arXiv:2304.02509v1 [cs.IT] 5 Apr 2023

证明 Reed-Muller 码在对称信道上达到了香农容量

Emmanuel Abbe and Colin Sandon
EPFL

摘要

Reed-Muller 码于 1954 年提出，其构造简单明确，基于多项式求值，并且长期以来一直被猜想能够在对称信道上达到香农容量。在过去几十年中，利用组合权重枚举器界、由尖锐阈值带来的擦除信道上的突破、超收缩性论证以及极化理论，人们在证明这一猜想方面取得了重大进展。最近的另一项重大进展确立了：在低于容量时，比特错误概率会缓慢趋于零。然而，当信道允许发生错误时，Bourgain-Kalai的结果并不适用于将趋于零的比特错误概率转化为趋于零的块错误概率，已知的重量枚举界也同样不适用。因此，关于 Reed-Muller码能够在对称信道上达到香农容量，并以高概率恢复码字的猜想，至今仍未解决。

本文完成了该猜想的证明。它使用了一种新的递归提升框架，该框架聚合了“子空间向日葵”上码字限制的译码，通过 L_p 布尔傅里叶分析处理其依赖性，并使用来自Sberlo-Shpilka的重量枚举器界的列表译码论证。该证明不要求基本情形的比特错误概率趋于零，而只需一个非平凡概率，此处针对一般对称码获得。这特别为Reeves-Pfister的趋于零的比特错误概率结果给出了缩短且收紧的论证，并且结合先前工作，它蕴含了RM码在纯态经典量子信道上的强窃听保密性。

目录

1 引言 3 1.1 猜想.3 1.2 进展及相关参考文献.4 1.3 从比特到块以及证明的关键部分.6 2 主要结果 8 3 证明技术 8 4 结论和未解决问题 12 5 设置：提升框架和向日葵 13 6 局部错误概率界 15 6.1 $P_e(m, r, \epsilon)$上的基本情形：弱解码.15 6.2 $P_e(m, m, r, \epsilon|z')$的傅里叶分析.16 6.3 通过单次向日葵增强和 L_2-范数趋于零的比特错误概率.17 6.4 通过 L_4-范数在低维子集上的非集中.18 6.5 大 $P_e(m, m, r, \epsilon|z')$的概率界.19 6.6 通过递归向日葵增强对 $P_e(m, r, \epsilon)$的界：达到临界区域 . 21 7 恢复码字 22 7.1 列表译码和重量枚举式.23 7.2 通过网格增强降低块错误概率.25 8 强逆定理 26 9 推广到BMS信道 28

1 引言

香农于1948年引入了信道容量的概念 [香农48], 作为消息能够通过有噪信道可靠传输的最大码率。特别地，对于经典的二元对称信道，该信道以概率 ϵ独立地翻转码字的每个坐标，香农的容量为 $1 - H(\epsilon)$，其中 H 是二元熵函数。为了证明容量是可达到的，香农使用了概率论论证，即随机均匀抽取一个码。在“最坏情况”或“汉明”设置下 [汉明50], 随机码也可以用来证明码率最高达到 $1 - H(2\epsilon)$ 是可达到的[1], 因为码字必须构成 ϵn半径球的一个打包（即距离为 $2\epsilon n$）。因此，由于允许罕见的错误事件，香农可以达到更高的码率。

此后，获得能够达到这些极限的显式码构造，在电气工程、计算机科学和数学领域引发了数十年的研究活动。

一种简单且显式的码 里德-穆勒码由 Muller 于 1954 [Mul54], 提出，是最早、最简单的码之一。Reed 随后不久便提出了一种译码算法，可在达到其最小距离一半的范围内成功译码 [Ree54]。码的构造可以用贪心过程来描述。考虑构造一个子空间 $\mathbb{F}_2^n$（一个线性码），其码长为 2 的幂，$n = 2^m$。自然可以从全0码字开始。如果需要选取第二个码字，那么在大多数相关准则下，全1码字都是最佳选择。如果现在要保留这两个码字，那么为了最大化码距，下一个最佳选择是一个由一半的0和一半的1组成的码字。若要继续依次构造基，可以再添加几个重量为 $n/2$ 的向量，以保持相对距离为一半，从而完成一阶里德-穆勒 $RM(m, 1)$ 码（也称为哈达玛码或增广单纯形码）。此时，如何选择下一个码字可能不那么显而易见，但可以直接在先前选取的码字的支撑集上重复前述构造，并在每次达到饱和后再次重复若干次，每次都将距离减半。由此得到 $RM(m, r)$ 码，其基也可等价地定义为次数至多为 r 的单项式在 m 个布尔变量上的求值向量：

$$RM(m, r) = \{(f(x_1), \ldots, f(x_{2^m})) : x_1, \ldots, x_{2^m} \in \mathbb{F}_2^m, f \in \mathbb{F}_2(X_1, \ldots, X_m), \deg(f) \le r\}. \quad (1)$$

如前所述，一阶 RM 码 $RM(m, 1)$ 是增广单纯形码或哈达玛码。单纯形码是“完美的”汉明码的对偶码，即它为该空间提供了完美的球填充（达到了球填充界）。对于一般的 RM 码而言，这一强性质显然不复存在，但RM码仍然保持了不错的距离（对于恒定码率，在根号级别的块长度下）。在最坏情况模型中，距离控制着错误译码能力，RM码并不能构成“良好”的码族（即具有渐近恒定码率和恒定相对距离的码族）。其他码可以实现更好的距离/码率权衡，例如扩展图码 [SS96]。然而，一旦置于香农概率错误模型下——在该模型中，最小距离不再是正确的评价指标——RM 码的表现出人意料地好，甚至可能与随机码一样好。

1.1 猜想

长期以来，人们一直猜想RM码在二元对称信道（BSC）上能够达到香农容量，更一般地说，在二元输入无记忆对称（BMS）信道（本文也简称为“对称信道”）上能够达到香农容量。我们参见第 9 节了解BMS信道的正式定义；目前，只需考虑作为主要关注对象的BSC，因为BMS信道是BSC的混合。

[1]应在 $\epsilon > 1/$的情况下使用 $1 - H(2\epsilon) \wedge 1$ 2.

猜想*1*。对于任意*BMS*信道 $\mathcal{P}$，以及低于由 $C(\mathcal{P}) = I(U, \mathcal{P}) = (1/2) \sum_{x \in \{0,1\}, y \in \mathcal{Y}} \mathcal{P}(y|x) \log_2 \mathcal{P}(y|x)/(\mathcal{P}(y|0)/2 + \mathcal{P}(y|1)/2)$给出的 $\mathcal{P}$ 容量的任意码率 R，其中[2] $\mathcal{Y}$是 $\mathcal{P}$的输出字母表（当 $\mathcal{P} = BSC(\epsilon)$ 时，$C(\mathcal{P}) = 1 - H(\epsilon)$），一系列码率为$R_i = \binom{m_i}{\leq r_i} 2^{-m_i}$趋近于 R 的*Reed–Muller*码(m_i, r_i)可以以高概率被成功译码，即任意一个 $\lfloor 2^{nR_i} \rfloor$ 码字都可以以概率 $1 - o_{m_i}(1)$ 被译码，尽管受到来自 $\mathcal{P}$ 的干扰。

[{"id": 0, "output": "很难追溯这一观点最早何时出现在文献中，但 [KKM+16a]报告称，它很可能早在20世纪60年代末就已存在。Shu Lin于1993年发表的一次演讲中明确提到了这一主张，演讲题为？RM码并没有那么糟？ [Lin93]。Dumer和Farrell于1993年发表的一篇论文也讨论了这一问题 [DF93]，，Costello和Forney于1997年发表的关于“通往信道容量之路”的论文同样如此 [CF07]。此后，这一主题受到了广泛关注；随着极化码的出现，相关研究活动也开始活跃起来 [Arı09]。Arıkan于2010年在都柏林举行的ITW会议上，将其称为编码理论中的主要未解决问题之一。由于RM码在计算机科学、电气工程和数学领域具有广泛的相关性[3]，相关研究分散在大量工作中 [Dum04, DS06, Dum06, CG05, HKL05, Ari08, Arı09, Ari10, KLP12, ASW15b, ASW15a, KKM+16a, KKM+17, MHU14, SSV17, AY19, YA20, SS20, KKM+16b, Sam18, Sam20, AHN21, HSS21, LHP20, FFHM21, ASY21, RP21, GEE+21, BHSS22, ASSY23]；另请参见 [ASSY23]。"}]

与极化码的关系在一篇突破性论文中，Arıkan 证明了显式构造的极化码能够在任意 BMS信道上达到香农容量 [Arı09，AT09]。鉴于极化码与 RM码之间的密切关系，人们更加确信RM码也可以被证明在BMS信道上达到容量。极化码由同一个方阵导出，即其各行对应于单项式的取值，该矩阵也可以表示为 $G_n := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{\otimes m}$，但极化码采用了不同的行选择方式，该方式取决于信道。可以如下看待其中的差异：对一个由独立同分布的伯努利（ G_n （在 $\mathbb{F}_2$上）ϵ）分量组成的向量应用 G_n，以压缩二元对称信道的噪声向量；极化码保留变换后向量中具有最大“条件熵”的行，并按照从上到下的顺序进行。使用“条件”熵是极化码的一项显著约束；它在译码复杂度方面带来了显著益处，也便于界定错误概率（这是一种“平均情况”度量），但对于性能而言，这未必（事实上也不是）最佳的处理方式。相反，RM码采用了一条更“宏观”且“通用”的规则：保留汉明重量最大的行。这对于最坏情况模型而言是一个自然选择（事实上可以证明，RM码是[4],的最佳子码，就距离而言），但在香农设定下，这未必自然。合理的预期仍是，最稠密的行能够有效地提取噪声的随机性[4]，但由于这对一个“平均情况”问题使用了“最坏情况度量”，因此要确立这一点困难得多。

1.2 进展及相关参考文献

我们现在按大致时间顺序概述该猜想的主要进展。

[2]这是信道在均匀输入分布下的互信息，由于BMS信道的对称性，该分布是最优输入分布。

[3]二进制或q元域上的RM码已被用于例如密码学 [Sha79, BF90, Gas04, Yek12],伪随机生成器和随机性提取器 [TZS06, BV10]，困难性放大、程序测试和交互式/概率证明系统 [BFL90, Sha92, ALM+98]、电路下界 [Raz87]，近似硬度 [BGH+12、BKS+10a]，低次测试 [AKK+05、KR06, JPRZ09, BKS+10b, HSS13]，私人信息检索 [CKGS98, DG16, CKGS98, BIK05, BIKR02]，和压缩感知 [CJ10, CHJ10, BMW15]。

[4]这一洞见促成了我们与 A. Wigderson 和 A. Shpilka 的合作 [ASW15b]。

1. [SP92] 是最早在香农场景下为 Reed–Muller码 的性能建立保证的工作之一，但针对固定的 r，且相较于容量缩放存在偏移。首次实现容量的缩放见于 [HKL05]，适用于 $r = 1$ 的特殊情形，2. 在此期间，Dummer 的一系列工作也在 Reed–Muller码 递归译码方面取得了重大进展 [Dum04、DS06、Dum06],，但尚未取得容量的结果。随后，极化码的突破在 [Arı09],中实现，使这一猜想重新受到关注，正如前文所述。

2.首个关于非恒定 r 的达到容量结果出现在 [ASW15b, ASW15a],，该工作为二元擦除信道和二元对称信道发展了重量枚举器界方法，并借鉴了关键论文 [KLP12]中的技术。在 [KLP12], 之前，20世纪70年代的一系列工作为RM码推导了重量枚举界：从Sloane和Berlekamp关于 $r = 2$ [SB70] 的原始工作，到两倍（以及2.5倍）最小距离 [KT70, KTA76]。然而，自1976年以来一直没有出现显著进展，直到 [KLP12] 突破了2.5倍的障碍，为小 r的更广泛范围内的距离提供了界，尤其是引入了epsilon-net方法。 [ASW15b] 的一项贡献是将这一方法扩展并细化到更大的 r范围，该范围可能与 m呈线性关系。

3. 随后，二元擦除信道（BEC）取得了突破，发表了广受赞誉的论文 [KKM+16a， KKM+17]。二元擦除信道是最简单的非平凡信道；它不允许发生错误，只会发生擦除。二元擦除信道尤其受益于一个很强的性质：在给定另一个受噪比特的情况下，错误译码一个比特这一事件，在擦除模式集合上是一个单调性质（退出函数）。这使得 [KKM+16a]能够将其与关于单调性质尖锐阈值的一般性结果联系起来 [FK96， BK97] 并得出一个优美的证明：任何具有足够对称性（即二重传递性）的码，在二元擦除信道上都能达到容量。此外，由于 [BK97],关于这种强对称性的结果，阈值实际上必然足够尖锐，这意味着，证明退出函数趋于零的“局部”分析足以得到趋于零的块错误概率。

4. 在 [SS20], 对 [ASW15b] 取得了重要改进，采用了类似的证明技术，但使用了更紧致且更通用的估计，从而为更大的 r生成了有用的重量枚举界，尤其是在 r 诱导恒定码率这一对猜想颇为重要的情形下。正如我们将看到的，这一改进将成为我们证明中某一步的关键。

5. 尽管极化码重新激发了人们对 RM 码猜想的研究热情，但由于二者的相似性，此前的进展所依据的技术与极化码并无明显联系。在 [AY19], 中，研究者建立了与极化理论的联系，表明按照 RM 码的顺序（按权重递减）逐比特译码时，条件熵也会极化。这进而意味着，通过保留“高熵”分量而得到的码（称为“双胞胎 RM 码”），必定能在任意 BMS信道上达到容量。要证明这一猜想，仍需证明这个“双胞胎 RM 码”等价于 RM 码。目前似乎已有充分证据支持这一点——这两种码在二元擦除信道上等价，数值模拟和部分理论结果也 [AHN21]支持这一结论——但这一研究计划仍有待完成，其中还蕴含着与加法组合学的有趣联系 [TV06，Lov17，San12]。

6. 一种新的分析方法在 [Sam18中，Sam20] 得以发展，用于在新的参数范围内获得 RM码的重量枚举式界。特别是， [Sam20]借助超收缩性论证，利用关于擦除信道的结果，得到了重量枚举式的新界。此外，如何利用擦除对偶性也在[HSS21] 中得到了进一步发展，并取得了一项重要里程碑：证明了 RM码能够以恒定码率在二元对称信道上进行译码。虽然这并未给出容量结果，但它解决了 [ASW15b] 中提出的一个开放问题，因为其中的技术似乎无法处理这一参数范围。

7. 在 [YA20], 中，提出了一种递归投影聚合算法，通过递归地将码字投影到子空间上，并使用多数投票聚合投影译码结果来译码码字。虽然该算法尚未获得容量结果，并且也仅限于较低的 r，但递归组合码字子组件译码这一高层次思想，与本文提出的通用增强过程具有某种共同之处。不过，我们在这里依靠的不是投影，而是限制（不会导致噪声增加），以及经过精心选择的"向日葵子空间"，以有效聚合这些限制，并实现受控的依赖性分析。

8. 最后，近期的另一项重大成果表明，对于任意BMS信道上的RM码，当码率低于容量时，退出函数或比特错误概率会趋于零。 [RP21] 的方法以面积定理和退出函数为基础，如 [KKM+16a], 所示，并基于退出函数的MMSE版本和RM码的嵌套性质，为BMS 信道推导出更具针对性的界。尽管 [RP21]的结果几乎确立了这一猜想，但由于得到的退出函数衰减速度非常慢，正如下一节所述，该猜想的主要部分似乎仍未解决。

我们参见 [ASY21、 ASSY23]以获取更多参考文献。

1.3 从比特到块以及证明的关键部分

如上所述，近期一篇论文 [RP21] 证明，对于任何低于容量的固定码率，RM 码在所有 BMS 信道上的"比特错误概率"都会趋于零，其比特错误按 $O(\log\log(n)/\sqrt{\log(n)})$ 的速率缩小。尽管这是一项重要成果，但如此缓慢的缩减速度并不意味着 RM 码能以经典意义上的方式达到容量，即恢复码字；无论是并集界，还是下文将讨论的现有重量枚举界，都无法得出这一结论。事实上，借助我们的提升框架，如此缓慢的衰减虽然足以跨过第一步，但在后续进展方面，与一种固定但非平凡的衰减相比并无太大优势；而后者正是我们在此能够更直接、更一般地证明的基本情形。之后的大部分工作都着眼于实现足够快的衰减，以便通过列表译码恢复码字，而这需要快得多的衰减速度。

让我们首先澄清人们可以为信道编码问题研究的不同类型的译码要求（假设为二元对称信道）。香农容量通常被定义为 [CK11, CT12, Gal08]作为所有码率 R 的上确界，使得存在一个编码映射 $E^n: [\lfloor 2^{nR} \rfloor] \to \mathrm{F}_2^n$ 和一个译码映射 $D^n: \mathrm{F}_2^n \to [\lfloor 2^{nR} \rfloor]$ 使得对于任何消息 $m \in \lfloor 2^{nR} \rfloor$，$\mathrm{P}(m \neq D^n(E^n(m) \oplus Z^n)) = o_n(1)$。从码字的角度来看，即，用 X^n 表示映射 E^n 和 X^n 表示返回与译码消息对应的码字的映射，即， $X^n(\cdot) = E^n(D^n(\cdot))$，先前的消息错误概率等于$\mathrm{P}(X^n(m) \neq X^n(X^n(m) \oplus Z^n))$。因此错误概率适用于消息，或者等价地，适用于整个码字，通常称为'块'错误概率或简称为错误概率。由于人们也可以考虑 m 被均匀随机抽取，将这种随机性添加到概率[5], 中，人们可以将块错误的符号简化为$\mathrm{P}(m \neq \hat{m})$或$\mathrm{P}(X^n \neq X^n)$（其中 X^n 在码字中均匀随机抽取）。

还可以定义"比特"错误概率，即码字中某个坐标被错误解码的概率，也就是 $\mathrm{P}(X_i \neq X_i(X^n \oplus Z^n))$（对于 Reed–Muller码，该概率与 i 无关）。下文将讨论，也可以考虑退出函数变体：移除待解码比特的含噪观测，并根据其他比特进行解码，即 $\mathrm{P}(X_i \neq X_1(X^n_{-i} \oplus Z^n_{-i}))$，其中 X^n_{-i} 是从 X^n中移除分量 i 后得到的 $(n-1)$ 维向量。

[5]RM码具有足够的对称性，使得任何码字在错误事件中的表现都相似。

有时会使用比特错误概率，因为它有助于证明更强的[6] 逆命题，即表明在容量以上甚至无法达到趋于零的比特错误概率（如本文以及 [RP21] 中所示）；而块错误概率则有助于证明信道容量定理中的可达性部分，且常用于恢复实际消息。

如果比特错误概率以 $o(1/n)$的速率趋于零，那么通过简单的并集界可以推出块错误概率也趋于零。然而，要为 RM 码确立这种缩放关系颇具挑战，而 [RP21] 得到的缩放关系要慢得多，即 $O(\log\log(n)/\sqrt{\log(n)})$。比 $o(1/n)$更弱的缩放关系，仍可能足以支持一种稍微复杂些的上界；这种上界会使用重量枚举界，例如 [SS20], 中的方法，并结合列表译码论证，譬如[KKM+16b]中所讨论的那样。然而，这种更复杂技术所需的缩放关系同样远达不到$O(\log\log(n)/\sqrt{\log(n)})$；特别是， [KKM+16b] 要求 $\overline{n^{-\Omega(1)}}$。

对于二元擦除信道，从比特错误概率转到块错误概率可以采取更直接的路径，因为二元擦除信道可以在单调布尔公式的研究框架下进行分析，并且在足够的对称性（这里由 Reed–Muller码保证）下，Bourgain 和 Kalai 的一般性结果 [BK97] 推导出了关于临界窗口标度的界，这直接意味着比特错误概率必须趋于零，当 $o(1/n)$（从而通过并集界得到趋于零的块错误概率）。详情请参见 [KKM+16a] 。遗憾的是，对于二元对称信道或其他BMS信道，在研究比特（或块）错误概率时，无法将错误事件表示为布尔单调性质，因此也就无法直接引入关于单调性质的尖锐阈值结果。事实上，除了形式上并非“布尔”的问题之外，错误事件还是非“单调”的（这也涉及对非布尔性质的潜在扩展）。因此，若要证明二元对称信道上的退出函数至少在 [RP21]中趋于零，就已经需要额外的工具。.

