mathrm{L}}(n,t)}{\mathbf{v}_m^{\mathrm{L}}(n+i,t+i)} &= \frac{\mathbf{v}_m^{\mathrm{L}}(n,t)}{\mathbf{v}_m^{\mathrm{L}}(n+1,t+1)}\cdot\frac{\mathbf{v}_m^{\mathrm{L}}(n+1,t+1)}{\mathbf{v}_m^{\mathrm{L}}(n+2,t+2)}\cdots\frac{\mathbf{v}_m^{\mathrm{L}}(n+i-1,t+i-1)}{\mathbf{v}_m^{\mathrm{L}}(n+i,t+i)} \\
&\leq \left(\frac{C_m}{n+i}\right)^i.
\end{aligned}
$$

这证明了第一个结论。

现在我们将确定仅参数 t 变化时的比值。

若 m 是偶数，则有

$$
\begin{aligned}
\frac{\mathbf{v}_m^{\mathrm{L}}(n,t)}{\mathbf{v}_m^{\mathrm{L}}(n-i,t)} &= \frac{\sum_{k=0}^{\lfloor 2t/m\rfloor}(-1)^k\binom{n}{k}\sum_{j=0}^{t-\lfloor m/2\rfloor k}2^j\binom{n}{j}\binom{t-\lfloor m/2\rfloor k}{j}}{\sum_{k=0}^{\lfloor 2t/m\rfloor}(-1)^k\binom{n-i}{k}\sum_{j=0}^{t-\lfloor m/2\rfloor k}2^j\binom{n-i}{j}\binom{t-\lfloor m/2\rfloor k}{j}} \\
&\overset{(*)}{\leq} \frac{\sum_{k=0}^{\lfloor 2t/m\rfloor}(-1)^k\binom{n}{k}}{\sum_{k=0}^{\lfloor 2t/m\rfloor}(-1)^k\left(\frac{n-i+1-k}{n-i+1}\right)\cdot\cdots\cdot\left(\frac{n-k}{n}\right)\binom{n}{k}\cdot\left(\frac{n-i+1-t+\lfloor m/2\rfloor k}{n-i+1}\right)^i} \\
&\leq \left(\frac{n-i+1}{n-i+1-t}\right)^i,
\end{aligned}
$$

其中 (*) 是对引理 2.1 的迭代应用。将此与

$$
\mathbf{v}_m^{\mathrm{L}}(n-i,t) \leq \left(\frac{t+i}{2n}\right)^i \mathbf{v}_m^{\mathrm{L}}(n,t+i)
$$

由引理 2.12 可得最终结论。

对于 m 为奇数的情况，我们将其最大化

$$\left(\frac{n-i+1}{n-i+1-j}\right)^i\left(\frac{n-i-j+1}{n-i-j+1-t+j(\lfloor m/2\rfloor+1)+k}\right)^i\left(\frac{n-i+2}{n-i+2-k}\right)^i$$

在约束 $0\le j\le\lfloor 2t/m\rfloor$ 和 $0\le k\le t$ 下，并得到

$$\frac{\mathbf{v}_m^{\mathrm{L}}(n,t)}{\mathbf{v}_m^{\mathrm{L}}(n-i,t)}=\frac{\sum_{k=0}^{t}\binom{n+1}{k}\sum_{j=0}^{\lfloor 2t/m\rfloor}(-2)^j\binom{n}{j}\binom{n-j}{t-j(\lfloor m/2\rfloor+1)-k}}{\sum_{k=0}^{t}\binom{n-i+1}{k}\sum_{j=0}^{\lfloor 2t/m\rfloor}(-2)^j\binom{n-i}{j}\binom{n-i-j}{t-j(\lfloor m/2\rfloor+1)-k}}\le\left(\frac{n-i+1}{n-i+1-t}\right)^i.$$

