多项式码列表译码的进展

Mrinal Kumar[1] 和 Noga Ron-Zewi[2]

[1]塔塔基础研究所技术与计算机科学学院，电子邮件：mrinal.kumar@tifr.res.in[2]海法大学计算机科学系。电子邮件：noga@cs.haifa.ac.il

arXiv:2603.03841v1 [cs.IT] 4 Mar 2026

摘要

纠错码是一种表示数据的方法，使得即使部分数据遭到破坏，也能恢复原始信息。这一基本思想可追溯至约一个世纪前香农和汉明的开创性工作：将数据编码为冗余形式，以便即使存在噪声或数据损坏，也能从冗余编码中译出原始信息。Reed-Solomon 码是一个重要的纠错码族，它通过对低次多项式求值来编码数据。在提出近六十年后，Reed-Solomon 码以及一些相关的基于多项式的码族，无论从理论角度还是从应用角度来看，至今仍受到广泛研究。

除了显而易见的通信用途外，Reed-Solomon 码等纠错码在理论计算机科学的各种应用中也很有用。这些应用往往要求能够应对大量错误，远超信息论所允许的范围。列表可译码码是一类特殊的纠错码，通过允许生成一个较小的候选译码列表，实现对传统方法无法纠正的更多错误进行纠正。事实证明，这些码在理论计算机科学和编码理论的各种应用中极为有用。

近年来，里德-所罗门码及相关的基于多项式的码族在列表译码方面取得了重大进展。这包括对这些码进行高效列表译码，直至信息论容量，并具有最优列表大小，且采用快速的近线性时间乃至亚线性时间算法。本书综述了这些进展。

目录

1 引言 **3**

1.1 列表译码.3 1.2 编码理论中的多项式.4 1.3 多项式码的列表译码.5 1.4 本综述的组织与范围.6

2 符号与定义 **7**

2.1 列表可译码码.7 2.2 有限域上的多项式.9 2.3 若干多项式码族.12 2.4 文献注记.13

3 算法列表译 码至 Johnson界 1 **4**

3.1 Reed-Solomon 码的唯一译码.14 3.2 超出唯一译码半径的 Reed-Solomon 码列表译码.17 3.3 译码至 Johnson界的 Reed-Solomon 码列表译码.20 3.4 超出 Johnson界的 Reed-Solomon 码列表译码的局限性 23 3.5 文献注记.25

4 达到容量的算法列表译码 **25**

4.1 超越唯一译码半径的重数码列表译码.25 4.2 达到容量的重数码列表译码.30 4.3 基于子域求值点、达到容量的 Reed-Solomon 码列表译码 34 4.4 文献注记.38

5 组合上界 列表大小 3 的上界 **8**

5.1 基于随机求值点的 Reed-Solomon 码.39 5.2 重数码.45 5.3 基于子域求值点的 Reed-Solomon 码.50 5.4 文献注记.53

6 近线性时间列 表译码 5 **5**

6.1 Reed-Solomon 码的快速列表译码，达到 Johnson 界.55 6.2 重数码的快速列表译码，达到容量.62 6.3 文献注记.69

7 局部列表译码 **69**

7.1 Reed-Muller码的局部纠错.72 7.2 超出唯一译码半径的Reed-Muller码局部列表译码.73 7.3 直至Johnson界的Reed-Muller码局部列表译码.77 7.4 直至最小距离的多变量重数码局部列表译码.81 7.5 文献注记.83

8 结论与开放问题 **84**

1 引言

在存在错误或噪声的情况下稳健且高效地通信与存储数据这一问题，是数学与工程的交中一个根本性的重要问题。纠错码理论（或编码理论）是在香农 [Sha48]与汉明[Ham50] 于20世纪40至50年代的里程碑式工作中发展起来的，旨在形式化并理解这些问题。该理论的核心概念是纠错码 （或简称为码）。一个纠错码 C，其码长 为 n，定义在有限字母表 Σ上，是 Σ^n的一个子集。 C 中的字被称为码字，并且通常，我们还将字符串的集合 M（称为消息）与码 C 相关联，使得存在一个双射Φ （称为编码映射），从 M 到 C。