因此，要证明比特错误概率快速衰减并非易事。我们的证明通过一系列环环相扣的步骤实现了这一目标。事实上，我们并未直接证明$o(1/n)$ 衰减，而是通过提升框架的 5 个中间层次获得这一结果（参见图1）：

1. 我们首先依赖于信道编码的弱解码准则；这并不是趋于零的退出概率，而是一个常数且非平凡的概率。也就是说，利用一般性的熵论证，我们首先证明，对于任何运行在容量以下且具有对称性的码，根据其他噪声比特估计一个比特的概率为 $1/2 - \Omega(1)$；

2. 接下来，我们通过一步“向日葵璔强”将其提升至 $O(2^{-\sqrt[3]{m}})$，并使用 L_1、L_2 布尔傅里叶估计。这改进了 $O(\log(m)/\sqrt{m})$ 的 [RP21] 尺度（并给出了更短的证明），但仍远未达到并集界所需的 $o(1/2^m)$，也未达到使用 [SS20]进行列表译码所需的尺度；

3. 我们进一步通过“递归向日葵增强”将其提升至 $2^{-\Omega(\sqrt{m}\log(m))}$；大部分技术工作都集中在这一步，尤其是 L_4 布尔傅里叶估计；

4. 然后，我们将上一个估计与列表译码论证相结合，利用 [SS20] 中的重量枚举器界 [KKM+16b], ，从而得到一个趋于零的块错误概率；这需要采用与 [SS20] 中类似的论证 [ASW15b], ，不过其中的定理是针对更强的缩放而表述的。此外，我们不仅需要 [SS20] 相对于

5. 我们进一步通过“网格增强”将这一块错误概率提升至 $\overline{2^{-2^{\Omega(\sqrt{m})}}}$，这自然意味着比特错误概率为 $2^{-2^{\Omega(\sqrt{m})}}$ （特别地为 $o(1/n)$）。

[6]“强”逆命题也指错误概率在容量以上趋于1。

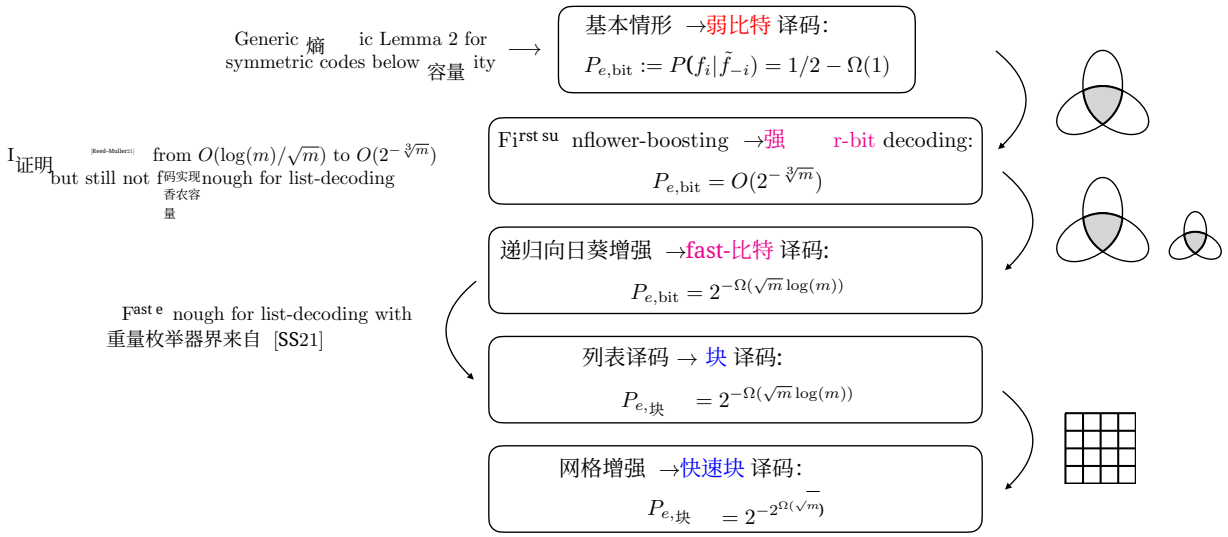

图 1：该变　　局部到整体误差界在我们的提升框架中的诸多改进　　.

2 主要结果

定理 *1.* 设 $\mathcal{P}$ 为一个 *BMS*信道，且 $C(\mathcal{P})$ 为其容量，即 $C(\mathcal{P}) = I(U,\mathcal{P}) = (1/2)\sum_{x\in\{0,1\},y\in\mathcal{Y}} \mathcal{P}(y|x) \log_2(\mathcal{P}(y|x)/(\mathcal{P}(y|0)/2 + \mathcal{P}(y|1)/2))$，其中 $\mathcal{Y}$ 是 $\mathcal{P}(C(\mathcal{P}) = 1 - H(\epsilon)$ 的输出字母表，当 $\mathcal{P}$ = 二元对称信道(ϵ)时。设 $\{m_i\}_{i\geq 1}$ 和 $\{r_i\}_{i\geq 1}$ 为正整数序列，满足对所有 i 均有 $r_i \leq m_i$，且 $\lim_{i\to\infty} m_i = \infty$。

- 如果 上极限$_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i} = R < C(\mathcal{P})$，则 $RM(m_i, r_i)$ 的块错误概率以 $2^{-2^{\Omega(\sqrt{m_i})}}$趋于零，即，可以以高概率从其受到的破坏中恢复任意 *RM* 码字。
- 如果 下极限$_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i} = R > C(\mathcal{P})$，那么 $RM(m_i, r_i)$ 的比特错误概率会增大至$1/2 - 2^{-\Omega(\sqrt{m})}$，也就是说，无法以渐近非平凡的概率解码 *RM* 码字的任何单个分量[7]，即使已知其受损版本。

该定理的一些推论：(i) 这表明，尽管 RM码具有简单明确的编码构造，其编码复杂度为 $O(n \log_2 n)$，并且对于所有容量相同的 BMS 信道都是通用的，但在采用最大似然解码实现容量方面，它能够达到 Shannon 随机码的性能。(ii) 正如 [RP21], 中所讨论的，我们的结果在量子情形下也具有影响。这表明，量子 Reed-Muller 码达到了 [Wil13], 中的哈希界；由于我们的结果适用于趋于零的块错误概率，结合 [Ren18] 的对偶性结果可知，对于二元对称信道和纯态窃听信道，RM码在经典-量子信道上都实现了强保密性。

定理 1 第 (i) 和(ii) 部分分别在第 7 节和第 8 节中针对二元对称信道进行了证明，而第 9 节则给出了将证明扩展到 BMS 信道所需的调整。

3 证明技术

我们将　证明RM码局部和全局错误事件的越来越强的界　　.

[7]这对于最优的最大似然解码器或最大后验概率解码器成立。

递归提升译码算法。 大部分工作都依赖于提供一种方法，将任何以非平凡但除此之外较弱的成功概率在 $RM(m,r)$ 中译出码字坐标的算法，转换为一种以更高且可控的成功概率在 $RM(m,r)$ 中译出码字分量的算法，其中 m 略大于 m。

基本情形。 我们的基本情形是一个较弱的界，用于约束在观测其他噪声比特时对一个比特进行译码的错误概率（即退出函数）。然而，这个界只需达到 $1/2 - \Omega(1)$，比[RP21]中证明的退出函数趋于零的界弱得多。事实上，对于任何低于容量且具有足够对称性的码，我们都可以通过依赖熵不等式的论证（引理2）普遍地得到这样一个较弱的界。

构造子空间向日葵。[8] 从这个基本情形出发，我们开始将较弱的错误界提升为更好的界。为了发展提升技术，我们考虑一个子空间 V 的$\mathbb{F}_2^m$，其中包含待译码的比特，并且 V 任意选取，但与 Z 相互独立，且维数为 m，例如取 $V = \mathbb{F}_2^m \times 0^{m-m}$。然后，我们使用大量 m维的 $\mathbb{F}_2^m$ 的子空间，W_1、W_b，它们都交于 V，且仅交于 V。我们使用贪心算法构造这些“花瓣”子空间 W_1、W_b（参见引理 1）。接下来，我们分别尝试从噪声码字在这些花瓣上的限制中译码相关比特，同时忽略目标比特的噪声值，以减轻这些解码之间的依赖关系。最后，我们对这些花瓣进行多数投票，以译码原始比特。在花瓣上进行处理的优势在于，我们有多个花瓣，并且它们的重叠由交集[9] V控制，这使我们能够管理依赖关系，并在多数投票分析中获得集中性。

分析花瓣上的条件概率。于是，研究的主要对象变成了：在将噪声限制在某个花瓣 W_i 并取固定值的条件下，错误译码一个比特的概率。为了更形式化地讨论这一点，考虑以概率 ϵ独立翻转比特的二元对称信道，并定义 $P_e(m,r,\epsilon)$ 为：在观测其他噪声比特时，对 $RM(m,r)$中某个码字的一个比特进行译码时的错误概率。我们用 $Z \in \mathbf{F}_2^{2^m}$ 表示指示哪些比特发生翻转的噪声向量。对于任意 $i \neq j$， W_i 与 W_j 的交集是 V，因此，在给定将 Z 限制到 V的条件下，将 Z 限制到 W_i 所得的结果彼此独立[10] 。这进一步意味着，在给定将 Z 限制到 V的条件下，它们能否正确译码目标比特彼此独立。因此，如果将 Z限制到 V 是“良好的”，即在给定该限制的条件下，以使目标比特错误的方式对码在各个 W_i 上的限制进行译码的概率至多为 $1/2 - \Omega(1)$，并且 b 足够大，那么我们几乎必然能够正确确定目标比特的值。

因此，我们需要证明，将 Z 限制到 V 是足够有可能良好的。令$Q_{m,m}(z')$为[11] 在观察其他噪声比特的条件下， 0^m 比特被错误解码的概率，其中条件是将 Z 限制到一个 m 维子空间（$V = \mathbf{F}_2^m \times 0^{m-m}$）为 z'。现在我们希望证明$\mathbf{P}_{z'}[Q_{m,m}(z') > 1/2 - c]$ 的上界，其中 c为某个适当的常数。更具体地说，在增强过程的早期，我们将得到 $\mathbf{E}_{z'}[Q_{m,m}(z')] = P_e(m,r,\epsilon)$的一个上界，该上界略小于 $1/2$；为了证明 $P_e(m,r,\epsilon) = o(1)$（第一种情况），我们需要证明 $\mathbf{P}_{z'}[Q_{m,m}(z') > (\mathbf{E}_{z'}[Q_{m,m}(z')] + 1/2)/2] = o(1)$。在该过程的后期，我们将得到 $P_e(m,r,\epsilon)$ 的相当紧的界，并且需要证明 $\mathbf{P}_{z'}[Q_{m,m}(z') > 1/3]$ 非常小，以便

[8]我们使用来自 [DF81] 的“向日葵”术语，BDBD22], 但不需要“向日葵引理” [DF81]。[9]我们使用一个重叠集合 V 大于 0^m ，因为任意两个维数大于 $m/2$ 的子空间都会在 0^m 以外的某处相交，而维数为 $m/2$ 的空间太小，无法有效译码。[10]实际码在 W_i 上的限制在码对 V 的限制条件下并非独立，但这无关紧要，因为错误译码目标比特的概率仅取决于 Z。[11]我们省略参数 r， ϵ 因为从现在起它们变为隐式。

证明关于 $P_e(m, r, \epsilon)$ 的足够严格的界（第二种情况）。

对 Q进行布尔傅里叶分析。由于 $\mathbf{P}_{z'}[Q_{m,m}(z') > 1/3] \leq 9\mathbf{E}_{z'}[Q^2_{m,m}(z')]$ 以及 $\mathbf{P}_{z'}[Q_{m,m}(z') > (\mathbf{E}_{z'}[Q_{m,m}(z')] + 1/2)/2] \leq \frac{16}{(1-2\mathbf{E}_{z'}[Q_{m,m}(z')])^2} Var_{z'}[Q_{m,m}(z')]$，我们依靠$Q$ 的傅里叶变换来估计其 L_1 和 L_2 范数。对于任意给定的 z'，Q_m、$_m(z')$的值是对所有 $z'' \in \mathbf{F}_2^m$的Q_m、$_m(z'')$取的期望，这些对象对 $\mathbf{F}_2^m$ 具有 z'的限制。这意味着，$_m$ (Q_m的傅里叶变换中)所有支撑在 $\mathbf{F}_2^m$ 中的项，也都属于$_m(Q_m$的傅里叶变换)，而那些支撑不在 $\mathbf{F}_2^m$ 中的项，则会在取平均时相互抵消。此外，$\mathbf{E}_{z'}[Q^2_{m,m}(z')] \leq \mathbf{E}_{z'}[Q_{m,m}(z')] = P_e(m, r, \epsilon)$。因此，为了证明 $P_e(m, r, \epsilon)$相对于 $P_e(m, r, \epsilon)$很小，只需证明：在较弱假设下（第一种情况），非恒定项的大部分权重位于不支撑在 $\mathbf{F}_2^m$ 中的项上；并且在较强假设下（第二种情况），大部分权重位于不支撑在 $\mathbf{F}_2^m$ 中的项上即可。

利用仿射不变性，将问题化归为子空间上的非集中。接下来，我们注意到，由于 RM 码的仿射不变性，若 $S \subseteq \mathbf{F}_2^m$，且 S' 是将线性变换应用于 S 后得到的集合，那么在 Q_m 的傅里叶变换中，由 S 和 S' 支撑的项的系数必然相同。我们还注意到，如果由 S 张成的 $\mathbf{F}_2^m$ 的子空间具有 d 维，那么在 S 的线性变换轨道中，包含于 $\mathbf{F}_2^m$ 的元素所占比例至多为 $2^{-d(m-m)}$。Q_m 的傅里叶变换中的每个非恒定项，其支撑张成的子空间维数至少为 1,[12] ；这足以说明 Q_m 足够接近常数，因此当 m 略大于 m 时，大多数 z 都是好的。这将带来趋于零的比特错误概率，其缩放为 $O(2^{-\sqrt[3]{m}})$，优于 [RP21] 给出的 $O(\log(m)/\sqrt{m})$，但还不足以继续进行列表译码。为了在下一阶段对 $P_e(m, r, \epsilon)$ 建立足够紧的界，我们需要证明，大部分权重都集中在支撑不包含于低维子空间的项上；这需要更多分析。

通过 L_4-范数的子空间上的非集中。接下来我们证明，对于任意低维集合 S，$Q_{m,\ m}$ 在由 S 的线性变换支撑的项上的傅里叶能量相对较小。对于 $z' \in \mathbf{F}_2^m$的任意给定取值，并在对 $Z = z'$进行条件化后，目标比特的取值总会出现以下三种情况之一：判断正确、判断错误，或者目标比特的两个可能取值等可能出现（平局情形）。因此 $Q_{m,\ m}(z') \in \{0, 1/2, 1\}$ 对所有 z'均成立。我们知道 $\mathbf{E}_{z'}[Q_{m,m}(z')] = o(1)$，因此这意味着$Q_{m,\ m}$ 集中在输入中的一小部分上。对于任意张成低维空间的集合 S，我们将通过界定其 L_4 范数并将其与 L_2 范数进行比较，证明由 S 的线性变换支撑的傅里叶基元素之和并不集中在输入中的一小部分上。这意味着，任意给定低维集合的轨道都不可能解释 $Q_{m,\ m}$中过多的傅里叶权重；并且在线性变换下，d-维集合至多有 2^{2^d} 个不同的轨道，因此这些项的权重总和将会很小。

重复. 先前的结果允许我们证明 $P_e(m, r, \epsilon)$ 相对于 $P_e(m, r, \epsilon)$ 较小，当 m相对接近 m时。反复应用这些界限，我们证明 $P_e(m, r, \epsilon) = 2^{-\Omega(\sqrt{m}\log(m))}$对于我们关心的 m、r 和 ϵ 的值。