利用引理 2.12 的第一部分，我们推导出该结论。 □

引理 *3.2* 的证明。对于 $x\in\mathbb{Z}_m^n$，令 $K_x:=\{y\in\mathscr{C}\colon d^{\mathrm{L}}(x,\ y)\le t\}$。然后

$$\sum_{r=1}^{2t}W(t,r)|E_r|=\sum_{x\in\mathbb{Z}_m^n}\binom{|K_x|}{2},$$

因为这两项都在计数形如 $(x,\{y,z\})$,的配对，其中 $x\in\mathbb{Z}_m^n$ 和 $y,z\in\mathscr{C}$ 彼此不同，且满足 $d^{\mathrm{L}}(x,y)$ $d^{\mathrm{L}}(x,z)\le t$。引理 2.14 和 2.16 给出

$$W(t,r)\le W(t,1)\le m\mathbf{v}_m^{\mathrm{L}}(n-1,t-1)\le\begin{cases}\frac{mt\mathbf{v}_m^{\mathrm{L}}(n,t)}{2n} & \text{if } m \text{ is even,}\\ \frac{mC_m\mathbf{v}_m^{\mathrm{L}}(n,t)}{n} & \text{if } m \text{ is odd and } t=\lceil\frac{m}{2}\rceil,\\ \frac{mt\mathbf{v}_m^{\mathrm{L}}(n,t)}{n} & \text{in all other cases,}\end{cases}\tag{A.1}$$

对于 $1\le r\le 2t$。所有 $x\in\mathbb{Z}_m^n$ 的 K_x 平均值为 $\frac{|\mathscr{C}|\mathbf{v}_m^{\mathrm{L}}(n,t)}{m^n}$。因此，由引理 2.1 给出的下界可得

$$\frac{|\mathscr{C}|^2\mathbf{v}_m^{\mathrm{L}}(n,t)^2}{10m^n}\le m^n\binom{|\mathscr{C}|\mathbf{v}_m^{\mathrm{L}}(n,t)/m^n}{2}\le\sum_{x\in\mathbb{Z}_m^n}\binom{|K_x|}{2}=\sum_{r=1}^{2t}W(t,r)|E_r|.\tag{A.2}$$

这证明了引理的第一个不等式。注意到 $\sum_{r=1}^{2t}W(t,r)|E_r|\le W(t,1)|E|$，整理并结合不等式 (A.1) 和 (A.2)，即可推出第二个不等式。

□

引理 *3.4* 的证明。设 $v\in\mathscr{C}_1$ 为$\mathbf{B}_m^{\mathrm{L}}(n,\ t,\ v)$与其他球$\mathbf{B}_m^{\mathrm{L}}(n,\ t,\ u)$ $u\in\mathscr{C}_1$的重叠，其大小为

$$\left|\mathbf{B}_m^{\mathrm{L}}(n,t,v)\cap\bigcup_{u\in\mathscr{C}_1\setminus\{v\}}\mathbf{B}_m^{\mathrm{L}}(n,t,u)\right|\le\sum_{r=1}^{2t}\deg_r(v)W(t,r)\le\left(\sum_{r=1}^{20}\deg_r(v)W(t,r)\right)+n^5W(t,21),\tag{A.3}$$

由引理 2.14。根据引理 2.16，在所有情况下都有 $W(t,r)\lesssim n^{-\lceil r/2\rceil/2}\mathbf{v}_m^{\mathrm{L}}(n,t)$。当 n 足够大时，可得 $n^5W(t,21)\lesssim\epsilon\mathbf{v}_m^{\mathrm{L}}(n,t)$。此外，根据 $\mathscr{C}_1$ 的定义，即对每个 $v\in\mathscr{C}$, $1\le r\le 20$，$\deg_r(v)$ $\le\varepsilon n^{\lceil r/2\rceil/2}$，和式 (A.3) 为 $\lesssim\varepsilon\mathbf{v}_m^{\mathrm{L}}(n,t)$。因此，对于每个 $v\in\mathscr{C}_1$，球 $\mathbf{B}_m^{\mathrm{L}}(n,t,v)$ 都包含 $(1-O(\varepsilon))\mathbf{v}_m^{\mathrm{L}}(v,t)$ 个不与其他此类球共享的唯一点，因此这些球的并集大小为 $\ge(1-O(\varepsilon))\mathbf{v}_m^{\mathrm{L}}(n,t)$ $|\mathscr{C}_1|$. 。由于此并集包含于 $\mathbb{Z}_m^n$，根据汉明界的定义，可得 $|\mathscr{C}_1|\le(1+O(\varepsilon))H_m(n,t)$。 □