码的码率 C定义为 $R(C) := \log(|C|)\ n \log(|\Sigma|)$，用于衡量码中的冗余量。具体而言，为了在存在噪声的情况下使用码进行通信，如果我们想通过噪声信道传输一条消息 $m \in M$，我们的做法是将其编码为 $\Phi(m)$，然后通过信道发送 $\Phi(m)$。因此，码率衡量的是，使用该码可以编码多少种可能的消息，占所有可能的长度为 n 、取值于 Σ的字符串的比例。码的最小（汉明）距离 C定义为 $\Delta(C) := \min_{c \neq c' \in C} \Delta(c, c')$，其中 $\Delta(c, c')$ 称为c 与 c'之间的汉明距离，表示 c 和 c' 不同的位置数。码的最小距离衡量了其中任意两个不同码字之间的汉明距离有多大，因而也反映了该码可能具有的抗噪能力。具体而言，传输过程中信道可能会篡改 $\Phi(m)$中的某些位置，接收方可能会收到一个字符串 $w \in \Sigma^n$。然而，如果 w 与 $\Phi(m)$之间的差异少于 $\Delta(C)\ 2$ 个位置，那么译码器就可以通过在 C 中搜索与接收字 w距离最近的唯一一个码字，唯一地恢复 $\Phi(m)$（进而恢复 m）。

上述讨论还凸显了码的码率与距离之间固有的张力——较高的码率似乎必然导致较低的距离（因此容错能力也较弱）。理解码率与距离之间精确的权衡关系，至今仍是编码理论核心领域中的一个基本开放问题。特别是，20世纪60年代的经典*Singleton*界 指出，对于大小为 $|C| = \Sigma^k$ 的线性码 $C \subseteq \Sigma^n$，必须满足 $\Delta(C) \leq n - k + 1$。这尤其意味着，对于任意码 C，都有 $\delta(C) \leq 1 - R(C)$，其中 $\delta(C) := \frac{\Delta(C)}{n}$ 是 C的相对距离 。以等号满足 Singleton 界的码称为最大距离可分（MDS）码；如今，我们已知多种具有这一性质的码族。

上述在噪声存在时使用通信编码的框架，显然也凸显了编码理论中备受关注的计算问题，即如何显式构造具有非平凡码率和距离的码族，以及如何为这些码设计高效的编码和译码算法。此外，这些计算层面的问题对计算机科学也十分重要，因为纠错码与复杂性理论、密码学、伪随机性和算法设计等领域之间存在许多令人惊讶的联系与应用；而这些领域往往需要显式且可高效译码的码。

1.1 列表译码

如果码 C 的距离为 $\Delta(C)$，那么显然，对于任意字 $w \in \Sigma^n$，与其汉明距离小于 $\frac{\Delta(C)}{2}$ 的码字至多有一个。因此，$\frac{\Delta(C)}{2}$ 称为该码的唯一译码半径。Elias [Eli57] 和 Wozencraft [Woz57]的研究引入了列表译码这一概念，将这一错误界限放宽至 $\frac{\Delta(C)}{2}$ 之外。在这一距离下，与 w 最近的码字未必唯一，但我们仍希望这类码字组成的列表 规模较小。更正式地，对于 $\alpha > 0$ 和一个正整数

L，若码 $C \subseteq \Sigma^n$ 满足：对于每个 $w \in \Sigma^n$，至多存在 L 个不同的码字 $c \in C$，使得汉明距离 $\Delta(w,c)$ 不超过 αn，则称该码 $C \subseteq \Sigma^n$ 为 (α, L)- 列表可译码 。

理解列表译码这一概念比唯一译码更进一步的一种方式，是借助 Johnson 的一个定理。该定理（非正式地）表明，每个码 C 都是 (α, L)-列表可译码的，且列表大小为常数 L，只要参数 α 小于码的距离 Δ 的某个函数 $J(\Delta)$。 $J(\Delta)$称为该码的*Johnson*界（或 Johnson 半径），它始终至少为 $\frac{\Delta}{2}$，但也可能大得多。此外，将前述 Singleton界推广到列表译码设定后可知，任何 (α, L)-列表可译码码都必须满足 $\alpha \leq \frac{L}{L+1}(1-R)$。注意， $L = 1$ 的情形对应于经典辛格尔顿界，它意味着 $\alpha \leq \frac{\delta}{2} \leq \frac{1-R}{2}$ ；但当 L 增大时，该界会接近其两倍。若一个码逼近这一界限，我们就称其达到列表译码容量；也就是说，对于任意 $\epsilon > 0$，它都是 $(1-R-\epsilon, O_\epsilon(1))$-列表可译码的。（即使列表大小是码长的函数，只要有界，我们也称该码达到了列表译码容量。）如今我们已知有多个达到容量的列表可译码码族，它们只需允许一个较小的（常数大小）列表，就能容忍几乎是唯一译码设定下可纠正错误数两倍的错误！