技术论证. 有一些这个论证的细节对于确立提升后的错误界下降得足够快是重要的。在提升的第一阶段，我们对错误率的界以 $m - m$ 的指数速度下降。这还不够快，无法得到我们论证中确立可以恢复码字所需的界，因此我们需要使用子空间向日葵进行第二阶段的提升。类似地，如果总是让所有的 W_i 的维数比 V 的维数大一，会更简单，但那样我们仍然需要有 $m - m = \Omega(\log(m))$ 以限制 W_i 的大多数解码的风险

[12]这正是我们要求解码某个比特时不得使用该比特的含噪版本的原因。如果允许使用目标比特的含噪版本，那么变换中就会出现一个支撑为 $\{0^m\}$ 的项。

尽管 Z 到 V 的限制表现良好，仍会将目标比特判断错误，而我们对 $P_e(m,r,\epsilon)$ 的界大致为 $P_e(m,r,\epsilon)/\sqrt{m}$，这将收紧得过于缓慢。

具有紧确列表译码的比特到块译码。 接下来的部分更为标准，但需要严格控制界，以便将各部分结合起来。我们可以将先前的界应用于每个比特，从而得到一种译码方式，以高概率至多有 $2^{m-\Omega(\sqrt{m}\log(m))}$ 个比特出错。为了准确确定码字是什么，我们使用列表译码，即列出与先前译码结果的距离不超过 $2^{m-\Omega(\sqrt{m}\log(m))}$ 的所有码字，然后译码为列表中与受干扰码字距离最近的元素。接着，我们对与真实码字距离不超过 $2\cdot 2^{m-\Omega(\sqrt{m}\log(m))}$ 的所有码字应用并集界。根据[13]中定理 1.2 的证明结果 [SS20]，$RM(m,r)$ 中与任一码字在至多 2^{m-l} 个元素上不一致的元素数量至多为

$$2^{\sum_{j=l}^{r} 17m(j-1)(j+2)+17(j+2)\binom{m-(j-1)}{\leq r-(j-1)}}$$

对于我们关心的 l 取值，它等于 $2^{O(l2^{m-l}(4(r-l)(m-r)/(m-l)^2)^{m/2})}$。对于某个与真实码字至少在 2^{m-l-1} 比特上不一致的码字，被污染的码与该码字的一致程度高于与真实码字的一致程度的概率至多为 $(4\epsilon(1-\epsilon))^{2^{m-l-2}}$（Bhattacharyya 界）。这些最后的步骤与 [KKM+16b]，中的论证类似，尽管他们的定理要求比此处允许的更严格得多的逐比特错误界（即 $n^{-\Omega(1)}$）。于是，存在一个与真实码字相距不超过 $2\cdot 2^{m-O(\sqrt{m}\log(m))}$ 且更有可能的码字的概率为 $\sum_{l=\Omega(\sqrt{m}\log(m))}^{m} 2^{O(l2^{m-l}(4(r-l)(m-r)/(m-l)^2)^{m/2})}(4\epsilon(1-\epsilon))^{2^{m-l-2}} \ll 2^{-\Omega(\sqrt{m}\log(m))}$。这表明我们能够以概率 $1-2^{-\Omega(\sqrt{m}\log(m))}$ 恢复该码字。

通过高维网格增强提升块错误概率。 为了建立更紧的块错误概率界，我们首先注意到，对于足够小的c，任意满足 $|S|=c\sqrt{m}$ 的集合 $S\subseteq\{0,...,m\}$ 以及任意 $x\in\{0,1\}^S$，将码限制在变量索引属于 S 且取值为 x 所指定值的比特上，所得的仍然是一个码率低于阈值的Reed–Muller码。因此，我们可以以概率 $1-2^{-\Omega(\sqrt{m}\log(m))}$从码字的含噪版本中确定其在这些比特上的限制。此外，能否从含噪版本中恢复码字在坐标属于 S 且取值为 x所指定值的比特上的限制，与另一个 x'对应事件是否发生无关。因此，以极高的概率，x 的大多数取值将是“良好”的；这里的“良好”是指我们能够从相应限制的含噪版本中恢复码字的对应限制。

进行这一步额外网格增强的好处是，我们几乎可以保证不会弄错太多比特，而且弄错的比特通常会以更容易处理的模式排列。具体而言，我们将 $\{0,...,m\}$ 划分为若干集合 S_1、.....、$S_{m'}$，每个集合的大小约为$c\sqrt{m}$。然后，对于每个 $1\leq i\leq m'$ 和 $x\in\{0,1\}^{S_i}$，我们根据含噪版本，确定码字在相应比特上的限制最可能取值。接着进行投票，也就是说，我们猜测码字中的每个比特都取这些重构结果中赋予它最多的那个值。对于每个 $x_1\in\{0,1\}^{S_1}$、$x_2\in\{0,1\}^{S_2}$、.....、$x_{m'}\in\{0,1\}^{S_{m'}}$，码中恰好有一个比特，其坐标属于 S_i，且对所有 i都取 x_i 指定的值。因此，多数部分重构结果出错的比特数至多等于这样的元组 $(x_1$、.....、$x_{m'})$ 的数量：其中至少一半的 x_i 是坏的。这样一来，除非出现坏 x异常多的极低概率情况，我们就能正确恢复大多数比特。进而，我们可以应用前述列表译码技术，将块错误概率降至 $2^{-2^{\Omega(\sqrt{m})}}$。

[13]定理 1.2 的下　　界于 [SS20] 不足以证明我们的界，但第 17 页的中间界可以　　.

4 结论和未解决问题

本文证明了这一猜想：Reed–Muller码能够在所有 BMS 信道上达到容量，并以经典意义将码字恢复至信道容量所对应的水平。本文表明，尽管 Reed–Muller码的构造简单、确定且与信道无关，所需时间为 $O(n)$，它们仍能像随机码一样，在所有 BMS 信道上普遍达到容量。

该论文尤其提出了一个用于译码的新提升框架。提升技术已在监督学习中得到广泛发展 [SF12], 以及社群检测中[Abb18] 其中，弱恢复是指恢复一个坐标，且错误概率至多为$1/2 - \Omega(1)$。然而，迄今为止，提升技术尚未在编码理论中得到广泛应用，弱恢复在这一背景下也尚未得到充分研究。我们的提升以这样一种弱恢复概念作为基本情形：在给定其他噪声比特的情况下对一个比特进行译码；该概念必须是非平凡的，但可以是常数（甚至可以缓慢增长到 $1/2$）。这一弱基本情形受益于其高度通用性：我们证明，只要一个码具有对称性（即坐标的选择无关紧要），任何低于容量的码都具备这样的基本情形。此外，建立这一基本情形要比证明 $O(\log(m)/\sqrt{m}$ 的趋零标度更简单，后者见 [RP21], ；而一轮直接的向日葵增强已经能使其更快衰减至 $O(2^{-\sqrt[3]{m}})$。如第 1.3 节所述，接下来的主要挑战在于达到 $2^{-\Omega(\sqrt{m}\log(m))}$ 的标度，而递归提升算法通过 L_2、L_4 反集中分析实现了这一点。现在有两个自然的方向：

- **译码复杂度：**关于RM码的主要未决问题现在是还要获得一种高效的译码算法，理想情况下达到容量。这在过去几十年中一直也是一个活跃的研究领域，相关成果综述见 [ASSY23]。极化码目前具有能够非常高效地进行译码这一显著优势，但代价是编码更加复杂（尽管仍然高效 [TV13]）且依赖于信道。此外，如 [HAU14、 GX15] 以及一般强极化 [BGN+22]所示，极化码与容量存在多项式间隙，因此能够以总体多项式复杂度逼近容量。事实上，极化码具有实际意义，并已进入5G协议 [3gp]。然而，与随机码和RM码相比，其缩放指数并非最优[HKO+18]，并且在某些情况下，RM码已经被证明具有有利的权衡[MHU14、 YA20]。如果能够为RM码获得一种达到容量且具有准最优缩放律的高效译码算法，那么RM码将令人惊叹：在性能上基本匹配随机码，同时又具备高效性。

  请注意，提升框架也可能有助于寻求高效的译码算法。事实上，提升步骤都相当高效。它通过调用基本情形 $2^{O(\sqrt[3]{m})}$ 次，使比特错误概率趋于零，并通过调用前一种情形 $e^{-O(\sqrt{m}\log(m))}$ 次、使用 $e^{O(\sqrt{m}\log(m))}$ 次调用，进一步达到 $e^{O(\sqrt{m}\log(m))}$ 的额外运行时间。这些方面还可以得到改进。然而，有两个步骤需要高效的对应方案，才能将当前的译码转变为高效的译码：（1）基本情形；（2）列表译码论证。由于基本情形现在远弱于趋于零的比特错误概率，事实上，对于我们的论证能够成立，可能的最弱基本概率将是 $1/2 - 2^{-o(\sqrt{m})}$，因此人们或许可以期待一种高效的实现方式，但这目前仍是一个开放问题。为RM码获得高效的列表译码是第二个有趣的开放问题。

- **超越RM码：**如前多次提到，我们的基本情形是通用的，适用于任何对称码。人们可以希望在比RM码更一般的设置中开发提升框架。我们当前的版本是针对超立方体上多项式的求值而定制的，第一个扩展将是在此类设置中。要超越多项式求值码，首先需要理解受限码的行为。

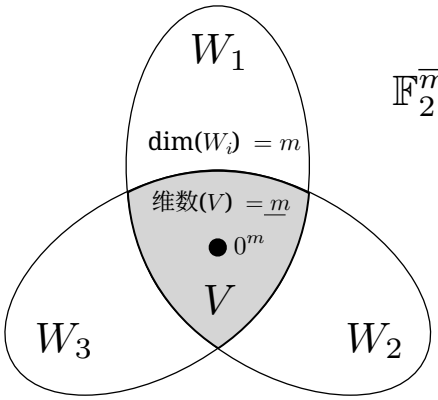

图 2: 一个（ m， m， m）子空间向日葵示意图，含有 3 个花瓣 W_1， W_2， W_3 和核 V .

5 设置：提升框架与向日葵

我们首先给出二元对称信道的证明，二元对称信道(ϵ)，因为它揭示了问题的本质，并将在第9节推广到其他 BMS 信道。

设 m， $r \in \mathbb{Z}^+$, $r \leq m$ 和 $\epsilon \in (0, 1/2)$。所用符号如下：

1。在 $RM(m, r)$ 中均匀随机抽取 f；这是传输的码字 d;

2. 生成噪声向量 $Z \in \mathbb{F}_2^{2^m}$ ：对每个 x，独立地以概率 ϵ 将 Z_x 设为 1，否则设为 0。

3. 集合 $\tilde{f} = f + Z$（在 $\mathbb{F}_2$ 上按分量计算）。

现在，设 $L_{m,r,\epsilon}(f)$ 为如下算法：在上述模型下，给定所有 $x \neq 0^m$ 的 $f(x)$ 的值，找出 $f(0^m)$ 最可能的取值；如果 0 和 1 的可能性相同，则返回一个均匀随机值。注意，我们移除了对 0^m 的观测，因为我们需要控制花瓣之间的依赖关系，而且这也与基本情形的设定相符。令

$$P_e(m, r, \epsilon) = \mathbb{P}(L_{m,r,\epsilon}(\tilde{f}) \neq f(0^m)).$$

备注*1.* 注意，对于任意 $f \in RM(m, r)$，运行 $L_{m,r,\epsilon}(f + f)$ 等价于运行$L_{m,r,\epsilon}(f)$，然后将 $f(0^m)$ 加到其输出上。因此，$L_{m,r,\epsilon}(f)$ 返回正确值的概率仅取决于 Z 的值。

注记2。 对于 0^m ，向解码器提供或不提供噪声比特，也就是说，使用比特错误概率而不是退出函数，当这些概率为常数量级时会有所不同，但当它们趋于零时则不再不同（因为二者相差一个常数因子）。因此，具有趋于零的比特错误概率等价于具有趋于零的退出函数。

定义 1. 对于任意 $0 \leq m < m < m$ 和 $b > 0$，一个大小为 b 的 (m, m, m)-子空间向日葵是 m-维子空间 $W_1, \ldots, W_b \subseteq \mathbb{F}_2^m$ 的一个集合，使得存在一个 m-维空间 $V \subseteq \mathbb{F}_2^m$ 满足对所有 i 有 $V \subseteq W_i$ 且对所有 $i \neq j$ 有 $W_i \cap W_j = V$。 W_i 被称为该向日葵的花瓣，而 V 被称为其核。

术语“向日葵”用于 [DF81] 集合，以及用于 [BDBD22] 子空间；我们在此仅依赖这一现有术语来描述感兴趣的子空间结构，但不需要与“向日葵引理”相关的结果 [DF81]，因为我们可以（高效地）构造我们的子空间向日葵。

现在，考虑以下算法用于将以高精度恢复 $f(0^m)$ 的能力对于某些指定的 m and r 转换为一种以更高精度恢复 $f(0^m)$ 的方法对于某些m 适度高于 m and 相同的 r，依赖于额外的参数 $m \leq m$ and b 如下：

提升算法$(f, m, m, m, r, \epsilon, b)$:

1. 选取一个大小为 b 的 (m, m, m)-子空间向日葵。

2. 在向日葵的每个花瓣上对 f 运行$L_{m,r,\epsilon}$，并返回最常见的输出（如遇平局，则掷一枚公平硬币）。

为了证明这是一种有用的方法，我们需要一些初步结果。首先，我们需要知道，可以找到一个足够大的子空间向日葵，正如下述引理所示。

引理 1. 令 $m < m < m$。那么就存在一个大小为 $2^{m+m+1-2m}$ 的 (m, m, m)-子空间向日葵 .

证明。我们任意选取一个 m 维核 V，并通过以下贪心算法构造花瓣 W_1，……，$W_{2^{m+m+1-2m}}$:

1. 对于 $1 \leq i \leq 2^{m+m+1-2m}$:

   (a) 设置 $W_i = V$(b) 当 $\dim(W_i) < m$ 时：i. 选取 $x \notin \cup_{i' \leq i} (W_{i'} + W_i)$。ii. 设置 $W_i = W_i + \{0, x\}$。

为了证明该算法可行，我们需要验证它的几个性质。首先，每个 W_i 最初都被设为 V，之后只会通过添加更多元素来改变，因此对于所有 i，始终有 $V \subseteq W_i$。其次，要求 $x \notin \cup_{i' \leq i} (W_{i'} + W_i)$ 可确保 $x \notin W_i$，并且对于每个 $i' < i$，$W_{i'} \cap (W_i + x) = \emptyset$。因此，对于所有 $i \neq j$，始终有 $W_i \cap W_j = V$。最后，注意每次执行到步骤 1.b.i 时，对于所有 $i' < i$，$(W_{i'} + W_i)$ 的维数至多为 $2m - m - 1$；而对于 $i' = i$，至多为 $m - 1$。因此，总会存在某个不属于 $\cup_{i' \leq i} (W_{i'} + W_i)$ 的 $x \in \mathbb{F}_2^m$。所以，该算法不会陷入停滞，从而能够找到具有所需性质的 W_1，……，$W_{2^{m+m+1-2m}}$，并构造出所需的向日葵。 □

接下来请注意，给定一个子空间向日葵，Z 在各个花瓣上的限制在给定 Z 在核上的限制后相互独立。为了讨论其含义，我们定义如下。

定义 2. 对于每个 $m \leq m$和 $z' \in \mathbb{F}_2^{2^m}$，令 $P_e(m, m, r, \epsilon | z')$ 为 $L_{m,r,\epsilon}(\tilde{f}) \neq f(0^m)$ 条件化于 Z 到 $\mathbb{F}_2^m \times 0^{m-m}$ 的限制为 z' 的概率。

在将 Z 限制到 V 为 z'的条件化下，仅根据将 f限制到 W_i来尝试确定 $f(0^m)$的值，将以概率 $P_e(m, m, r, \epsilon | z')$给出错误答案，并且这对所有 i都是独立的。因此，鉴于 m 合理地大于 $2m - m$，只需使 $P_e(m, m, r, \epsilon | z')$非平凡地小于 $1/2$，就几乎可以确保我们能够正确确定 $f(0^m)$的值。这就引出了这样一个问题： $P_e(m, m, r, \epsilon | z')$如此小的可能性有多大。

6 界定局部错误概率

6.1 $P_e(m,\ r,\ \epsilon)$ 上的基本情形：弱解码

我们首先在 $P_e(m,r,\epsilon)$ 上建立我们的基本情形，该基本情形只要求码具有对称性。我们直接针对一般的 BMS 信道和一般的"对称"码（如引理中所定义）陈述以下引理。

引理*2.* 设 $\mathcal{P}$ 是一个 *BMS*信道，且 $\{C_i\}_{i\geq 1}$ 是一个码率为 $\{R_i\}_{i\geq 1}$ 的码序列，满足上极限 $_{i\to\infty} R_i < C(\mathcal{P})$，并且 C_i 中的一个随机码字的每个坐标都服从参数为$1/2$ 的伯努利分布。令 $P_e(C_i, \mathcal{P}, j)$表示：在给定对随机码字 C_i 的其他噪声分量的观测结果时，最大似然解码器错误地解码分量 j 的概率。假设 $P_e(C_i, \mathcal{P}, j)$ 与 j 独立，并将其记为 $P_e(C_i, \mathcal{P})$。则存在 $c>0$，使得对于所有充分大的 i，$P_e(C_i, \mathcal{P}) < 1/2 - c$。

证明。令 $c' = C(\mathcal{P})$ −上极限$_{i\to\infty} R_i$。对于所有充分大的 i 值，省略隐含的索引 i，并记 X 为 C_i 的随机码字，Y 为其受干扰版本，以及 n =dim(C_i)，我们有

$$\begin{aligned} H(Y) &\leq H(Y,X) = H(Y|X) + H(X) && (2)\\ &\leq n(H(\mathcal{P}) + R) = n(H(Y_1) - (C(\mathcal{P}) - R)) && (3)\\ &\leq n(H(Y_1) - c'/2). && (4)\end{aligned}$$