引理 *3.5* 的证明。取一个大小为 $X \subseteq \mathscr{C}_2$ 的最大子集，其中 X 中任意两个不同元素之间的 Lee 距离都大于 t。对于每个 $x \in X$，都可以找到一个含有 n 的 $\lceil \log(n)/\varepsilon \rceil$ 元素子集 $A_x \subseteq \mathscr{C} \cap \mathbf{B}_m^{\mathrm{L}}(n, 20, x)$。对于不同的 $x, y \in X$，有 $d(x,y) > t \geq 60$，因此 $A_x \cap A_y = \emptyset$。

其中一个球 $\mathbf{B}_m^{\mathrm{L}}(n, t, u)$ $u \in \bigcup_{x\in X} A_x$ 与所有其他此类球的并集的交集大小至多为

$$\begin{aligned}\frac{\log(n)}{\varepsilon} W(t,1) + n^5 W(t,21) &\leq \begin{cases} \left(\frac{\log(n)mt}{\varepsilon 2n} + \frac{n^5 t^{11}}{2n^{11}}\right) \mathbf{v}_m^{\mathrm{L}}(n,t) & \text{if } m \text{ is even,} \\ \left(\frac{\log(n)mC_m}{\varepsilon n} + \frac{n^5 C_m^{11}}{n^{11}}\right) \mathbf{v}_m^{\mathrm{L}}(n,t) & \text{if } m \text{ is odd and } t = \lceil \frac{m}{2} \rceil, \\ \left(\frac{\log(n)mt}{\varepsilon n} + \frac{n^5 t^{11}}{n^{11}}\right) \mathbf{v}_m^{\mathrm{L}}(n,t) & \text{else,} \end{cases} \\ &= o(\mathbf{v}_m^{\mathrm{L}}(n,t)),\end{aligned}$$

当 $n \to +\infty$ 和 C_m 足够大时。事实上，对于与 u处于同一个 A_x 中的每个 $\lceil \log(n)/\varepsilon \rceil - 1$ 个点 $\tilde{u}$，重叠为 $\leq W(t,1)$，而每个满足 $\tilde{u}$ 位于某个非 A_x 的A_y 中的球 $\mathrm{B}_m^{\mathrm{L}}(n,t,\tilde{u})$，与 $\mathrm{B}_m^{\mathrm{L}}(n,t,u)$ 的交集至多包含 $\leq W(t,21)$ 个元素。由于$W(t,r) = 0$，若 $r > 2t$，则与给定球相交的其他球至多有 $\Delta(G[S])$ 个 $\leq n^5$。因此，球 $\mathrm{B}_m^{\mathrm{L}}(n,t,u)$ $u \in \bigcup_{x\in X} A_x$ 的并集大小为 $|X|\lceil \log(n)/\varepsilon \rceil \cdot (1 - o(1))\mathrm{v}_m^{\mathrm{L}}(n,t)$。由于该数量至多为 m^n，因此得到

$$|X| \leq \frac{m^n}{\lceil \log(n)/\varepsilon \rceil \cdot (1 - o(1))\mathbf{v}_m^{\mathrm{L}}(n,t)} \lesssim \frac{\varepsilon H_m(n,t)}{\log(n)}.$$