在通信场景中，当接收方掌握关于所传输消息的一些边信息，能够据此从列表中排除某些码字时，列表译码便会很有用；列表可译码码也是构造唯一可译码码的重要基础。此外，列表可译码码还充当桥梁，连接上述对抗差错模型 （由汉明 [Ham50]首创；在此模型中，对手可以任意篡改码字条目中的一部分）与随机差错模型 （由香农 [Sha48]首创；在此模型中，每个码字条目都以某个固定概率独立地发生错误）。众所周知，与对抗模型相比，随机差错模型能够容忍更多错误（大约多一倍）。因此，借助列表可译码码，即使同时存在随机错误（此时列表通常只包含一个码字）和对抗错误（允许列表较短），也能处理比对抗性唯一译码设定下更多的错误。事实证明，列表可译码码对于计算机科学中的应用也非常有用，例如复杂性理论中的困难性结果，以及扩张图、提取器和伪随机生成器等各种伪随机对象的显式构造。

上述应用凸显了关于列表可译码码的两个主要基础问题。第一个是组合问题，目标是针对给定的译码半径，界定各种码的列表大小。第二个是计算问题，即设计显式列表可译码码及高效的列表译码算法，使其在给定接收字后输出与之接近的码字列表。这类成果中相当一部分针对的是基于低次多项式 的代数纠错码族（这同样受到上述应用的启发）。本综述旨在探讨其中的一些进展，重点讨论我们接下来将介绍的基于多项式的码族。

1.2 编码理论中的多项式

自该研究领域早期以来，代数方法，尤其是有限域上低次多项式的性质，在编码理论的发展中发挥了极其重要的作用。事实上，基于低次多项式（单变量或多变量）求值构造的纠错码族，是研究最为深入的码族之一。

这类码族的典型代表无疑是里德-所罗门码。该码的码字对应于所有次数小于 k 且系数为

有限域 $\mathbb{F}_q$ 中，在指定集合 $E \subseteq \mathbb{F}_q$（由 n 个域元素组成）上的取值。此类码的距离源于基本的代数事实：两个不同的次数小于 k 的一元多项式不可能在超过 k 个输入上取相同值。因此，里德-所罗门码是 MDS 码。

作为 Reed-Solomon 码核心的低次多项式的数学性质得到了广泛推广，并催生了许多其他基础且经过充分研究的码族。一些经典的例子包括*Reed-Muller*码，其码字对应于在乘积集合上对低次多元 多项式求值；BCH 码，其码字对应于求值落在某个小子域中的低次单变量多项式；以及代数几何 （AG）码，其码字对应于在某条代数曲线的有理点上对某些函数求值。

除了优雅的形式和基础的数学性质之外，在各种通信场景中，上述基于多项式的码在许多情况下实现了码率与纠错半径之间的最优权衡；其代数结构也有利于快速编码和译码算法。此外，Reed-Solomon 码等基于多项式的码因其良好的具体参数，也在实践中得到广泛应用。这些码的代数性质也常常有助于计算机科学应用。例如，一个有用的性质是乘法性质，它保证一对码字（例如，一对次数为 k 的多项式的求值）逐点相乘后，所得结果是另一个相关码中的码字（对应于次数为$2k$ 的多项式的求值）。

在本综述中，我们将重点关注基于多项式的码的列表译码性质，接下来对此进行讨论。

1.3 多项式码的列表译码

Sudan [Sud97]和 Guruswami-Sudan [GS99] 在20世纪90年代的著名研究，提出了高效（多项式时间）的算法，使 Reed-Solomon 码能够在唯一译码半径之外进行列表译码，直至 *Johnson*界。请注意，在这一界限内，列表大小保证为常数，因此问题仅在于计算，也就是说，设计高效的列表译码算法，在给定接收字后输出与之接近的码字列表。这一成果引发了人们对 Reed-Solomon 码超出 *Johnson*界后的列表可译码性的浓厚兴趣。超出这一半径后，问题既涉及组合方面，也涉及计算方面：既要证明列表大小的上界（若存在这样的上界），也要寻求高效的列表译码算法。尽管这一领域仍然极为活跃，且有许多尚待探索的研究方向，但对这一问题的关注一直是推动该领域其他许多重要进展的重要动力。