此外，定义 $Y_{<j} = (Y_1,\ \ldots\ldots,\ Y_{j-1})$ 和 $Y_{-j} = (Y_1,\ \ldots\ldots,\ Y_{j-1},\ Y_{j+1},\ \ldots\ldots,\ Y_n)$，我们有

$$H(Y) = \sum_{j=1}^{n} H(Y_j|Y_{<j}), \tag{5}$$

并且必定存在 j，使得

$$H(Y_j|Y_{<j}) \leq H(Y_1) - c'/2 = H(Y_j) - c'/2. \tag{6}$$

此外，

$$\begin{aligned} H(X_1) - H(X_1|Y_2,\ldots,Y_n) &= I(X_1;Y_2,\ldots,Y_n) && (7)\\ &\geq I(Y_1;Y_2,\ldots,Y_n) = I(Y_j;Y_{-j}) && (8)\\ &\geq I(Y_j;Y_{<j}) \geq c'/2, && (9)\end{aligned}$$

其中（8）中的不等式使用了 $H(Y_2,\ \ldots\ldots,\ Y_n|X_1,\ Y_1) = H(Y_2,\ \ldots\ldots,\ Y_n|X_1)$。因此

$$H(X_1|Y_2,\ldots,Y_n) \leq 1 - c'/2. \tag{10}$$

最后，由于对于二元随机变量 U，$1 - \max_u p_U(u) = 1 - 2^{-H_\infty(U)} \leq 1 - 2^{-H(U)}$，其中$H_\infty(U)$ 是最小熵，根据詹森不等式（用于处理条件熵），我们有，

$$P_e(C,\mathcal{P}) \leq 1 - 2^{-H(X_1|Y_2,\ldots,Y_n)} \tag{11}$$

并且可以取任意 $c < (2^{c'/2} - 1)/2$（或 $c < (2^{c'} - 1)/2$ 通过收紧（4））。 □

对称性条件对任何双重传递码（如RM码）都成立 [KKM+16a],这意味着以下内容。

推论 1. 令 $\epsilon \in (0, 1/2)$，且 $\{m_i\}_{i\geq 1}$ 和 $\{r_i\}_{i\geq 1}$ 为正整数序列，使得$r_i \leq m_i$ 对所有 i 以及 极限$_{i\to\infty} m_i = \infty$ 和 上极限$_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i} < 1 - H(\epsilon)$。然后存在 $c>0$，使得 $P_e(m_i, r_i, \epsilon) < 1/2 - c$，对所有充分大的 i成立。

6.2 $P_e(m,\ m,\ r,\ \epsilon|z')$的傅里叶分析

从现在起，设定 $k = m - m$ 并考虑 ϵ，r 固定。为了分析函数 $Q_{m,\ m}\colon \mathrm{F}_2^m \ni z' \mapsto P_e(m,\ m,\ r,\ \epsilon|z')$ 的行为，我们将使用傅里叶分析。给定一个函数 $\mathcal{G}\colon \{0,1\}^{2^m} \to \mathrm{R}$，令 $\langle\mathcal{G}\rangle = \sum_{z'\in\{0,1\}^{2^m}} \epsilon^{|z'|}(1-\epsilon)^{2^m-|z'|}\mathcal{G}(z')$；给定两个函数$\mathcal{G}$，$\mathcal{H}\colon \{0,1\}^{2^m} \to \mathrm{R}$，令

$$\langle\mathcal{G},\mathcal{H}\rangle = \sum_{z'\in\{0,1\}^{2^m}} \epsilon^{|z'|}(1-\epsilon)^{2^m-|z'|}\mathcal{G}(z')\mathcal{H}(z').$$

现在，对每个 $S \subseteq \mathrm{F}_2^m$，令 $\mathcal{X}_S\colon \{0,1\}^{2^m} \to \mathrm{R}$ 为满足以下条件的函数:

$$\mathcal{X}_S(z') = \left(\frac{\epsilon}{1-\epsilon}\right)^{|S|/2}\left(-\frac{1-\epsilon}{\epsilon}\right)^{|\{x\in S:z'_x=1\}|}$$

对所有 z' 均成立。这些函数构成从 $\{0,1\}^{2^m}$ 到 R 的函数空间上偏置测度对应的正交归一傅里叶-沃尔什基，因此

$$Q_{m,m} = \sum_{S\subseteq\mathbb{F}_2^m} \langle Q_{m,m},\mathcal{X}_S\rangle\mathcal{X}_S.$$

此外，由于 $L_{m,\ r,\ \epsilon}(f)$ 与 $f(0^m)$ 相互独立，因此 $P_e(m,\ m,\ r,\ \epsilon|z')$ 与 z'_0 以及 0 相互独立，只要 $0^m \in S$。现在，对每个 $x \in \mathrm{F}_2^m$，令 $e_m(x)$ 为 F_2^m 中的元素，其前 m 个坐标由 x 给出，其余坐标设为 0。接下来，注意对所有 $m < m$，

$$Q_{m,m} = \sum_{S\subseteq\mathbb{F}_2^m} \langle Q_{m,m},\mathcal{X}_{e_m(S)}\rangle\mathcal{X}_S$$

因为对于任何无法表示为 $\mathcal{X}_{e_m(S)}$ 的 S'（其中 $S \subseteq \mathrm{F}_2^m$），都存在 $x \in S'$，使得在将 Z 限制到 $\mathrm{F}_2^{2^m}$ 为 z'这一条件下，Z_x 仍然是随机的，因此它对 $Q_{m,m}$ 的贡献会相互抵消。接下来，注意到

$$\begin{aligned}
\mathbb{P}[P_e(m,m,r,\epsilon|z') \geq 1/3] &\leq \mathbb{E}[9P^2_{m,m,r,\epsilon}(z')] &(12)\\
&= 9\langle Q_{m,m},Q_{m,m}\rangle &(13)\\
&= 9\sum_{S\subseteq\mathbb{F}_2^m}\langle Q_{m,m},\mathcal{X}_{e_m(S)}\rangle^2 &(14)
\end{aligned}$$

因此，为了界定 $P_e(m,\ m,\ r,\ \epsilon|z') \geq 1/3$ 的概率，只需证明乘积 $\langle Q_{m,m},\mathcal{X}_{e_m(S)}\rangle$ 足够小。

接下来注意到，$Q_{m,\ m}$ 在仿射变换下具有对称性。因此，如果 S' 是 S 的仿射变换（更具体地说，是线性变换），那么必然有$\langle Q_{m,m},\mathcal{X}_S\rangle = \langle Q_{m,m},\mathcal{X}_{S'}\rangle$。现在，对每个 $S \subseteq \mathrm{F}_2^m$，令 S为 S 和 $\mathcal{X}_S = \sum_{S'\in S}\mathcal{X}_{S'}$的仿射变换集合。此外，令 S 为 F_2^m的一个最大子集列表，其中任意两个子集都不在仿射变换下等价。于是，对每个 $S \subseteq \mathrm{F}_2^m$，令 $\dim(S)$ 表示由 S张成的 F_2^m子空间的维数。给定 $S \subseteq \mathrm{F}_2^m$，存在 $\dim(S)$ 个非零线性无关点x_1，……，$x_{\dim(S)} \in S$。对于任意线性变换 π，当且仅当对所有 i，$\pi(S)$ 属于 F_2^m，且 $\pi(x_i) \in \mathrm{F}_2^m$。此外，对于随机线性变换 π，并在$\pi(x_1)$，……，$\pi(x_{i-1})$取任意固定值的条件下，$\pi(x_i)$的概率分布是在那些

不属于 $Span(\pi(x_1),\ .....,\ \pi(x_{i-1}))$ 的点上的均匀分布。因此 $\mathrm{P}[\pi(S) \subsetneq \mathrm{F}_2^m] \leq (2^{m-m})$ $^{\dim(S)} = 2^{-k\cdot\dim(S)}$。因此

$$\sum_{S\subseteq\mathbb{F}_2^m} \langle Q_{m,m}, \mathcal{X}_{e_m(S)}\rangle^2 \leq \sum_{S\in\mathbb{S}} |\overline{S}| 2^{-k\cdot\dim(S)} \langle Q_{m,m}, \mathcal{X}_S\rangle^2 \tag{15}$$

$$= \sum_{S\in\mathbb{S}} \frac{1}{|\overline{S}|} 2^{-k\cdot\dim(S)} \langle Q_{m,m}, \mathcal{X}_{\overline{S}}\rangle^2. \tag{16}$$

6.3 通过单次向日葵增强和 L_2-范数实现趋于零的比特错误概率

回想一下 $k = m - m$.

引理 3. 设 $0 \leq m < \underline{m}$ 和 $r \geq 0$ 为整数，且 $\epsilon \in (0, 1/2)$。那么，当通过将其中每个元素独立地以概率 ϵ 设为1，否则设为0 的方式选取 $z' \in \{0,1\}^{2^m}$ 时，

$$\mathbb{P}[P_e(\underline{m}, m, r, \epsilon|z') \geq P_e(m, r, \epsilon)/2 + 1/4] \leq \frac{2^{2-k}}{(1/2 - P_e(m, r, \epsilon))^2}.$$

证明。 首先，令 $c = 1/2 - P_e(m, r, \epsilon)$，并注意到

$$\mathbb{P}[P_e(\underline{m}, m, r, \epsilon|z') \geq 1/2 - c/2] \tag{17}$$

$$\leq \mathbb{E}[(P_e(\underline{m}, m, r, \epsilon|z') - (1/2 - c))^2]](4/c^2) \tag{18}$$

$$= \frac{4}{c^2} \sum_{S\subseteq\mathbb{F}_2^m : S\neq\emptyset} \langle Q_{m,m}, \mathcal{X}_{e_m(S)}\rangle^2 \tag{19}$$

$$\leq \frac{4}{c^2} \sum_{S\in\mathbb{S}: S\neq\emptyset} \frac{1}{|\overline{S}|} 2^{-k\cdot\dim(S)} \langle Q_{m,m}, \mathcal{X}_{\overline{S}}\rangle^2 \tag{20}$$

$$= \frac{4}{c^2} \sum_{S\in\mathbb{S}: S\neq\emptyset, 0^{\underline{m}}\notin S} \frac{1}{|\overline{S}|} 2^{-k\cdot\dim(S)} \langle Q_{m,m}, \mathcal{X}_{\overline{S}}\rangle^2 \tag{21}$$

$$\leq \frac{4}{c^2} \sum_{S\in\mathbb{S}: S\neq\emptyset, 0^{\underline{m}}\notin S} \frac{1}{|\overline{S}|} 2^{-k} \langle Q_{m,m}, \mathcal{X}_{\overline{S}}\rangle^2 \tag{22}$$

$$\leq \frac{2^{2-k}}{c^2} \sum_{S\in\mathbb{S}} \frac{1}{|\overline{S}|} \langle Q_{m,m}, \mathcal{X}_{\overline{S}}\rangle^2 \tag{23}$$

$$= \frac{2^{2-k}}{c^2} \mathbb{E}[P_e^2(m, m, r, \epsilon|z')] \tag{24}$$

$$\leq \frac{2^{2-k}}{c^2} \tag{25}$$

如所需。 □

因此我们得到以下结果，这意味着来自 [RP21], 即，趋于零的比特错误概率，衰减更快，在 m.

引理 4. 设 $\epsilon \in (0, 1/2)$，以及 $m_1, m_2, m_3, ...$ 和 $r_1, r_2, ...$ 为正整数序列，使得 极限$_{i\to\infty}\, m_i = \infty$ 且上极限$_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i} < 1 - H(\epsilon)$。则 极限$_{i\to\infty} P_e(m_i, r_i, \epsilon) = O(2^{-\sqrt[3]{m_i}})$。

证明。首先，对每个 i 令 $m_i' = \overline{m_i} - 2\lfloor \sqrt[3]{m_i} \rfloor$，并注意到上极限 $\limsup_{i\to\infty} \binom{m_i'}{\leq r} 2^{-m_i}$ 等于上极限 $\limsup_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i}$。现在，令 $m_i = \underline{m_i} - 3\lfloor \sqrt[3]{m_i} \rfloor$，对每个 i，并考虑使用以下增强算法从 f 确定的值 $f(0^{m_i})$：

选取一个 $(\underline{m_i},\ m_i',\ m_i)$-子空间向日葵，其大小为 $2^{\underline{m_i}+m_i-2m_i'+1}$，且独立于 $\tilde{f}$。

2. 在向日葵的每个花瓣上运行 $L_{m_i',r_i,\epsilon}$ 对 f 的限制，并返回最常见的输出。

根据引理 1，可以找到这样的子空间向日葵，从而能够执行该算法。此外，如果我们令 z' 为 Z 在核上的限制，那么在 z' 取定值的条件下，算法最后一步中对 L 的每次使用都会独立地返回一个与 $f(0^{m_i})$ 不同的值，其概率为 $P_e(m_i, m_i', r_i, \epsilon|z')$。根据推论 1，存在 $c > 0$，使得对于所有充分大的 i，$P_e(\overline{m_i'}, r_i, \epsilon) < 1/2 - c$。那么前一个引理意味着

$$\mathbb{P}[P_e(\underline{m_i}, m_i', r_i, \epsilon|z') \geq 1/2 - c/2] \leq 2^{2-\lfloor \sqrt[3]{m_i} \rfloor}/c^2$$

对于任何这样的 i。条件化于 z' such that $P_e(m_i, m_i', r_i, \epsilon|z') < 1/2 - c/2$ 的任何固定值，该算法以至多 $(4(1/2-c)(1/2+c))^{2^{m_i+m_1-2m_i'}}$ 的概率返回错误答案，因此其返回与 $f(0^{m_i})$ 不同的值的总体概率至多为 $2^{2-\lfloor \sqrt[3]{m_i} \rfloor}/c^2 + (1-4c^2)^{2^{\lfloor \sqrt[3]{m_i} \rfloor}} = O(2^{-\sqrt[3]{m_i}})$。此外，该算法从不使用 $\tilde{f}(0^{m_i})$ 的值，并且 L 计算 $f(0^m)$ at least 与任何忽略 $f(0^m)$ 值的其他算法一样准确，因此它也具有 $O(2^{-\sqrt[3]{m_i}})$ 的错误率，如所期望。

□

6.4 通过 L_4-范数在低维子集上的非集中

此时，我们知道 $P_e(m_i, r_i, \epsilon)$ 随着 i 增加而趋于 0。然而，为了证明我们可以以高概率恢复 f，我们需要对 $P_e(m_i, r_i, \epsilon)$ 有更紧的界，而为了得到这些界，我们需要界定 $Q_{m,m}$ 的傅里叶变换中具有低维支撑的项的贡献，而不仅仅是论证每个非常数项的支撑维数至少为 1。柯西-施瓦茨无法对傅里叶项建立非平凡的界；然而，我们可以使用 $\mathcal{X}_S$ 在输入空间中其取值最高的大小为 $P_e(m, r, \epsilon)$ 的那部分上的平均值来界定 $\langle Q_{m,m}, \mathcal{X}_S \rangle$，而这又可以使用某个 $b > 2$ 的 $\mathcal{X}_S^b$ 的期望值来界定。更正式地，对于任意 $S \subseteq \mathbb{F}_2^m$，必须有

$$\begin{aligned}
&\langle Q_{m,m}, \mathcal{X}_{\overline{S}} \rangle && (26)\\
&= \sum_{z' \in \{0,1\}^{2^m}} \epsilon^{|z'|}(1-\epsilon)^{2^m-|z'|} Q_{m,m}(z') \mathcal{X}_{\overline{S}}(z') && (27)\\
&\leq \left(\sum_{z' \in \{0,1\}^{2^m}} \epsilon^{|z'|}(1-\epsilon)^{2^m-|z'|} Q_{m,m}^{4/3}(z') \right)^{3/4} \sqrt[4]{\sum_{z' \in \{0,1\}^{2^m}} \epsilon^{|z'|}(1-\epsilon)^{2^m-|z'|} \mathcal{X}_{\overline{S}}^4(z')} && (28)\\
&= \langle Q_{m,m}^{4/3} \rangle^{3/4} \sqrt[4]{\langle \mathcal{X}_{\overline{S}}^4 \rangle} && (29)\\
&\leq \langle Q_{m,m} \rangle^{3/4} \sqrt[4]{\langle \mathcal{X}_{\overline{S}}^4 \rangle} && (30)\\
&= P_e^{3/4}(m, r, \epsilon) \sqrt[4]{\langle \mathcal{X}_{\overline{S}}^4 \rangle}. && (31)
\end{aligned}$$

此时，我们需要对 $\langle \mathcal{X}_S^4 \rangle$ 给出界，例如如下所示。

引理 5. 令 m 为正整数，$S \subseteq \mathbb{F}_2^m$，以及 $\epsilon \in (0,\ 1/2)$。则 $\langle \mathcal{X}_S^4 \rangle \le 2^{2dm+8d^2}(1/\epsilon(1-\epsilon))^{2^d}$，其中 $d =$ 维数(S)

证明。首先，注意到

$$\langle \mathcal{X}_{\overline{S}}^4 \rangle = \sum_{S_1,S_2,S_3,S_4 \in \overline{S}} \langle \mathcal{X}_{S_1} \cdot \mathcal{X}_{S_2} \cdot \mathcal{X}_{S_3} \cdot \mathcal{X}_{S_4} \rangle.$$

如果存在某个 x，它恰好属于 S_1、S_2、S_3 中的一个，并且 S_4，那么 $\langle \mathcal{X}_{S_1} \cdot \mathcal{X}_{S_2} \cdot \mathcal{X}_{S_3} \cdot \mathcal{X}_{S_4} \rangle = 0$，因为满足 $z'_x = 1$ 的 z' 的贡献抵消了满足 $z'_x = 0$ 的 z' 的贡献。如果不存在这样的 x，那么

$$\begin{aligned}
&\langle \mathcal{X}_{S_1} \cdot \mathcal{X}_{S_2} \cdot \mathcal{X}_{S_3} \cdot \mathcal{X}_{S_4} \rangle && (32)\\
&\le \max(((1-\epsilon)+\epsilon)^{2|S|}, (((1-\epsilon)^2+\epsilon^2)/\sqrt{\epsilon(1-\epsilon)})^{4|S|/3}, (((1-\epsilon)^3+\epsilon^3)/(\epsilon(1-\epsilon)))^{|S|}) && (33)\\
&\le (1/\epsilon(1-\epsilon))^{|S|}. && (34)
\end{aligned}$$