注意，$\bigcup_{x\in X} \mathbf{B}_m^{\mathrm{L}}(n, t, x) = \mathbb{Z}_m^n$，且 $\mathbf{B}_m^{\mathrm{L}}(n, t, x)$ 中任意一对元素的 Lee 距离都不超过 $2t$。由于 $G[S_2]$ 中的独立集由 Lee 距离大于 $2t$的元素组成，因此，每个 $x \in X$至多从 $\mathbf{B}_m^{\mathrm{L}}(n, t, x)\cap S_2$中选取一个元素，即可得到一个独立集。由于 $|\mathbf{B}_m^{\mathrm{L}}(n, t, x) \cap S_2| \leq n^5$，由此可得

$$i(G[S_2]) \leq n^{5|X|} \leq 2^{O(\varepsilon H_m(n,t))}.$$

□

引理 *3.7* 的证明。对于 $x \in \mathbb{Z}_m^n$，令 $K_x := \{y \in \mathscr{C} \colon d^{\mathrm{L}}(x, y) \leq t\}$，并对 $r \in \mathbb{N}$ 令 $S_r := \{x \in \mathbb{Z}_m^n \colon |K_x| = r\}$。于是 $m^n + \gamma \mathbf{v}_m^{\mathrm{L}}(n, t) \leq |\mathscr{C}|\mathbf{v}_m^{\mathrm{L}}(n, t) = \sum_{r\geq 1} r|S_r|$. 因此，$\mathscr{C}$中距离至多为 $2t$ 的数对数量至少为

$$\frac{\gamma \mathbf{v}_m^{\mathrm{L}}(n,t)}{m\mathbf{v}_m^{\mathrm{L}}(n-1,t-1)} \leq \frac{\gamma \mathbf{v}_m^{\mathrm{L}}(n,t)}{W(t,1)} \leq \frac{1}{W(t,1)} \sum_{r\geq 1} |S_r|(r-1) \leq \frac{1}{W(t,1)} \sum_{r\geq 1} |S_r| \binom{r}{2}.$$

现在，这一结论可由引理 2.12 推得。 □

引理 *3.9* 的证明。利用结构归纳法，我们观察到 $I \subseteq P \cup f(P)$。算法终止时，我们知道 $\Delta(G_i) < \Delta$，因此 $|E(G_i)| < (|V(G_i)|\Delta/2)$。由此，引理 3.7 得出 $|f(P)| = |V(G_i)| \leq (1+\varepsilon)H_m(n,t)$。为了证明 $|P| \leq \varepsilon H_m(n,t)\log(n)/n$，我们根据 $V(G_i)$ 的大小，将算法分为两个阶段进行讨论。

- 令 P_1 表示当 $|V(G_{i-1})| \geq 2H_m(n,t)$ 时添加到 P 中的节点集合 $u \in P$。
- 令 P_2 表示当 $|V(G_{i-1})| < 2H_m(n,t)$ 时添加到 P 中的节点集合 $u \in P$。

随着我们向 P_1 添加节点，根据引理 3.2，我们至少从 G_{i-1} 中移除比例为 $\beta \gtrsim n/H_m(n,t)$ 的节点，以得到 G_i。因此 $(1-\beta)^k m^n \leq 2H_m(n,t)$。根据引理 2.11，我们有 $n/H_m(n,t) \to 0$，因为 $n \to +\infty$，使得 $\beta \leq \log\left(\frac{1}{1-\beta}\right)$ 对于足够大的 n 成立，因此

$$|P_1| \leq \frac{\log\left(\frac{m^n}{2H_m(n,t)}\right)}{\log\left(\frac{1}{1-\beta}\right)} \leq \frac{\log(\mathbf{v}_m^{\mathrm{L}}(n,t))}{\beta} \overset{(*)}{\lesssim} \frac{\log(n)H_m(n,t)}{n},$$

其中 (*) 推论自引理 2.1 和 2.10。在第 k 步之后，我们在每一步至少移除 εn 个顶点， $0 < \varepsilon$ 取足够小。因此我们有

$$|P_2| \leq \frac{2H_m(n,t)}{\varepsilon n}.$$

由此得到

$$|P| = |P_1| + |P_2| \lesssim \frac{H_m(n,t)\log(n)}{n}.$$

此外

$$|P \cup f(P)| \lesssim \frac{H_m(n,t)\log(n)}{n} + (1+\varepsilon)H_m(n,t),$$

因此

$$i(G[P \cup f(P)]) \leq 2^{|P|} \cdot i(f(P)) \leq 2^{(1+2\varepsilon)H_m(n,t)}.$$

□