其中包括发现了里德-所罗门码的变体，并证明这些变体能够达到列表译码容量，且列表大小与广义辛格尔顿界相匹配；同时，还为这些码设计了可高效运行、达到容量的列表译码算法。这类码的典型例子包括折叠 *Reed-Solomon* 码：它将低次多项式的相关取值 打包成一个码字条目；以及重数码：其编码还包括低次多项式导数 的取值。

近期，该领域的研究也推动了人们对 Reed-Solomon 码超越 Johnson界的组合列表可译码性的理解取得重大进展。具体而言，研究表明，某些 Reed-Solomon 码在远超 Johnson界的范围内无法实现列表译码，且其列表大小会随码长呈多项式增长（更不用说达到常数列表大小了）；与此同时，研究还表明，以随机求值点构造的 Reed-Solomon 码能够达到列表译码容量，并且以高概率，其列表大小符合广义辛格尔顿界。寻找满足这一性质的显式求值点，并

设计相应的高效列表译码算法，是撰写本综述时该领域的一项重大悬而未决的问题。

上述所有基于多项式的码的一个缺点是，它们的字母表非常大（相对于码长呈多项式级）。通过采用适当的代数几何码变体，可以将字母表大小降至常数。就效率而言，我们现在已经知道上述列表解码算法的快速近线性时间实现。此外，利用*Reed-Muller*码和多变量重数码，还可以得到局部列表译码算法，能够在次线性时间内对单个码字分量进行列表译码。

1.4 本综述的组织与范围

本综述的组织结构如下：

- 在第2节中，我们首先给出列表可译码码与低次多项式的形式化定义和基本事实，并介绍将成为本综述重点的若干族基于多项式的码。

- 在第3节中，我们给出将里德-所罗门码列表译码至Johnson界的高效（多项式时间）算法，同时也给出超出Johnson界时里德-所罗门码列表大小的组合下界。

- 在第 4 节中，我们介绍了能够以高效（多项式时间）方式将重数码列表译码至容量的算法，并证明类似的算法也可用于对以子域求值点为求值点的 Reed-Solomon 码进行列表译码，所需时间略高于平凡的次指数时间。具体而言，这些算法表明，重数码在容量处的列表大小至多为码长的多项式，而以子域求值点为求值点的 Reed-Solomon 码的列表大小至多为码长的次指数函数。

- 在第 5 节中，我们给出了基于多项式的码在容量处列表大小的组合上界。具体而言，我们证明，以随机求值点为求值点的 Reed-Solomon 码和重数码的列表大小实际上是一个与码长无关的常数（甚至达到广义辛格尔顿界）；此外，通过转而考虑适当的子码，也可以将以子域求值点为求值点的 Reed-Solomon 码的列表大小降至常数，并将列表译码算法的运行时间降至多项式时间。

- 在第 6 节中，我们将介绍前几节所述的一些列表译码算法的更快速、近线性时间实现。

- 在第 7 节中，我们将介绍基于多元多项式的码的局部列表译码算法，这些算法能够在次线性时间内译码单个码字条目。

本综述介绍的部分内容也见于其他综述。具体而言，第 3.1 节介绍的 Reed-Solomon 码唯一解码算法也见于关于纠错码的在线教材[GRS，第 12.1] 节；第 3.2 节和第 3.3 节介绍的 Reed-Solomon 码列表译码算法也见于 [GRS，第 12.2], 节、Guruswami 关于算法列表译码的综述 [Gur06b，第 4] 节，以及 Sudan 最近关于代数在算法编码理论中应用的综述 [Sud25，第 4 节和第 5] 节。第 4.1 节介绍的超出唯一译码半径的重数码列表译码算法，沿用了 [GRS 第 17] 节中的讲述方式（另见

[Sud25，第 6]节），该节讨论的是相关的折叠 Reed-Solomon 码族。第 7.1 节介绍的 Reed-Muller码局部纠错算法也见于 Yekhanin 关于局部可解码码的综述 [Yek12，第 2]节。

本综述仅关注基于多项式的码的列表译码性质。在撰写本综述的同时，人们发现某些基于扩展子的码具有可与基于多项式的码相媲美的列表译码性质；尤其是，它们能够在常数大小的字母表上以最优列表大小译码至容量，且所需时间近乎线性 [ST25, JMST25]。