我们有，$S_1 \cup S_2 \cup S_3 \cup S_4$ 必须包含$\dim(S_1 \cup S_2 \cup S_3 \cup S_4)$ 个线性无关的点。如果不存在一个 x 恰好属于这些集合中的一个，那么这些点中的每一个都必须至少属于两个

S_i $d \ge$ $S_1 \cup S_2 \cup S_3 \cup S_4$ $/2$ 2^{2dm}，这意味着 $\dim(\ )$。F_2^m $2d$ 中至多有 个-维子空间，并且任意这样的子空间中至多包含个仿射变换。因此，$\langle \mathcal{X}_S^4 \rangle \le 2^{2dm+8d^2}(1/\epsilon(1-\epsilon))^{2^d}$，如所需。 2^{2d^2} S □

6.5 界定较大 $P_e(m,m,r,\epsilon|z')$ 的概率

这最终使我们能够如下界定 $\sum_{S \subseteq \mathbb{F}_2^m} \langle Q_{m,m}, \mathcal{X}_{e_m(S)} \rangle^2$：

引理 6。设 $0 \le m \le m$ 和 $r \ge 0$ 为整数，且 $\epsilon \in (0,\ 1/2)$。令 $z' \in \{0,1\}^{2m}$ 的每个元素独立地以概率 ϵ 设为 1，否则设为 0，则

$$\mathbb{P}[P_e(\underline{m},m,r,\epsilon|z') \ge 1/3] \le 18P_e^{5/4}(m,r,\epsilon) + 9P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k$$

证明。对于任意整数 $0 \le d_0 \le m$,

$$\begin{aligned}
&\sum_{S \subseteq \mathbb{F}_2^{\frac{m}{2}}} \langle Q_{m,m}, \mathcal{X}_{e_m(S)} \rangle^2 && (35)\\
&\le \sum_{S \in \mathbb{S}} \frac{1}{|\overline{S}|} 2^{-k \cdot \dim(S)} \langle Q_{m,m}, \mathcal{X}_{\overline{S}} \rangle^2 && (36)\\
&= \sum_{d=0}^{m} \sum_{S \in \mathbb{S}:\dim(S)=d} \frac{1}{|\overline{S}|} 2^{-kd} \langle Q_{m,m}, \mathcal{X}_{\overline{S}} \rangle^2 && (37)\\
&= \sum_{d=0}^{d_0-1} \sum_{S \in \mathbb{S}:\dim(S)=d} \frac{1}{|\overline{S}|} 2^{-kd} \langle Q_{m,m}, \mathcal{X}_{\overline{S}} \rangle^2 + \sum_{d=d_0}^{m} \sum_{S \in \mathbb{S}:\dim(S)=d} \frac{1}{|\overline{S}|} 2^{-kd} \langle Q_{m,m}, \mathcal{X}_{\overline{S}} \rangle^2 && (38)
\end{aligned}$$

现在请注意，对于任意给定的 d，F_2^m 中 d-维子集在仿射变换下至多有 2^{2^d} 个等价类，因为每个这样的集合都可以映射到 F_2^d 的一个子集。反过来，对于每个 d，F_2^m 中至少有 $2^{d(m-d)}$ d-维子空间，因此对于任意集合

S 至少有 $2^{\dim(S)(m-\dim(S))}$ 个集合可以通过对 S应用仿射变换生成。因此，

$$\sum_{d=0}^{d_0-1}\sum_{S\in\mathbb{S}:\dim(S)=d}\frac{1}{|\overline{S}|}2^{-kd}\langle Q_{m,m},\mathcal{X}_{\overline{S}}\rangle^2 \tag{39}$$

$$\leq \sum_{d=0}^{d_0-1}\sum_{S\in\mathbb{S}:\dim(S)=d}\frac{1}{|\overline{S}|}\langle Q_{m,m},\mathcal{X}_{\overline{S}}\rangle^2 \tag{40}$$

$$\leq \sum_{d=0}^{d_0-1}\sum_{S\in\mathbb{S}:\dim(S)=d}\frac{1}{|\overline{S}|}P_e^{3/2}(m,r,\epsilon)\sqrt{\langle\mathcal{X}_{\overline{S}}^4\rangle} \tag{41}$$

$$\leq \sum_{d=0}^{d_0-1}\sum_{S\in\mathbb{S}:\dim(S)=d}2^{-d(m-d)}P_e^{3/2}(m,r,\epsilon)2^{md+4d^2}(1/\epsilon(1-\epsilon))^{2^{d-1}} \tag{42}$$

$$\leq \sum_{d=0}^{d_0-1}2^{2^d}2^{-d(m-d)}P_e^{3/2}(m,r,\epsilon)2^{md+4d^2}(1/\epsilon(1-\epsilon))^{2^{d-1}} \tag{43}$$

$$= P_e^{3/2}(m,r,\epsilon)\sum_{d=0}^{d_0-1}2^{5d^2}(4/\epsilon(1-\epsilon))^{2^{d-1}} \tag{44}$$

$$\leq P_e^{3/2}(m,r,\epsilon)\sum_{d=0}^{d_0-1}(64/\epsilon(1-\epsilon))^{2^d} \tag{45}$$

$$\leq 2P_e^{3/2}(m,r,\epsilon)(64/\epsilon(1-\epsilon))^{2^{d_0-1}}. \tag{46}$$

现在，我们可以利用这样一个事实来界定高维项的贡献：$Q_{m,m}$ 的变换中所有系数的平方和至多为 $P_e(m,r,\epsilon)$，然后再将 2^{-kd} 的因子考虑在内。更准确地说，

$$\sum_{d=d_0}^{m}\sum_{S\in\mathbb{S}:\dim(S)=d}\frac{1}{|\overline{S}|}2^{-kd}\langle Q_{m,m},\mathcal{X}_{\overline{S}}\rangle^2 \tag{47}$$

$$\leq 2^{-kd_0}\sum_{d=d_0}^{m}\sum_{S\in\mathbb{S}:\dim(S)=d}\frac{1}{|\overline{S}|}\langle Q_{m,m},\mathcal{X}_{\overline{S}}\rangle^2 \tag{48}$$

$$\leq 2^{-kd_0}\sum_{S\in\mathbb{S}}\frac{1}{|\overline{S}|}\langle Q_{m,m},\mathcal{X}_{\overline{S}}\rangle^2 \tag{49}$$

$$= 2^{-kd_0}\sum_{S\subseteq\mathbb{F}_2^m}\langle Q_{m,m},\mathcal{X}_S\rangle^2 \tag{50}$$

$$= 2^{-kd_0}\langle Q_{m,m},Q_{m,m}\rangle \tag{51}$$

$$\leq 2^{-kd_0}\langle Q_{m,m}\rangle \tag{52}$$

$$= P_e(m,r,\epsilon)2^{-kd_0}. \tag{53}$$

因此，

$$\sum_{S\subseteq\mathbb{F}_2^m}\langle Q_{m,m},\mathcal{X}_{e_m(S)}\rangle^2 \leq 2P_e^{3/2}(m,r,\epsilon)(64/\epsilon(1-\epsilon))^{2^{d_0-1}}+P_e(m,r,\epsilon)2^{-kd_0}.$$

特别地，如果我们设 $d_0 = \max\left\{\lceil \log_2 \frac{\log(1/P_e(m,r,\epsilon))}{4\log(64/\epsilon(1-\epsilon))} \right\}, 0\right\}$ 我们得到

$$\sum_{S\subseteq \mathbb{F}_2^{\frac{m}{2}}} \langle Q_{m,m}, \mathcal{X}_{e_m(S)}\rangle^2 \leq 2P_e^{5/4}(m,r,\epsilon) + P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k$$

这进而意味着

$$\begin{aligned}
&\mathbb{P}[P_e(\underline{m},m,r,\epsilon|z') \geq 1/3] && (54)\\
&\leq \mathbb{E}[9P^2_{\underline{m},m,r,\epsilon}(z')] && (55)\\
&= 9\langle Q_{\underline{m},m}, Q_{\underline{m},m}\rangle && (56)\\
&= 9\sum_{S\subseteq \mathbb{F}_2^{\frac{m}{2}}} \langle Q_{m,m}, \mathcal{X}_{e_m(S)}\rangle^2 && (57)\\
&\leq 18P_e^{5/4}(m,r,\epsilon) + 9P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k && (58)
\end{aligned}$$

如所需。 □

6.6关于 $P_e(m,r,\epsilon)$ 的界：通过递归向日葵增强达到临界区域

此时，我们终于可以开始使用以下内容递归地构造关于 P_e 的界：

引理7。令 m、$\overline{m}$、k 和 r 为正整数，使得 $k \leq \min(m, \overline{m}-m)$ 且 $\epsilon \in (0, 1/2)$。那么

$$P_e(\overline{m},r,\epsilon) \leq 18P_e^{5/4}(m,r,\epsilon) + 9P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k + (8/9)^{2^{\overline{m}-m-k}}.$$

证明。令 $\tilde{m} = m-k$，并考虑使用以下增强算法译码 $\tilde{f}(0^m)$ 在 f 中的值：

1. 独立于 $\tilde{f}$，选取一个大小为 $2^{m+\tilde{m}-2m+1}$ 的 $(\overline{m}, \tilde{m}, m)$-子空间向日葵。
2. 运行 $L_{\tilde{m}}$ 将其限制在 f 的每个花瓣上，并返回出现次数最多的输出。

根据引理 1，可以找到这样的子空间向日葵，因此该算法可以执行。此外，若令 z' 表示 Z 在核上的限制，那么在给定z' 的固定取值后，算法最后一步中的每次 L 调用都会独立地返回一个与 $f(0^m)$ 不同的值，其概率为 $P_e(m, m, r, \epsilon|z')$。

$$\mathbb{P}[P_e(\underline{m},m,r,\epsilon|z') \geq 1/3] \leq 18P_e^{5/4}(m,r,\epsilon) + 9P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k$$

根据前一个引理，并且在条件化于 z' 的任意固定值且满足 $P_e(m,m,r,\epsilon|z') < 1/3$ 的情况下，该算法返回错误答案的概率至多为$(8/9)^{2^{m+\tilde{m}-2m}} = (8/9)^{2^{\tilde{m}-m-k}}$。因此，该算法将 $f(0^m)$ 判错的概率至多为

$$18P_e^{5/4}(m,r,\epsilon) + 9P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k + (8/9)^{2^{\overline{m}-m-k}}.$$

该算法中没有任何部分使用 $f(0^m)$ 的值，而 $L_{m,r,\epsilon}(f)$ 从 f 在计算出 $f(0^m)$，其准确率至少与任何忽略 $f(0^m)$ 值的其他算法所达到的准确率一样高，因此其错误率至多为

$$18P_e^{5/4}(m,r,\epsilon)+9P_e(m,r,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m,r,\epsilon))}\right)^k+(8/9)^{2^{\overline{m}-m-k}},$$

如所需。 □

这使我们能够将关于 $P_e(m,\ r,\ \epsilon)$ 的界转换为关于 $P_e(m,\ r,\ \epsilon)$ 的更紧界，其中 m 略大于 m。现在我们的计划是利用这一点证明越来越紧的界，从引理4所确立的界开始。由此得到以下结果。

引理 8. 令 $\epsilon\in(0,1/2)$，以及 $m_1,m_2,m_3,\ldots$ 和 $r_1,r_2,\ldots$ 为正整数序列，使得 极限$_{i\to\infty}\,m_i=\infty$ 且上极限$_{i\to\infty}\binom{m_i}{\le r_i}2^{-m_i}\le 1-H(\epsilon)$。则存在 $c>0$ 使得$P_e(m_i,r_i,\epsilon)=O(m_i^{-c\sqrt{m_i}})$。

证明. F 首先，注意到对于任意充分小的常数 c'，都将有

$$\limsup_{i\to\infty}\binom{m_i-c'\sqrt{m_i}}{\le r}2^{-m_i}$$

也严格小于 $1-H(\epsilon)$。因此，选择这样的 c' 并令 $m_i'=m_i-\lfloor c'\sqrt{m_i}\rfloor$ 对每个 i成立，并回忆一下 $P_e(m_i',\ r_e,\ \epsilon)=O(2^{-\sqrt[3]{m_i}})$，根据引理 4。这意味着存在 i_0，使得对所有 $i\ge i_0,\ m_i\ge 2$ 并且

$$P_e(m_i-\lfloor c'\sqrt{m_i}\rfloor,r_i,\epsilon)\le\min(e^{-108\ln(64/\epsilon(1-\epsilon))\sqrt[4]{m_i}},2^{-2\log_2^2(m_i)}/54^4).$$

因此，对于任意 $i\ge i_0$ 和 $m''\ge m_i-\lfloor c'\sqrt{m_i}\rfloor$，必定有娱乐主管

$$\begin{aligned}
&P_e(m''+2\lceil\log_2 m_i\rceil,\ r_i,\ \epsilon) && (59)\\
&\le 18P_e^{5/4}(m'',r_i,\epsilon)+9P_e(m'',r_i,\epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m'',r_i,\epsilon))}\right)^{\log_2(m_i)}+(8/9)^{m_i} && (60)\\
&\le 2^{-\log_2^2(m_i)/2}P_e(m'',r_i,\epsilon)/3+m_i^{-\log_2(m_i)/4}P_e(m'',r_i,\epsilon)/3+(8/9)^{m_i} && (61)\\
&\le\max(2^{-\log_2^2(m_i)/4}P_e(m'',r_i,\epsilon),3(8/9)^{m_i}). && (62)
\end{aligned}$$

应用此操作$\left\lceil\frac{\lfloor c'\sqrt{m_i}\rfloor}{2m_i}\right\rceil$次意味着对于所有 $i\ge i_1$，

$$P_e(m_i,r_i,\epsilon)\le\max\left(2^{-c'\log_2(m_i)\sqrt{m_i}/16},3(8/9)^{m_i}\right).$$

这为我们得出了 $c=c'/16$ 所需的结论。 □

7 恢复码字

此时，我们终于准备好从能够以高概率恢复码中的任意给定比特，进展到能够以高概率完全恢复码字。

7.1 列表译码与重量枚举式

为此，我们首先将证明：在以下意义下，存在一个既接近真实码字、又比真实码字更合理的码字，这种情况极不可能发生。

引理 9. 设 $c > 0$, $\epsilon \in (0, 1/2)$，且 $m_1, m_2, \ldots$ 和 $r_1, r_2, \ldots$ 是正整数序列，满足 $\lim_{i\to\infty} m_i = \infty$ and $|m_i - 2r_i| = O(\sqrt{m_i})$。那么，当 $i \to \infty$ 趋于极限时，若从 $RM(m_i, r_i)$ 中随机抽取 f，且 f 是 f 的含噪版本，其中每个比特都以概率 ϵ 独立翻转，则以概率 $1 - O(2^{-2^{m/3}})$，不存在与 f 不同的 $f^\star \in RM(m_i, r_i)$，使得 $f^\star$ 与 f 至多在 $2^{m-c\sqrt{m}}\log_2(m)$ 个元素上不一致，并且 $f^\star$ 与 $\tilde{f}$ 一致的元素数不少于 f。

证明。首先，注意到在 [SS20], 的定理 1.2 的证明第 17 页中，$RM(m, r)$ 中与 f 至多在 2^{m-l} 个元素上不一致的元素数量至多为

$$2^{\sum_{j=l}^{r} 17m(j-1)(j+2)+17(j+2)\binom{m-(j-1)}{\leq r-(j-1)}}$$

对每个 $l \in \mathbb{Z}^+$ 都成立。给定 $f^\star \in RM(m, r)$，$f^\star$ 与 $\tilde{f}$ 的一致程度至少和 f 一样高的概率至多为 $(4\epsilon(1-\epsilon))^{|\{x:f(x)\neq f^\star(x)\}|/2}$，因为我们需要翻转至少等于距离一半数量的比特。因此，存在一个不同于 f 的码字，它与 f 的距离在 $2^{m-c\sqrt{m}\log_2(m)}$ 个元素以内，且与 $\tilde{f}$ 的一致程度至少和 f 一样高的概率至多为：

$$\sum_{f^\star\in RM(m,r):0<|\{x:f(x)\neq f^\star(x)\}|\leq 2^{m-\lfloor c\sqrt{m}\log_2(m)\rfloor}} (4\epsilon(1-\epsilon))^{|\{x:f(x)\neq f^\star(x)\}|/2} \tag{63}$$

$$= \sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r} \sum_{f^\star\in RM(m,r):2^{m-l-1}<|\{x:f(x)\neq f^\star(x)\}|\leq 2^{m-l}} (4\epsilon(1-\epsilon))^{|\{x:f(x)\neq f^\star(x)\}|/2} \tag{64}$$

$$\leq \sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r} \sum_{f^\star\in RM(m,r):2^{m-l-1}<|\{x:f(x)\neq f^\star(x)\}|\leq 2^{m-l}} (4\epsilon(1-\epsilon))^{2^{m-l-2}} \tag{65}$$

$$\leq \sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r} (4\epsilon(1-\epsilon))^{2^{m-l-2}} 2^{\sum_{j=l}^{r} 17m(j-1)(j+2)+17(j+2)\binom{m-(j-1)}{\leq r-(j-1)}}. \tag{66}$$

现在，注意到 $|m-2r| = O(\sqrt{m})$，因此存在 i_0，使得只要 $i \geq i_0$，就有 $|m-2r| \leq c\sqrt{m}\log_2(m)/2 - 2$。给定这样的 i，注意到对于任意满足 $j \geq l \geq \lfloor c\sqrt{m}\log_2(m)\rfloor$ 的情况，Chernoff 界表明

$$\binom{m-(j-1)}{\leq r-(j-1)} \leq 2^{m-(j-1)} e^{-\left(\frac{m-r}{m-j+1}-\frac{1}{2}\right)^2 (m-j+1)} \tag{67}$$

$$= 2^{m-(j-1)} e^{-\frac{(m-2r+j-1)^2}{4(m-j+1)}} \tag{68}$$

$$\leq 2^{m-(j-1)} e^{-\frac{(c\sqrt{m}\log_2(m)/2)^2}{4m}} \tag{69}$$

$$= 2^{m-(j-1)} e^{-\frac{c^2\log_2^2(m)}{16}}. \tag{70}$$

因此，对于 i的任何足够大取值，存在一个不同于 f的码字，该码字与 f 相差至多 $2^{m-c\sqrt{m}\log_2(m)}$ 个元素，并且在至少同样多的元素上与 $\tilde{f}$ 一致

由于 f 至多为:

$$\sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r}(4\epsilon(1-\epsilon))^{2^{m-l-2}}2^{\sum_{j=l}^{r}17m(j-1)(j+2)+17(j+2)2^{m-(j-1)}}e^{-\frac{c^2\log_2^2(m)}{16}} \tag{71}$$

$$\leq \sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r}(4\epsilon(1-\epsilon))^{2^{m-l-2}}2^{17mr(r-1)(r+2)+17r(r+2)2^{m-(l-1)}}e^{-\frac{c^2\log_2^2(m)}{16}} \tag{72}$$

$$= 2^{17mr(r-1)(r+2)}\sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r}2^{\left(136r(r+2)e^{-\frac{c^2\log_2^2(m)}{16}}-\log_2(1/4\epsilon(1-\epsilon))\right)2^{m-l-2}}. \tag{73}$$

现在，观察到 $136r(r+2))e^{-\frac{c^2}{\log_2^2(m)\,16}} = O(1)$，因此每当 i 足够大时，这将小于

$$2^{17mr(r-1)(r+2)}\sum_{l=\lfloor c\sqrt{m}\log_2(m)\rfloor}^{r}2^{-\log_2(1/4\epsilon(1-\epsilon))2^{m-l-3}} \tag{74}$$

$$\leq r2^{17mr(r-1)(r+2)-\log_2(1/4\epsilon(1-\epsilon))2^{m-r-3}} = O(2^{-\sqrt[3]{n}}). \tag{75}$$

因此不存在这样的 $f^\star$，其概率为 $1-O(2^{-\sqrt[3]{n}})$，正如所期望的。 □

这暗示了以下用于恢复码字的算法。

RM reconstruction algorithm(m,r,ϵ,f,c)：

1. 对于每个 x，令 $f(x)$ 为给定 f 时 $f(x)$ 的最可能值，或者如果 0 和 1 等可能则取均匀随机值。

2. 设 ℓ 为 $RM(m,r)$ 中所有与 f 至多在 $2^{m-c\sqrt{m}\log_2(m)/2}/2$ 个元素上不一致的元素组成的列表。

3. 返回 ℓ 中与 f 在最多元素上相符的元素，出现平局时均匀随机选择。

我们声称，以如下意义，这能够以高概率完全恢复原始码字

定理 2. 设 $\epsilon\in(0,1/2)$，且 $m_1,m_2,\ldots$ 以及 $r_1,r_2,\ldots$ 是正整数序列，满足 $\lim_{i\to\infty}m_i=\infty$ 和上极限 $\lim_{i\to\infty}\binom{m_i}{\leq r_i}2^{-m_i}<1-H(\epsilon)$。另设 c 为引理 8 所述存在的常数。那么当 $i\to\infty$ 取极限时，若 f 是从 $RM(m,r)$ 中随机抽取的，且 f 是 f 的含噪版本，其中每个比特以概率 ϵ 独立翻转，则 *RM reconstruction algorithm*$(m,r,\epsilon,\tilde{f},c)$ 以概率 $1-O(2^{-c\sqrt{m}\log_2(m)/2})$ 返回 f。

证明. 首先，注意由引理 8 以及 x 不同值之间的对称性，$\mathrm{P}[f(x)\neq f(x)]=O(m^{-c\sqrt{m}})$ 对所有 x 成立。所以，$f\in\ell$ 以概率 $1-O(2^{-c\sqrt{m}\log_2(m)/2})$，在这种情况下 ℓ 的每个元素将与 f 至多在 $2^{m-c\sqrt{m}\log_2(m)/2}$ 个元素上不一致。由前一个引理，该概率

˜发生这种情况，并且 ℓ 中存在一个元素，该元素与 f 一致的元素数量至少和 f 一样多，其概率为 $1-O(2^{-2^{m/3}})$（注意 $\ell \subseteq RM(m_i, \max(r_i, m_i/2))$，因此我们不必担心在 r_i 过小时无法应用引理）。因此，该算法以 $1-O(2^{-c\sqrt{m}\log_2(m)/2})$的概率恢复 f，如所需。

□

7.2 通过网格增强降低块错误概率

到目前为止，我们知道可以以较高概率恢复该码，但我们的错误概率界趋于 0 的速度相当慢。接下来我们将证明更好的错误概率界，为此，我们将考虑以下算法。

RM reconstruction algorithm2$(m, r, \epsilon, f, c, c')$:

1. 令 $m' = \lceil \sqrt{m}/c \rceil$。 2. 将索引 $1, ..., m$ 划分为集合 $S_1, ..., S_{m'}$，使这些集合的大小尽可能相等。 3. 对每个 $1 \leq i \leq m'$ 和 $x \in \{0,1\}^{S_i}$，令 $f^{(i,x)} = RM\ reconstruction\ algorithm(m, r, \epsilon, \tilde{f}_{S_i,x}, c')$，其中 $\tilde{f}_{S_i,x}$ 是 $\tilde{f}$ 在满足以下条件的点上的限制：其坐标索引属于 S_i，且取值为 x 所指定的值。 4. 对每个 $x \in \{0,1\}^m$，令 $\widehat{f}(x)$ 为 $f^{(i,x_{S_i})}(x)$ 在 $1 \leq i \leq m'$ 上的众数，其中 x_{S_i} 是 x 中索引属于 S_i 的子串。 5. 令 ℓ 为 $RM(m, r)$ 中所有满足与 ˆ f 至多在 $2^{m-\sqrt{m}\log_2(m)/2}$ 个元素上不一致的元素所组成的列表。˜ 6. 返回 ℓ 中与 f 在最多元素上相同的元素。

—

我们声称 该算法以极高的概率恢复该码，具体而言 .

定理 3。 设 $\epsilon \in (0, 1/2)$，且 m_1、m_2、.....以及 r_1、r_2、.....是满足 $\lim_{i\to\infty} m_i = \infty$ 且 $\limsup_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i} < 1 - H(\epsilon)$ 的正整数序列。存在 c、c'、$c'' > 0$，使得在 ˜趋于无穷的极限下，当 $i \to \infty$ 时，若 f 从 $RM(m, r)$ 中随机抽取，且 f 是 f 的含噪版本，其中每个 ˜比特都以概率 ϵ 独立翻转，则 $RM\ reconstruction\ algorithm2(m_i, r_i, \bar{\epsilon}, f, c, c')$ 以概率 ˉ $1 - O(2^{-2^{c''\sqrt{m}}})$ 返回 f。

证明。首先，注意到对于足够小的 c，$\limsup_{i\to\infty} \binom{m_i - c\sqrt{m_i}}{\leq r} 2^{-m_i} < 1 - H(\epsilon)$ 也成立，并选取这样一个 c。运行此算法时，始终有 $c\sqrt{m} - c^2 - 1 \leq |S_j| \leq c\sqrt{m} + 1$，因此对于任意级数 $j_1, j_2, ...$，都有 $\limsup_{i\to\infty} \binom{m_i - |S_{j_i}|}{\leq r} 2^{-m_i} < 1 - H(\epsilon)$。现在，令 c' 为引理 8 声明存在的、对应于 (m'_1, r'_1), (m'_2, r'_2).....的常数，其中列出了所有可能的 i 和 j 取值对应的 $(m_i - |S_j|, r_i)$ 值。

接下来，对于每个 $1 \leq j \leq m'$ 和 $x \in \{0,1\}^{S_j}$，令 $B_{j,x}$ 为指示变量：如果 $f^{(j,x)}$ 等于 f 的适当限制，则其值为 0；否则为 1。根据前述定理，对于 j 和 x 的任意选择，$\mathrm{P}[B_{j,x} = 1] = O(2^{-c'\sqrt{m}\log_2(m)/2})$。此外，$B_{j,0^{S_j}}$, ..., $B_{j,1^{S_j}}$ 是

对于任意 j 都相互独立，因为用于生成的 $RM\ reconstruction\ algorithm$ 迭代是在 f 限制于互不重叠的集合后运行的。因此，

$$\mathbb{P}\left[\sum_{x\in\{0,1\}^{S_j}} B_{j,x} \geq 2^{c\sqrt{m}/2}\right] \leq 2^{|S_j|\cdot c\sqrt{m}/2} 2^{\left(O(1)-c'\sqrt{m}\log_2(m)/2\right)2^{c\sqrt{m}/2}} = O(2^{-2^{c\sqrt{m}/2}}/m).$$

如果 $\sum_{x\in\{0,1\}^{S_j}} B_{j,\ x} < 2^{c\sqrt{m}/2}$ 对于所有 j
则

$$\begin{aligned}
&|\{x : \widehat{x} \neq f(x)\}| && (76)\\
&\leq \sum_{T\subseteq\{1,\ldots,m'\}:|T|\geq m'/2} \prod_{j\in T} 2^{c\sqrt{m}/2} \prod_{j\notin T} 2^{|S_j|} && (77)\\
&\leq \sum_{T\subseteq\{1,\ldots,m'\}:|T|\geq m'/2} 2^{|T|\cdot c\sqrt{m}/2} 2^{(m'-|T|)(c\sqrt{m}+1)} && (78)\\
&\leq \sum_{T\subseteq\{1,\ldots,m'\}:|T|\geq m'/2} 2^{(3/4)cm'\sqrt{m}+m'/2} && (79)\\
&\leq 2^{(3/4)cm'\sqrt{m}+3m'/2} && (80)\\
&\leq 2^{(3/4)m+(3/4)c\sqrt{m}+(3/2)(\sqrt{m}/c+1)} && (81)\\
&= o(2^{m-\sqrt{m}\log_2(m)}). && (82)
\end{aligned}$$

这进而意味着，对于所有 j 和 $RM\ reconstruction\ algorithm$2，$\sum_{\vec{x}\in\{0,1\}^{S_j}} B_{j,x} < 2^{c\sqrt{m/2}}$ $(m_i, r_i, \epsilon, \tilde{f}, c, c')$ 返回非 f 结果的概率为 $O(2^{-\sqrt[3]{n}})$。因此，该算法以 $1 - O(m'2^{-2^{c\sqrt{m}/2}}/m + 2^{-\sqrt[3]{n}})$ $= 1 - O(2^{-2^{c\sqrt{m}/2}})$ 的概率返回 f，如所需。

□

8 强逆定理

提升框架中唯一要求码的码率低于信道容量的部分，是用于确立一个非平凡基本情形的熵论证。因此，对于任何码率高于信道容量的码，都不可能以显著高于 $1/2$ 的准确率，从其他比特的含噪版本中恢复一个比特；否则，我们的论证将意味着，对于某些码率高于信道容量的码，我们可以以高概率恢复码字。对此论证最明显的应用只能排除以 $1/2 + \Omega(1)$的准确率恢复一个比特的能力，但更为仔细的应用可以对我们恢复比特时的准确率设定严格得多的界限。为了说明这一点，请考虑以下引理4的变体。

引理 10。设 $\epsilon \in (0, 1/2)$、$c > 0$ 以及 $m_1, m_2, m_3, \ldots$ 和 $r_1, r_2, \ldots$ 为正整数序列，使得 $\lim_{i\to\infty} m_i = \infty$ 且 $P_e(m_i, r_i, \epsilon) \leq 1/2 - 2^{-c\sqrt{m_i}/3}$ 对所有 i 都成立。此外，对每个 i，令 $m'_i = m_i + 2\lfloor c\sqrt{m_i}\rfloor$。则 $P_e(m'_i, r_i, \epsilon) = O(2^{-c\sqrt{m_i}/3})$。

证明。首先，令 $m_i = m_i - \lfloor c\sqrt{m_i}\rfloor$，对于每个 i 并考虑尝试使用以下增强算法从 f 确定 $f(0^{m_i})$ 的值：

1. 从 $\mathbb{F}_2^{m'_i}$, V 中随机选取一个 m_i 维子空间。

2. 独立于 f，从 $\mathbb{F}_2^{m_i}$ 中选取 m_i 维子空间 W_1、……、$W_{2^{m'_i+m_i-2m_i+1}}$，使得对于所有 j，$V \subseteq W_j$，且对于所有 $j' \neq j$，$W_j \cap W_{j'} = V$。

3. 对每个 j，在 f 到 W_j 的限制上运行 $L_{m_i,\ r_i,\ \epsilon}$，并返回最常见的输出。

根据引理 1，可以找到这样一组 $\mathbb{F}_2^{m'_i}$ 的子空间，因此该算法可以执行。此外，若令 z' 为 Z 在 V 上的限制，那么在 z' 取定值的条件下，算法最后一步中的每次 L 都会独立地返回一个与 $f(0^{m'_i})$ 不同的值，其概率为 $P_e(m_i,\ m_i,\ r_i,\ \epsilon|z')$。于是引理 3 推出

$$\mathbb{P}[P_e(m_i, m_i, r_i, \epsilon|z') \geq 1/2 - 2^{-c\sqrt{m_i}/3}/2] \leq \frac{2^{2-\lfloor c\sqrt{m_i}\rfloor}}{2^{-2c\sqrt{m_i}/3}}$$

对任意 i 均成立。在任意固定的 z' 取值且满足 $P_e(m_i,\ m_i,\ r_i,\ \epsilon|z') < 1/2 - 2^{-c\sqrt{m_i}/3}/2$ 的条件下，该算法给出错误答案的概率至多为 $(4(1/2 - 2^{-c\sqrt{m_i}/3}/2)(1/2 + 2^{-c\sqrt{m_i}/3}/2))^{2^{m'_i+m_1-2m_i}}$，因此它返回与 $f(0^{m'_i})$ 不同值的总体概率至多为 $2^{2+2c\sqrt{m_i}/3-\lfloor c\sqrt{m_i}\rfloor} + (1 - 2^{-2c\sqrt{m_i}/3})^{2^{\lfloor c\sqrt{m_i}\rfloor}} = O(2^{-c\sqrt{m_i}/3})$。此外，该算法从不使用 $\tilde{f}(0^{m'_i})$ 的值，并且计算 $f(0^m)$ 的准确度至少不低于任何其他忽略 $\tilde{f}(0^m)$ 值的算法，因此它的错误率也为 $O(2^{-c\sqrt{m_i}/3})$，符合要求。

□

此时，我们可以使用之前的增强论证来证明，对于任意 c' 如果 $P_e(m'i,\ r_i,\ \epsilon) = O(2^{-c\sqrt{m_i}/3})$，那么我们可以从 $RM(m_i + c'\sqrt{m_i},\ r_i)$ 中恢复出一个码字，其概率为 $1 - o(1)$，其中其每个比特均以概率 ϵ 被翻转。更正式地，我们可以证明以下引理8 和定理 2。

引理 11。设 $\epsilon \in (0, 1/2)$、$c > 0$ 和 $m_1, m_2, m_3, \ldots$ 以及 $r_1, r_2, \ldots$ 为正整数序列，使得 $\lim_{i\to\infty} m_i = \infty$ 且 $P_e(m_i, r_i, \epsilon) \leq 1/2 - 2^{-c\sqrt{m_i}/3}$ 对所有 i 均成立。则存在 $c' > 0$，使得 $P_e(m_i + 3\lfloor c\sqrt{m_i}\rfloor, r_i, \epsilon) = O(m_i^{-c'\sqrt{m_i}})$。

证明。根据前一个引理，我们知道 $P_e(m_i + 2\lfloor c\sqrt{m_i}\rfloor, r_e, \epsilon) = O(2^{-c\sqrt{m_i}/3})$。这意味着存在 i_0，使得对于所有 $i \geq i_0$, $m_i \geq 2$ 和

$$P_e(m_i + 2\lfloor c\sqrt{m_i}\rfloor, r_i, \epsilon) \leq \min(e^{-108\ln(64/\epsilon(1-\epsilon))\sqrt[4]{m_i}}, 2^{-2\log_2^2(m_i)}/54^4).$$

Th对任意 $i \geq i_0$ 和 $m'' \geq m_i + 2\lfloor c\sqrt{m_i}\rfloor$，根据引理 7，必然 t

$$P_e(m'' + 2\lceil \log_2 m_i\rceil, r_i, \epsilon) \tag{83}$$

$$\leq 18P_e^{5/4}(m'',\ r_i,\ \epsilon) + 9P_e(m'',\ r_i,\ \epsilon)\left(\frac{4\log(64/\epsilon(1-\epsilon))}{\log(1/P_e(m'', r_i, \epsilon))}\right)^{\log_2(m_i)} + (8/9)^{m_i} \tag{84}$$

$$\leq 2^{-\log_2^2(m_i)/2}P_e(m'', r_i, \epsilon)/3 + m_i^{-\log_2(m_i)/4}P_e(m'', r_i, \epsilon)/3 + (8/9)^{m_i} \tag{85}$$

$$\leq \max(2^{-\log_2^2(m_i)/4}P_e(m'', r_i, \epsilon), 3(8/9)^{m_i}). \tag{86}$$

反复应用这一结论意味着，对于所有 $i \geq i_1$,

$$P_e(m_i + 3\lfloor c\sqrt{m_i}\rfloor, r_i, \epsilon) \leq \max\left(2^{-c\log_2(m_i)\sqrt{m_i}/16}, 3(8/9)^{m_i}\right).$$