最后，本综述不讨论列表可译码码的任何应用。编码理论中的一些应用见 [Gur04, 第 11], 节；理论计算机科学中的应用见 [Sud00], [Tre04, 第 4], [节、 12], [Gur06a], [Vad12, 第 5], 节，以及 [GRS, 第 20 节和第 24] 节。列表恢复是列表译码概念的一种推广，对编码理论和理论计算机科学中的应用很有用，相关综述见 [RV25]。

2 记号与定义

本节首先介绍一些基本记号，然后分别在第 2.1 节和第 2.2 节给出列表可译码码和低次多项式的形式化定义，并陈述一些基本事实。最后，在第 2.3 节中，我们介绍若干基于多项式的码族，它们将是本综述的重点。

记号。对于两个字符串 u、$v \in \Sigma^n$，u 与 v 之间的（汉明）距离是 u 与 v 不同的位置数，记为 $\Delta(u,v) := |\{i \in [n] : u_i \neq v_i\}|$；$u$ 与 v 之间的相对（汉明）距离是 u 与 v 不同的位置所占的比例，记为 $\delta(u,v) := \Delta(u,v)/n$。如果字符串 $u \in \Sigma^n$ 与字符串 $v \in \Sigma^n$ 的距离 $\delta(v,u) \leq \alpha$ ($\delta(v,u) > \alpha$，则称 $u \in \Sigma^n$ 与 $v \in \Sigma^n$ 是 α-近的（分别称为 α-远的）。对于 $w \in \Sigma^n$ 和 $\alpha \in [0,1)$，我们将以 w 为中心、半径为 α 的汉明球定义为集合 $B(w,\alpha) := \{u \in \Sigma^n \mid \delta(u,w) \leq \alpha\}$。

对于任意素数幂 q，我们用 $\mathbb{F}_q$ 表示含有 q 个元素的有限域。对于域 $\mathbb{F}$ 和 $u \in \mathbb{F}^n$，u 的（汉明）权重 $|u|$ 是 u中非零分量的个数，即 $|u| := |\{i \in [n] : u_i \neq 0\}|$。全文中，我们令 $\mathbb{N} := \{0,1,2,\ldots\}$ 表示非负整数集合。对于向量 $\mathbf{i} = (i_1,\ldots,i_m) \in \mathbb{N}^m$，$\mathbf{i}$ 的权重 $\mathrm{wt}(\mathbf{i})$ 等于 $\mathrm{wt}(\mathbf{i}) = \sum_{j=1}^m i_j$；对于 $\mathbf{i} = (i_1,\ldots,i_m)$、$\mathbf{j} = (j_1,\ldots,j_m) \in \mathbb{N}^m$，我们令 $\binom{\mathbf{i}}{\mathbf{j}} := \prod_{k=1}^m \binom{i_k}{j_k}$。

2.1 列表可译码码

在正式定义列表可译码码之前，我们先介绍一些关于纠错码的基本记号与定义。

一个（纠错）码是一个子集 $C \subseteq \Sigma^n$。我们分别称 Σ 和 n为该码的字母表和码长，而 C 中的元素称为码字。码码率 $C \subseteq \Sigma^n$ 为$R := \log(|C|)/(n \cdot \log(|\Sigma|))$，$C$的（汉明）距离为 $\Delta(C) := \min_{c \neq c' \in C} \Delta(c,c')$，其相对距离为$\delta(C) := \Delta(C)/n$。

我们称码 $C \subseteq \Sigma^n$ 是 $\mathbb{F}$-线性的，如果 $\Sigma = \mathbb{F}^s$ 对于某个域 $\mathbb{F}$ 和正整数 s成立，并且 C 是 Σ^n的 $\mathbb{F}$-线性子空间。如果 $\Sigma = \mathbb{F}$，且 C 是 $\mathbb{F}$-线性码，那么我们就简称 C 为线性码。对于 $\mathbb{F}$-线性码 $C \subseteq \Sigma^n$，C 的码率等于$\dim_{\mathbb{F}}(C)/(n \cdot \dim_{\mathbb{F}}(\Sigma))$，而 C 的距离等于$\min_{0 \neq c \in C} |c|$。线性码 C的生成矩阵是一个（满秩）矩阵 $G \in \mathbb{F}^{n \times k}$，使得 $\mathrm{Image}(G) = C$，