这就得到了关于 $c' = c/16$ 的所需结论。

□

引理 *12.* 设 $\epsilon \in (0, 1/2)$，$c > 0$，和 $m_1, m_2, \ldots$ 以及 $r_1, r_2, \ldots$ 为正整数序列，满足 $\lim_{i\to\infty} m_i = \infty$，$|r_i - m_i/2| = O(\sqrt{m_i})$，且对所有 i，$P_e(m_i, r_i, \epsilon) \leq 1/2 - 2^{-c\sqrt{m_i}/3}$。再设 c' 为前一个引理所述存在的常数。那么，当 $i \to \infty$ 趋于极限时，若从 $RM(m + 3\lfloor c\sqrt{m}\rfloor, r)$ 中随机抽取 f，并且 f 是 f 的含噪版本，其中每个比特都以概率 ϵ 独立地以翻转，则 RM *reconstruction algorithm* $(m_i+3\lfloor c\sqrt{m_i}\rfloor, r_i, \epsilon, f, c')$ 以 $1 - O(2^{-c'\sqrt{m}} \log_2(m)/2)$ 的概率返回 f。

证明。首先注意，根据前一个引理以及不同 x 取值之间的对称性，对于所有 x，$\mathbf{P}[f(x) \neq f(x)] = O(m_i^{-c'\sqrt{m_i}})$。因此，$f \in \ell$ 的概率为 $1 - O(2^{-c'\sqrt{m_i}} \log_2(m_i)/2)$，在这种情况下，$\ell$ 中的每个元素与 f 的差异至多涉及 $2^{m_i - c'\sqrt{m_i}} \log_2(m_i)/2$ 个元素。根据引理 9，ℓ 中存在一个元素与 f 一致的元素个数至少与 f 一样多，且上述情况发生的概率为 $1 - O(2^{-\sqrt[3]{n}})$。因此，该算法以概率 $1 - O(2^{-c'\sqrt{m}} \log_2(m)/2)$ 恢复 f，如所求。 □

给定任意序列 m_i 和 r_i，满足 $|r_i - m_i/2| = O(\sqrt{m_i})$ 且 $RM(m_i, r_i)$ 的码率低于信道容量，则存在 $c > 0$，使得 $RM(m_i + c\sqrt{m_i}, r_i)$ 的码率也低于信道容量。因此，无法恢复从 $RM(m_i + c\sqrt{m_i}, r_i)$ 中抽取的码字这一事实意味着，对于除有限多个 i 之外的所有情形，$P_e(m_i, r_i, \epsilon) > 1/2 - 2^{-c\sqrt{m_i}/9}$。此外，$P_e(m, r, \epsilon)$ 关于 r 单调不减，这意味着对于任意满足 $RM(m_i, r_i)$ 的码率低于信道容量的序列 m_i 和 r_i，$P_e(m_i, r_i, \epsilon) = 1/2 - 2^{-\Omega(\sqrt{m_i})}$。

此外，请注意，虽然这是一个关于我们根据除 $f(x)$之外的 f的值来确定 $f(x)$的值时准确性的界，但我们可以将任何一个在给定 f的所有值时寻找 $f(x)$的算法转换为一个忽略 $f(x)$的算法，方法是仅将 $f(x)$的值在其输入中随机设定。因此，对于任何试图在给定 f的情况下计算 $f(0^m)$的算法 $L^\star$，如果 RM 码的码率高于信道容量，则有

$$\mathbb{P}[L^\star(\tilde{f}) = f(0^m)] \leq 1 - \epsilon + O(2^{-c\sqrt{m}}) - \Omega(\mathbb{P}[L^\star(\tilde{f}) \neq \tilde{f}(0^m)])$$

对于某个常数 $c > 0$。换言之，给定 f 的全部内容，我们无法以显著高于 $1 - \epsilon$的准确度确定 $f(x)$的值，而达到高的准确度的唯一方式，基本上总是假设 $f(x)$是 $f(x)$。因此，不存在一种算法能够恢复 $f(x)$，其效果显著优于取 $f(x)$的值。

9 推广至 BMS 信道

现在，考虑这样一种情况：不是以某个固定概率 ϵ翻转每个比特 X，而是对于每个比特，$\epsilon \in [0, 1/2]$ 我们的信道根据某个概率分布生成 $Z \in \mathbf{F}_2$，使其以概率 ϵ 为 1，否则为 0，然后输出 $(\epsilon_u, X_u + Z_u)$。我们声称，我们的结果可以推广为这样一个结论：对于任何此类信道，如果 $\limsup_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i}$ 严格小于信道容量，那么经过该信道传输后，我们能够以概率 $1 - o(1)$恢复 $RM(m, r)$ 中的码字。

为了证明这一点，我们首先注意到，对于任意正整数 k，如果在从信道接收到 ϵ 后将其舍入到最接近的 $1/k$ 倍数，就会得到一个容量相同或更低的新信道。然而，当 $k \to \infty$ 趋于极限时，该信道的容量趋于原信道的容量，因此对于足够大的 k，该信道的容量仍大于上极限 $\limsup_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i}$。所以，我们可以选择这样的 k，将信道输出的所有 ϵ 舍入到最接近的 $1/k$ 倍数，然后用舍入到这些倍数的 epsilon 的平均值替换这些 epsilon。因此，我们可以假设 ϵ 只有有限个可能取值。

将 BMS信道称为 $\mathcal{P}$，并将 $P_e(m,r,\mathcal{P})$ 定义为 $P_e(m,r,\epsilon)$ 的适当类比，即，在给定所有 ϵ 以及 $f(x)$的值的情况下，我们能够正确确定 $f(0^m)$ 的值的~概率。对于 BMS信道，基本情形成立，其核心思想与之前相同：通过寻找一组在 V处相交的子空间W_i，分别在每个子空间上运行恢复算法，并得出结论：目标比特的值就是其译码结果中占多数的值，从而逐步对我们能够达到的逐位错误率设置越来越紧的界。然而，现在算法能否利用某个子空间正确恢复目标比特，取决于该子空间上 ϵ 和 Z 的值，而不仅仅取决于 Z 的值。这使得使用傅里叶变换来界定错误向量在 V 上的限制是不良的概率这一论证变得更加复杂。

为了更精确地说明，设 k 为比特 $f(x)$的可能有序对(ϵ_x, Z_x)的数量。为了定义傅里叶变换的适当基，我们需要 k 个从有序对空间(ϵ_x, Z_x)到R的标准正交函数，$\mathcal{X}^{(0)}$,...,$\mathcal{X}^{(k-1)}$。此外，我们希望 $\mathcal{X}^{(0)}$是常数函数1，以便我们可以有独立于大多数输入的项。这允许我们为所有不相交的 $S_1,\ldots,S_{k-1}\subseteq\{0,1\}^m$ 定义$\mathcal{X}_{(S_1,\ldots,S_{k-1})}$，使得对于每个$(\epsilon,Z)$,

$$\mathcal{X}_{(S_1,\ldots,S_{k-1})}(\epsilon,Z)=\prod_{i=1}^{k-1}\prod_{x\in S_i}\mathcal{X}^{(i)}(\epsilon_x,Z_x)$$

$\mathcal{X}^{(i)}$ 的标准正交性意味着这些也是标准正交的，并且有k^m 个，因此它们构成了以(ϵ,Z)形式输入并返回实数的函数的标准正交基。在这种情况下，$Q_{m,m}$ 在线性变换下仍然是对称的，因此如果π 是这样的变换，则$\langle Q_{m,m},\mathcal{X}_{(S_1,\ldots,S_{k-1})}\rangle=\langle Q_{m,m},\mathcal{X}_{(\pi(S_1)\ldots,\pi(S_{k-1}))}\rangle$ 对于所有 $S_1,\ldots,S_{k-1}$。 $\mathcal{X}^{(i)}$ 正交这一事实意味着对于所有 $i\neq 0$,

$$\begin{aligned}
&E_{(\epsilon,Z)}[\mathcal{X}^{(i)}(\epsilon,Z)] && (87)\\
&=E_{(\epsilon,Z)}[\langle\mathcal{X}^{(0)}(\epsilon,Z),\mathcal{X}^{(i)}(\epsilon,Z)\rangle] && (88)\\
&=\langle\mathcal{X}^{(0)},\mathcal{X}^{(i)}\rangle && (89)\\
&=0 && (90)
\end{aligned}$$

因此，情况仍然是

$$Q_{\underline{m},m}=\sum_{S_1,..,S_{k-1}\subseteq\mathbb{F}_2^m:S_i\cap S_j=\emptyset}\langle Q_{m,m},\mathcal{X}_{(e_m(S_1),\ldots,e_m(S_{k-1}))}\rangle\mathcal{X}_{(S_1,\ldots,S_{k-1})}$$

因为所有其他项对 $Q_{m,m}$ 的贡献会相互抵消。类似地，对于给定的 $S_1,\ldots,S_{k-1}\subseteq\mathrm{F}_2^m$ 和一个随机线性变换 π，对于所有 i，$\pi(S_i)$ 属于 F_2^m 的概率至多为 $2^{-(m-m)\dim(\cup_i S_i)}$。对之前的记号稍作修改，~~令 $(S_1,\ldots,S_{k-1})$~~ 为所有形如 $(\pi(S_1)\ldots,\pi(S_{k-1}))$ 的元组构成的集合，其中线性变换为 π；令 S 为一个极大列表，其中包含在该线性变换下不等价的 F_2^m 子集的 $(k-1)$ 元组。我们仍设 $\mathcal{X}_{(S_1,\ldots,S_{k-1})}=\sum_{(S'_1,\ldots,S'_{k-1})\in(S_1,\ldots,S_{k-1})}\mathcal{X}_{(S'_1,\ldots,S'_{k-1})}$。我们关于 $\lim_{i\to\infty}P_e(m_i,r_i,\mathcal{P})=O(2^{-\sqrt[3]{m_i}})$ 的证明与之前基本相同。不过，支撑用于界定 $\mathcal{X}_{(S_1,\ldots,S_{k-1})}$ 四次幂期望的引理的计算细节需要作如下更新。

引理 13.令 m 为正整数，且 S_1、...、S_{k-1} 为$\mathbb{F}_2^m$ 的不相交子集。此外，选取一个*BMS*信道 $\mathcal{P}$，其 ϵ 具有有限多个可能值，并选取适当的函数 $\mathcal{X}_{(i)}$，以及 $B=$最大值$_{i,\ \epsilon,\ z}|\mathcal{X}_{(i)}(\epsilon、\ z)|$。则 $\langle\mathcal{X}^4_{(S_1,\ \ldots,\ S_{k-1})}\rangle\leq 2^{2dm+8d^2}B^{2^{d+2}}$，其中 $d=$维数$(\cup_i S_i)$。

证明. 首先，观察到

$$\langle \mathcal{X}_{\overline{S}}^4 \rangle = \sum_{(S_1^{(1)},\ldots,S_{k-1}^{(1)}),\ldots,(S_1^{(4)},\ldots,S_{k-1}^{(4)}) \in \overline{S}} \langle \mathcal{X}_{(S_1^{(1)},\ldots,S_{k-1}^{(1)})} \cdot \mathcal{X}_{(S_1^{(2)},\ldots,S_{k-1}^{(2)})} \cdot \mathcal{X}_{(S_1^{(3)},\ldots,S_{k-1}^{(3)})} \cdot \mathcal{X}_{(S_1^{(4)},\ldots,S_{k-1}^{(4)})} \rangle$$

如果存在任何一个恰好属于其中一个 $S_j^{(i)}$ 的 x，那么$\langle \mathcal{X}_{(S_1^{(1)},\ldots,S_{k-1}^{(1)})} \cdot \mathcal{X}_{(S_1^{(2)},\ldots,S_{k-1}^{(2)})} \cdot \mathcal{X}_{(S_1^{(3)},\ldots,S_{k-1}^{(3)})} \cdot \mathcal{X}_{(S_1^{(4)},\ldots,S_{k-1}^{(4)})} \rangle = 0$，因为对在 x 上取不同值的 z 和 ϵ 的选择所作出的贡献彼此抵消。如果不存在这样的 x，那么 $\langle \mathcal{X}_{(S_1^{(1)},\ldots,S_{k-1}^{(1)})} \cdot \mathcal{X}_{(S_1^{(2)},\ldots,S_{k-1}^{(2)})} \cdot \mathcal{X}_{(S_1^{(3)},\ldots,S_{k-1}^{(3)})} \cdot \mathcal{X}_{(S_1^{(4)},\ldots,S_{k-1}^{(4)})} \rangle \leq B^4 \sum_i |S_i| \leq B^{2^{d+2}}$。此外，$\cup_i$、$_j S_j^{(i)}$ 必须包含维数($\cup_{i,j} S_j^{(i)}$)个线性无关的点。如果不存在恰好属于这些集合中的一个集合的 x，那么这些点中的每一个都必须至少属于具有 i 不同取值的两个 $S_j^{(i)}$，这意味着 $d \geq$ 维数($\cup_{i,j} S_j^{(i)}$)/2。$\mathbb{F}_2^m$中至多有 $2^{2dm}2d$维的子空间，并且任意这样的子空间中至多包含 2^{2d^2} 个关于(S_1, ..., S_{k-1})的线性变换。因此 $\langle \mathcal{X}_S^4 \rangle \leq 2^{2dm+8d^2} B^{2^{d+2}}$，如所需。 □

这一变化与以下事实相结合：对于满足dim($\cup_i S_i$) $= d$的元组(S_1,..., S_{k-1})，等价类数量的显然上界是 k^{2^d}而不是 2^{2^d}，因此我们对 $\mathbb{P}[P_e(m, m, r, \mathcal{P}|z') \geq 1/3]$得到的界从 $18P_e^{5/4}(m, r, \mathcal{P}) + 9P_e($ $m, r, \mathcal{P})$ Ä^{4}log(64/ϵ(1−ϵ))log($1/P_e(m,r,\mathcal{P})$)ä$^{m-m}$变为$18P_e^{5/4}(m, r, \mathcal{P}) + 9P_e(m, r, \mathcal{P})$ Ä^{c}log($1/P_e(m,r,\mathcal{P})$)ä$^{m-m}$，其中某个其他常数 c取决于这些参数。然而，对于足够不利的ϵ，这从不会比我们得到的界更宽松，因此，利用该界证明：如果上极限$_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i}$严格小于信道容量，那么存在 $c' > 0$使得 $P_e(m_i, r_i, \mathcal{P}) = O(m_i^{-c'\sqrt{m_i}})$ 的论证基本保持不变。

最后，我们需要处理论证中的这一部分：如何从能够以 $1 - O(m_i^{-c'\sqrt{m_i}})$ 的准确率恢复每个比特，转变为能够以较高的成功概率完整恢复码字。这一部分几乎可以原封不动地保留。有人可能会认为，在决定返回 ℓ 中的哪个元素时，应当考虑 ϵ 的取值；但基本上，忽略它们只是将信道简化为噪声为 $\mathbb{E}[\epsilon]$ 的二元对称信道。论证中证明：在距离 $2^{m-c\sqrt{m}\log_2(m)/2}$ 以内，不太可能存在某个码字，它与~真实码字相比，在更多位置上与 f 相符。这一部分对任意$\epsilon \in (0, 1/2)$ 都成立，因此足以证明该算法以概率 $1 - 2^{-\Omega(\sqrt{m}\log(m))}$ 返回真实码字。进一步收紧错误概率界限的部分，只是将我们以概率 $1 - 2^{-\Omega(\sqrt{m}\log(m))}$ 恢复码字的能力，以及以概率 $1 - O(2^{-\sqrt[3]{n}})$ 将基本准确的译码转变为完全准确的译码的能力，作为黑箱来使用，因此无需改动。综合以上内容，可得如下定理：

定理 4. 设 $\mathcal{P}$ 是 *BMS* 信道，且 m_1、m_2、... 和 r_1、r_2、... 是正整数序列，使得 $\lim_{i\to\infty} m_i = \infty$ 和 $\limsup_{i\to\infty} \binom{m_i}{\leq r_i} 2^{-m_i}$ 严格小于 $\mathcal{P}$ 的容量。存在 c、c'、$c'' > 0$ 以及一个算法 $RM\ reconstruction\ algorithm^\star$，使得当 $i \to \infty$ 趋于无穷时，若 ~f 是从 $RM(m_i, r_i)$ 和 $f = \mathcal{P}(f)$ 中随机抽取的，则 $RM\ reconstruction\ algorithm^\star(m_i, r_i, \mathcal{P}, f, c, c')$ 以概率 $1 - O(2^{-2^{c''}\sqrt{m}})$ 返回 f。

逆命题本质上使用了相同的增强论证，即采用反证法排除以下可能性：当码率大于信道容量时，仅根据其他比特的含噪版本，以非平凡的准确度确定 $f(x)$的值。逆命题使用了引理 4的一个变体，以证明我们可以从 $P_e(m, r, \epsilon) = 1/2 - 2^{-c\sqrt{m}}$开始增强，而不必从 $P_e(m, r, \epsilon) = 1/2 -$ $\Omega(1)$ 开始；然而，引理的两个版本都只使用了引理

3 作为其关于将 Z 限制到 V 的概率信息来源。如果将逆定理调整为一般BMS信道，即如果该码的码率超过信道的容量，那么$P_e(m_i, r_i, \epsilon) \geq 1/2 - 2^{-c\sqrt{m_i}}$ 对于某个常数 c 成立，则无需进行任何并非在将原始论证调整到一般BMS信道时已经必需的改动。

更确切地说，要将逆定理部分推广到一般的 BMS 信道，我们可以修改如下论证：我们可以假设 ϵ 只有有限多个可能取值。具体而言，我们可以用一个新信道替代实际的 BMS 信道，其中每个可能的 ϵ 值都替换为 $\lfloor k\epsilon \rfloor / k$，并指出，由于原信道等价于添加了更多噪声后的新信道，因此我们至少应能在新信道上同样准确地恢复码字。我们需要将所有 $P_e(m, r, \epsilon)$ 替换为 $P_e(m, r, \mathcal{P})$，将前面各节中所有用到引理的地方替换为相应的推广版本，将引理 11 的证明中的 $4\log(64/\epsilon(1-\epsilon))$ 项替换为引理 7 的推广版本所得到的结果，并将 $e^{-108\ln(64/\epsilon(1-\epsilon))\sqrt[4]{m_i}}$ 项替换为必要的表达式，以确保含有 $4\log(64/\epsilon(1-\epsilon))$ 项的分数仍小于 $\sqrt[4]{m_i}/27$。观察到，˜只要在输入中随机设定 $f(x)$ 的值，我们就能把一个在已知全部 f 的情况下恢复 $f(x)$ 的算法，转换为一个忽略 $f(x)$ 的˜˜值的算法；这一观察可以推广为：˜只要在输入中随机设定 $f(x)$ 的值，并任意设定 ϵ_x 的值˜，我们就能把一个在已知全部 f 和 ϵ 的情况下恢复 $f(x)$ 的算法，转换为一个忽略 $f(x)$ 的˜˜值的算法。这意味着，对于任何试图在已知 f 和 ϵ 以及 ϵ_x 的任意可能取值时计算 $f(0^m)$ 的算法 $L^\star$， ϵ'，

$$\mathbb{P}[L^\star(\tilde{f}, \epsilon) = f(0^m) | \epsilon_{0^m} = \epsilon'] \leq 1 - \epsilon' + O(2^{-c\sqrt{m}}) - \Omega(\mathbb{P}[L^\star(\tilde{f}) \neq \tilde{f}(0^m) | \epsilon_{0^m} = \epsilon'])$$

˜对于某个常数 $c > 0$。换句话说，即使给定 f 和 ϵ 的全部信息，我们也无法以显著高于 $1 - \epsilon_x$的准确度确定 $f(x)$ 的值；而要达到如此高的准确度˜，唯一的办法就是大多数时候猜测 $f(x)$ 是 $f(x)$，除非 $\epsilon_x = 1/2$。

参考文献

[3gp] 3GPPTSG RANWG1 #87最终报告 v1.0.0。12[Abb18] Emmanuel Abbe。社群检测与随机块模型。Foundations and Trends in Communicationsand InformationTheory，14(1-2):1–162，2018。 12[AHN21] Emmanuel Abbe、JanHazla和IdoNachum。近乎Reed–Muller码在随机错误下实现恒定码率。IEEE信息论汇刊，67(12):8034–8050，2021年。 4，5[AKK+05] Noga Alon、Tali Kaufman、Michael Krivelevich、Simon Litsyn和Dana Ron。Reed–Muller码测试。IEEE Trans. Inf.Theory，51(11):4032–4039，2005。4[ALM+98] S. Arora、C. Lund、R. Motwani、M.Sudan和M. Szegedy。证明验证与近似问题的近似困难性。ACM学报（JACM），45(3):501–555，1998。 4[Ari08] E. Arikan。极化码与Reed-Muller 码的性能比较。IEEE通信快报，12(6):447–449，2008年6月。4[Arı09] E.Arıkan。信道极化：一种为对称二元输入无记忆信道构造容量达成码的方法。IEEE信息论汇刊，55(7):3051–3073，2009。 4，5

[Ari10] E.Arikan。关于从极化编码视角看Reed-Muller码的综述。载于2010年IEEE信息论研讨会（信息论研讨会（ITW2010），开罗），第1–5页。IEEE，2010年。4[ASSY23] Emmanuel Abbe、Ori Sberlo、AmirShpilka和Min Ye。Reed-Muller码。《通信与信息论基础与趋势》，20(12):1–156，2023年。4、6、12[ASW15a] E.Abbe、A. Shpilka和A. Wigderson。随机擦除和错误下的Reed–Muller码。《IEEE信息论汇刊》，61(10):5229–5252，2015年。4、5[ASW15b] EmmanuelAbbe、Amir Shpilka和AviWigderson。随机擦除和错误下的Reed-Muller码。载于第四十七届ACM计算理论研讨会论文集，STOC ’15，第297–306页，纽约，纽约州，美国，2015年。计算机协会。4、5、7[ASY21] Emmanuel Abbe、Amir Shpilka和MinYe。Reed–Muller码：理论与算法。《IEEE信息论汇刊》，67(6):3251–3277，2021年。4、6[AT09] E. Arıkan和E. Telatar。关于信道极化的码率。载于2009年IEEE国际信息论研讨会，第1493–1495页。IEEE，2009年。4[AY19] E. Abbe和M.Ye。Reed-Muller码实现极化。载于2019年IEEE第60届计算机科学基础年度研讨会（FOCS），第273–286页。IEEE，2019年。4、5[BDBD22] A. Blokhuis、M. DeBoeck和J. D’haeseleer。关于两两交于一点的k-空间的向日葵界。《设计、编码与密码学》，90(9):2101–2111，2022年9月。9、14[BF90] D. Beaver和J.Feigenbaum。在多预言机查询中隐藏实例。载于STACS90，第37–48页。Springer，1990年。4[BFL90] L. Babai、L.Fortnow和C. Lund。非确定性指数时间具有双证明者交互协议。载于《计算机科学基础》，1990年论文集，第31届年度研讨会，第16–25页。IEEE，1990年。4[BGH+12] B. Barak、P. Gopalan、J.Hastad、R.Meka、P.Raghavendra和D. Steurer。让长码变得更短。载于第53届IEEE计算机科学基础年度研讨会，FOCS 2012，新不伦瑞克，新泽西州，美国，2012年10月20–23日，第370–379页，2012年。4[BGN+22] Jaros ̷law B ̷lasiok、Venkatesan Guruswami、PreetumNakkiran、AtriRudra和MadhuSudan。一般强极化。《《ACM学报》》，69(2)，2022年3月。12[BHSS22] Siddharth Bhandari、Prahladh Harsha、RamprasadSaptharishi和Srikanth Srini- ̈vasan。随机集合的消失空间及其在Reed-Muller码中的应用。载于Shachar Lovett（编），第37届计算复杂性会议，CCC2022，2022年7月20–23日，费城，宾夕法尼亚州，美国，LIPIcs第234卷，第31:1–31:14页。Schloss Dagstuhl - Leibniz-Zentrumf ̈ur Informatik，2022年。4[BIK05] AmosBeimel、YuvalIshai和EyalKushilevitz。信息论私人信息检索的一般构造。《计算机与系统科学杂志》，71(2):213–247，2005年。4

[BIKR02] AmosBeimel、Yuval Ishai、Eyal Kushilevitz 和 Jean-Fran˛cois Raymond。突破信息论私人信息检索的 $o(n^{1/(2k-1)})$ 障碍。载于第43届计算机科学基础研讨会（FOCS2002），2002年11月16日至19日，加拿大不列颠哥伦比亚省温哥华，论文集，第261–270页。IEEE计算机学会，2002年。4[BK97] J.Bourgain和 G. Kalai。群对称性下变量的影响与阈值区间。《几何与泛函分析》，7(3):438–461，1997年。5, 7[BKS+10a] A. Bhattacharyya、S. Kopparty、G. Schoenebeck、M. Sudan 和D.Zuckerman。Reed-Muller 码的最优测试。载于《2010年IEEE第51届计算机科学基础年度研讨会》论文集，FOCS '10，第488–497页，2010年。4[BKS+10b] Arnab Bhattacharyya、Swastik Kopparty、Grant Schoenebeck、Madhu Sudan和David Zuckerman。Reed-Muller 码的最优测试。载于IEEE第51届计算机科学基础年度研讨会，FOCS2010，2010年10月23日至26日，美国内华达州拉斯维加斯，第488–497页。IEEE计算机学会，2010年。4[BMW15] Alexander Barg、AryaMazumdar 和 RongrongWang。随机子字典的受限等距性质。IEEE信息论汇刊，61(8):4440–4450，2015年。4[BV10] A. Bogdanov 和 E. Viola。多项式的伪随机比特。SIAM《计算学报》，39(6):2464–2486，2010年。4[CF07] D.J.Costello 和 G. D. Forney。信道编码：通往信道容量之路。《IEEE会刊》，95(6):1150–1177，2007年。4[CG05] C.Carlet 和P.Gaborit。关于构造具有良好代数免疫度的平衡布尔函数。载于《国际信息论研讨会》论文集，2005年。ISIT 2005，第1101–1105页。IEEE，2005年。4[CHJ10] Robert Calderbank、Stephen Howard 和Sina Jafarpour。构造一大类满足统计等距性质的确定性测量矩阵。《IEEE信号处理精选主题期刊》，4(2):358–374，2010年。4[CJ10] Robert Calderbank和 SinaJafarpour。Reed–Muller测量矩阵与 LASSO。载于序列及其应用国际会议，第442–463页。Springer，2010年。4[CK11] ImreCsiszar和 Janos Korner。《信息论：离散无记忆系统的编码定理》。剑桥大学出版社，第2版，2011年。6[CKGS98] Benny Chor、Eyal Kushilevitz、Oded Goldreich和 Madhu Sudan。私人信息检索。《ACM学报》，45(6):965–981，1998年。4[CT12] T.M. Cover和J.A. Thomas。《信息论基础》。Wiley，2012年。6[DF81] MichelDeza 和 PeterFrankl。每个大型等距 $(0, +1, -1)$ 向量集都构成一个向日葵。《组合数学》，1:225–231，1981年09月。9, 14[DF93] I.Dumer 和P. Farrell。线性分组码的擦除纠正性能。载于代数编码研讨会，第316–326页。Springer，1993年。4

[DG16] Zeev Dvir和Sivakanth Gopi。次多项式通信的双服务器私人信息检索。《ACM学报》，63(4):39:1–39:15，2016年。4[DS06] I. Dumer和K. Shabunov。一般Reed-Muller码的递归纠错。《离散应用数学》，154(2):253–269，2006年。编码与密码学。4，5[Dum04] I. Dumer。低码率Reed-Muller码的递归译码及其性能。《IEEE信息论汇刊》，50(5):811–823，2004年5月。4，5[Dum06] I. Dumer。Reed-Muller码的软判决译码：一种简化算法。《IEEE信息论汇刊》，52(3):954–963，2006年3月。4，5[FFHM21] Dorsa Fathollahi、Nariman Farsad、Seyyed Ali Hashemi和Marco Mondelli。Reed-Muller码的稀疏多译码器递归投影聚合。载于2021年IEEE国际信息论研讨会（ISIT），第1082–1087页。IEEE，2021年。4[FK96] E. Friedgut和G. Kalai。每个单调图性质都具有尖锐阈值。《美国数学会会刊》，124(10):2993–3002，1996年。5[Gal08] Robert G. Gallager。《数字通信原理》。剑桥大学出版社，2008年。6[Gas04] W. Gasarch。关于私人信息检索的综述。载于《EATCS通报》。Citeseer，2004年。4[GEE+21] Marvin Geiselhart、Ahmed Elkelesh、Moustafa Ebada、Sebastian Cammerer和Stephan ten Brink。Reed–Muller码的自同构集成译码。《IEEE通信汇刊》，69(10):6424–6438，2021年。4[GX15] Venkatesan Guruswami和Patrick Xia。极化码：极化速度与和容量的多项式间隙。《IEEE信息论汇刊》，61(1):3–16，2015年。12[Ham50] R. W. Hamming。检错码与纠错码。《贝尔系统技术期刊》，29(2):147–160，1950年。3[HAU14] S. H. Hassani、K. Alishahi和R. L. Urbanke。极化码的有限长度标度。《IEEE信息论汇刊》，60(10):5875–5898，2014年。12[HKL05] T. Helleseth、T. Klove和V. I. Levenshtein。二元线性码的纠错能力。《IEEE信息论汇刊》，51(4):1408–1423，2005年4月。4，5[HKO+18] H. Hassani、S. Kudekar、O. Ordentlich、Y. Polyanskiy和R. Urbanke。BEC和BSC信道上的Reed-Muller码的近最优标度。载于2018年IEEE国际信息论研讨会（ISIT），第311–315页。IEEE，2018年。12[HSS13] Elad Haramaty、Amir Shpilka和Madhu Sudan。小素数域上多元多项式的最优测试。《SIAM计算学报》，42(2):536–562，2013年。4

[HSS21] Jan Hazla、Alex Samorodnitsky 和 Ori Sberlo。关于在二元对称信道上译码恒定比例错误的码。载于 Samir Khuller 和 Virginia Vassilevska Williams 编，STOC '21：第53届 ACM SIGACT 计算理论年会，线上活动，意大利，2021年6月21日至25日，第1479–1488页。ACM，2021。4, 5[JPRZ09] Charanjit S. Jutla、Anindya C. Patthak、Atri Rudra 和 David Zuckerman。素数域上低次数多项式的测试。Random Struct. Algorithms，35(2):163–193，2009。4[KKM+16a] S. Kudekar、S. Kumar、M. Mondelli、H. D. Pfister、E. Sa¸so˘glu 和 R. Urbanke。Reed-Muller 码在擦除信道上达到容量。载于第四十八届 ACM 计算理论研讨会（STOC）论文集，第658–669页。ACM，2016年。4, 5, 6, 7, 15[KKM+16b] Shrinivas Kudekar、Santhosh Kumar、Marco Mondelli、Henry D Pfister 和 R¨udiger Urbanke。比较 Reed-Muller 码在 BMS 信道上的比特映射与块映射译码阈值。载于 2016 IEEE信息论国际研讨会（ISIT），第1755–1759页，2016年。4, 7, 11[KKM+17] S. Kudekar、S. Kumar、M. Mondelli、H. D. Pfister、E. Sa¸so˘glu 和 R. Urbanke。Reed–Muller码在擦除信道上达到容量。IEEE信息论汇刊，63(7):4298–4316，2017。4, 5[KLP12] T. Kaufman、S. Lovett 和 E. Porat。Reed–Muller码的重量分布与列表译码大小。IEEE信息论汇刊，58(5):2689–2696，2012年。4, 5[KR06] Tali Kaufman 和 Dana Ron。一般域上多项式的测试。SIAM J. Comput.，36(3):779–802，2006年。4[KT70] T. Kasami 和 N. Tokura。关于 Reed-Muller 码的重量结构。信息论，IEEE Transactions on，16(6):752–759，1970年11月。5[KTA76] T. Kasami、N. Tokura 和 S. Azumi。关于 Reed-Muller 码重量小于 2.5d 的重量枚举。信息与控制，30(4):380 – 395，1976。5[LHP20] Mengke Lian、Christian H¨ager 和 H. D. Pfister。使用冗余码约束译码 Reed–Muller 码。载于 2020年 IEEE信息论国际研讨会（ISIT），第42–47页。IEEE，2020年。4[Lin93] S. Lin。RM码并不那么差。载于 IEEE Inform. Theory Workshop，1993。邀请报告。4[Lov17] Shachar Lovett。《加法组合学及其在理论计算机科学中的应用》。研究生综述第8号。计算理论文库，2017。5[MHU14] M. Mondelli、S. H. Hassani 和 R. L. Urbanke。从极化码到 Reed-Muller 码：一种改善有限长度性能的技术。IEEE Transactions on Communi- cations，62(9):3084–3091，2014年。4, 12[Mul54] D. E. Muller。布尔代数在开关电路设计与错误检测中的应用。IRE电子计算机专业组汇刊，(3):6–12，1954。3

[Raz87] A. A. Razborov。带逻辑加法完备基上有界深度电路规模的下界。数学札记，41(4):333–338，1987。4[Ree54] I. Reed。一类多重错误纠正码及其译码方案。IRE 信息论专业组汇刊，4(4):38–49，1954。3[Ren18] Joseph M. Renes。信道与编码的对偶性。IEEE信息论汇刊，64(1):577–592，2018。8[RP21] G. Reeves 和 H. D. Pfister。Reed-Muller 码在 BMS 信道上达到容量。2021。arXiv:2110.14631。4, 6, 7, 8, 9, 10, 12, 17[Sam18] Alex Samorodnitsky。含噪函数 ℓ_q 范数的上界。CoRR，abs/1809.09696，2018。4, 5[Sam20] Alex Samorodnitsky。含噪函数 ℓ_q 范数的上界。IEEE信息论汇刊，66(2):742–748，2020年。4, 5[San12] Tom Sanders。关于 Bogolyubova-Ruzsa 引理。《分析与偏微分方程》，5(3):627 – 655，2012年。5[SB70] N. J. A. Sloane 和 E. Berlekamp。二阶 Reed-Muller 码的重量枚举式。信息论，IEEE Transactions on，16(6):745–751，1970年11月。5[SF12] Robert E. Schapire 和 Yoav Freund。《提升：基础与算法》。麻省理工学院出版社，2012年。12[Sha48] C. E. Shannon。通信的数学理论。《贝尔系统技术期刊》，27(3):379–423，1948。3[Sha79] A. Shamir。如何分享秘密。《ACM 通讯》，22(11):612–613，1979。4[Sha92] A. Shamir。IP= PSPACE。ACM学报（JACM），39(4):869–877，1992。4[SP92] V. M. Sidel’nikov 和 A. S. Pershakov。大量错误下 Reed-Muller 码的译码。《信息传输问题》，28(3):80–94，1992。5[SS96] M. Sipser 和 D. A. Spielman。扩展码。IEEE Trans. on Inform. Theory，42:1710–1722，1996年。3[SS20] O. Sberlo 和 A. Shpilka。关于 Reed-Muller 码对随机错误与擦除的性能。载于第十四届 ACM-SIAM 离散算法年度研讨会论文集，第1357–1376页。SIAM，2020年。4, 5, 7, 11, 23[SSV17] R. Saptharishi、A. Shpilka 和 B. L. Volk。从随机错误中高效译码 Reed–Muller 码。IEEE信息论汇刊，63(4):1954–1960，2017。4[TV06] Terence Tao 和 Van H. Vu。《加法组合学》。剑桥高等数学研究丛书。剑桥大学出版社，2006年。5[TV13] I. Tal 和 A. Vardy。如何构造极化码。IEEE信息论汇刊，59(10):6562–6582，2013年。12

[TZS06] Amnon Ta-Shma、David Zuckerman 和 Shmuel Safra。源自 Reed-Muller 码的提取器。*J. Comput. Syst. Sci.*，72(5)：786–812，2006年。4[Wil13] Mark M. Wilde。量子信息论。剑桥大学出版社，2013年。8[YA20] Min Ye 和 Emmanuel Abbe。Reed-Muller 码的递归投影聚合译码。*IEEE*信息论汇刊，66(8)：4948–4965，2020年。4，6，12[Yek12] S. Yekhanin。局部可译码。*Foundations and Trends*® 理论计算机科学，6(3)：139–255，2012年。4