而 C 的校验矩阵是一个（满秩）矩阵 $H \in \mathbb{F}^{(n-k)\times n}$，使得 $\ker(H) = C$。C 的对偶码是码 $C^{\perp} \subseteq \mathbb{F}^n$，它包含所有满足以下条件的字符串 $c' \in \mathbb{F}^n$：对于所有 $c \in C$，均有 $\sum_{i=1}^{n} c'_i \cdot c_i = 0$。根据定义可知，$(C^{\perp})^{\perp} = C$，并且 H 是 C 的校验矩阵，当且仅当 H^T 是 $C^{\perp}$的生成矩阵。

对于一个相对距离为 δ 的码 $C \subseteq \Sigma^n$ 和给定的 $\alpha < \frac{\delta}{2}$，从$\alpha$比例的错误中进行（唯一）译码的问题是：给定一个字符串 $w \in \Sigma^n$，求满足$\delta(c, w) \leq \alpha$ 的唯一 $c \in C$ （如果存在）。

列表译码是一种通过返回一个较短的邻近码字列表来纠正超过 $\frac{\delta}{2}$ 错误比例的方法。更正式地说，对于 $\alpha \in (0, 1)$ 和一个正整数 L，我们称一个码$C \subseteq \Sigma^n$ 是（α, L）-列表可译码的，如果对于任意 $w \in \Sigma^n$，至多有 L 个不同的码字 $c \in C$ 满足 $\delta(c, w) \leq \alpha$。从 α比例的错误中进行列表译码的问题是：给定一个字符串 $w \in \Sigma^n$，求满足 $\delta(c, w) \leq \alpha$ 的码字列表 $c \in C$。

Johnson界。Johnson界指出，任意 相对距离为 δ 的码都能从比例为 $\alpha < 1 - \sqrt{1-\delta}$ 的错误中进行列表译码，列表大小取决于 α 与 $1 - \sqrt{1-\delta}$ 的接近程度。注意，对于任意 $\delta \in (0,1)$，$1 - \sqrt{1-\delta} \in (\frac{\delta}{2}, \delta)$，因此这一界优于唯一译码界。

定理 2.1（Johnson界）。设 $C \subseteq \Sigma^n$ 是一个相对距离为 δ 的码。那么对于任意 $\alpha < 1 - \sqrt{1-\delta}$, C 是 (α, L) 列表可译码的，列表大小为 $L = \frac{\delta - \alpha}{(1-\alpha)^2 - (1-\delta)}$。

证明。设 $w \in \Sigma^n$ 是一个字符串，且 $\mathcal{L} = \{c \in C \mid \delta(c, w) \leq \alpha\}$。我们的目标是证明$L := |\mathcal{L}| \leq \frac{\delta - \alpha}{(1-\alpha)(1-\delta)}$。证明方法是分别给出列表中一对不同码字之间平均一致度的上界和下界，即 $\Pr_{c \neq c' \in \mathcal{L}, i \in [n]}[c_i = c'_i]$, 然后比较这两个界。

对于上界，注意到由于 C 的相对距离为 δ，我们有 $\delta(c, c') \geq \delta$，对任意不同的$c, c' \in \mathcal{L}$均成立。因此，我们有

$$\Pr_{c \neq c' \in \mathcal{L}, i \in [n]} \left[c_i = c'_i\right] \leq 1 - \delta. \tag{1}$$

接下来，我们给出上述表达式的一个下界。对于 $i \in [n]$, 令 t_i 表示$\mathcal{L}$ 中在第 i 个位置上与 w 相同的码字数量，即 $t_i := |\{c \in \mathcal{L} \mid c_i = w_i\}|$. 注意到，由于 $\delta(c, w) \leq \alpha$ 对任意 $c \in \mathcal{L}$均成立，我们有 $\mathbb{E}_{i \in [n]}[t_i] \geq L(1-\alpha)$。因此，我们有：

$$\begin{aligned} \Pr_{c \neq c' \in \mathcal{L}, i \in [n]} \left[c_i = c'_i\right] &\geq \Pr_{c \neq c' \in \mathcal{L}, i \in [n]} \left[c_i = c'_i = w_i\right] \\ &\geq \frac{\mathbb{E}_{i \in [n]} \binom{t_i}{2}}{\binom{L}{2}} \geq \frac{\binom{\mathbb{E}_{i \in [n]} t_i}{2}}{\binom{L}{2}} \geq \frac{\binom{L(1-\alpha)}{2}}{\binom{L}{2}}, \end{aligned} \tag{2}$$

其中，倒数第二个不等式由凸性得出。

结合 (1) 和 (2) 中给出的界，可得以下不等式：

$$\binom{L(1-\alpha)}{2} \leq \binom{L}{2} \cdot (1-\delta),$$

整理后即得到所需的界 $L \leq \frac{\delta - \alpha}{(1-\alpha)(1-\delta)}$。

□

广义辛格尔顿界。 经典辛格尔顿界 表明，任何码率为 R 、相对距离为 δ 的码都必须满足 $\delta \leq 1-R$。广义辛格尔顿界 推广了这一事实，表明任何码率为 R 的(α, L)-列表可译码都必须满足 $\alpha \lesssim \frac{L}{L+1} \cdot (1-R)$。注意，唯一译码的经典辛格尔顿界对应于 $L = 1$这一特殊情形，此时 $\alpha \leq \frac{\delta}{2} \leq \frac{1-R}{2}$。

定理 2.2 （广义辛格尔顿界）。 设 $C \subseteq \Sigma^n$ 是码率为 R 的码，且是（α, L）-列表可译码的。那么

$$\alpha \leq \frac{L}{L+1} \cdot (1 - R + o_L(1)),$$

其中，对于固定的 L，项 o_L（1）随着码长 n趋于无穷而趋于零。

证明。 令 $b := \frac{L+1}{L} \cdot \alpha n$，为简单起见，假设 b 是整数。

我们首先断言，对于任意字符串 $u \in \Sigma^{n-b}$， C 中以前缀 u开头的不同码字至多有 L 个。为此，反设存在一个字符串 $u \in \Sigma^{n-b}$ 以及 $L+1$ 个不同的码字c_0， c_1，……， $c_L \in C$，它们的前缀均为 u。令 $w \in \Sigma^n$ 为一个字符串，其前 $n-b$ 个分量与 u相同；对于 $i = 0$，1，……， L， w和 c_i 在后续第 i个长度为 $\frac{b}{L+1}$ 的块上相同（为简单起见，再次假设 $\frac{b}{L+1}$ 是整数）。那么根据构造，对于任意 $i \in \{0, 1, \ldots, L\}$，

$$\delta(w, c_i) \leq \frac{L}{L+1} \cdot \frac{b}{n} = \alpha,$$

这与 C 是 $(\alpha,\ L)$-列表可译码的假设相矛盾。

现在，由于对于任意字符串 $u \in \Sigma^{n-b}$， C 中至多有 L 个码字的前缀为 u，因此有 $|C| \leq \Sigma^{n-b} \cdot L$；整理并取对数可得

$$\frac{b}{n} \leq 1 - \frac{\log(|C|)}{n \cdot \log(|\Sigma|)} + \frac{\log(L)}{n \cdot \log(|\Sigma|)}.$$

将上述不等式中的值 $R = \frac{\log(|C|)}{n \cdot \log(|\Sigma|)}$ 和 $b = \frac{L+1}{L} \cdot \alpha n$ 代入，可得

$$\alpha \leq \frac{L}{L+1} \cdot \left(1 - R + \frac{\log(L)}{n \cdot \log(|\Sigma|)}\right) = \frac{L}{L+1} \cdot (1 - R + o_L(1)),$$

至此，定理得证。 □

上述广义辛格尔顿界特别意味着，对于某个 $\epsilon = \epsilon(L)$，$(\alpha,\ L)$-列表可译码码必须满足$\alpha \leq 1 - R - \epsilon$；当 L 增大时，该值趋近于零（具体而言， $\epsilon = O(\frac{1}{L})$，或等价地，$L = O(\frac{1}{\epsilon})$）。如果一个码 $\mathcal{C} \subseteq \Sigma^n$达到列表译码容量，–也就是说，它对任意 $\epsilon > 0$[1] 都是 $(1 - R - \epsilon,\ O_\epsilon(1))$-列表可译码的，那么我们就称该码达到了列表译码容量。

2.2 有限域上的多项式

本综述主要关注基于有限域上低次多项式的代数码。接下来，我们将介绍一些定义，并汇集若干关于有限域上多项式的已知事实，这些内容将用于定义此类码并分析其列表译码性质。

[1]我们有时会滥用记号，称该码达到了列表译码容量，即使列表大小以码长的某个函数为界。

2.2.1 单变量多项式

对于域 $\mathbb{F}$，我们用 $\mathbb{F}[X]$ 表示 $\mathbb{F}$ 上一元多项式的环，用 $\mathbb{F}(X)$ 表示以不定元 X 为变量、$\mathbb{F}$ 上有理函数的域。多项式 $f(X) = \sum_{i\in\mathbb{N}} f_i X^i \in \mathbb{F}[X]$ 的次数 $\deg(f)$ 是使得 $f_i \neq 0$ 成立的最大 i。我们用 $\mathbb{F}_{<d}[X]$（分别用 $\mathbb{F}_{\leq d}[X]$）表示 $\mathbb{F}$ 上所有次数小于 d（分别不超过 d）的一元多项式构成的线性空间。多项式 $f(X) \in \mathbb{F}[X]$ 的一个根是满足 $f(a) = 0$ 的点 $a \in \mathbb{F}$。众所周知，次数为 d 的非零多项式 $f(X) \in \mathbb{F}[X]$ 在 $\mathbb{F}$ 中至多有 d 个根。

有时，统计根时也需要考虑重数。为定义这一概念，我们首先需要定义（哈斯）导数的概念，它是经典导数的一种变体，更适用于有限域。设 $f(X) \in \mathbb{F}[X]$ 是域 $\mathbb{F}$上的非零一元多项式。对于非负整数i，i阶（哈斯）导数 $f^{(i)}(X)$定义为展开式中 Z^i 的系数，其中 f

$$f(X+Z) = \sum_{i\in\mathbb{N}} f^{(i)}(X) Z^i.$$

特别地，对于任意 $a \in \mathbb{F}$，分别将上式中的 $a, X-a$ 代入 X, Z，即可得到展开式

$$f(X) = \sum_{i\in\mathbb{N}} f^{(i)}(a)(X-a)^i. \tag{3}$$

上述展开式应与更熟悉的经典导数对应的泰勒展开进行比较；在后者中，$(X-a)^i$ 的系数还要除以一个额外的因子 $i!$。消去这个额外因子 $i!$（它在有限域上可能为零）是很方便的，也往往能使定理的表述更加简洁。

多项式 $f(X) \in \mathbb{F}[X]$ 在点 $a \in \mathbb{F}$ 处的重数，记为 $\mathrm{mult}(f, a)$，是最大的整数s，使得对任意非负整数 $i < s$，都有 $f^{(i)}(a) = 0$。注意，对任意$a \in \mathbb{F}$，$\mathrm{mult}(f, a) \geq 0$，并且对 f 的任意根 a，$\mathrm{mult}(f, a) > 0$。下述事实是 (3) 中所给展开式的直接推论，它推广了低次单变量多项式根的数量上界这一众所周知的结果，同时也考虑了重数。

事实 2.3. 设 $f(X) \in \mathbb{F}[X]$ 是次数为 d 的非零一元多项式。则

$$\sum_{a\in\mathbb{F}} \mathsf{mult}(f, a) \leq d.$$

特别地，对任意正整数 s，$\mathsf{mult}(f, \mathbf{a}) \geq s$ 至多对点 $a \in \mathbb{F}$ 的 $\frac{d}{s|\mathbb{F}|}$比例成立。

注意，上述事实中“特别地”部分的 $s = 1$ 情形对应于低次单变量多项式根的数量的标准上界。

我们注意到以下关于 Hasse 导数的基本性质，这些性质可直接由 Hasse 导数的定义得出。

引理 2.4。对于任意域 $\mathbb{F}$、单变量多项式 $f(X)$ $g(X) \in \mathbb{F}[X]$ 以及非负整数 i、j，下述结论成立：

1. *(Linearity)* $(f(X) + g(X))^{(i)} = f^{(i)}(X) + g^{(i)}(X)$.
2. （乘积法则）$(f(X) \cdot g(X))^{(i)} = \sum_{k=0}^{i} f^{(k)}(X) \cdot g^{(i-k)}(X)$。

3.（迭代应用）$(f^{(i)}(X))^{(j)} = \binom{i+j}{i} \cdot f^{(i+j)}(X)$。

请注意，与经典导数不同，Hasse 导数只有在额外乘以一个二项式系数后才具有迭代性；但另一方面，乘积法则不需要额外乘以二项式系数。

最后，对于一元多项式 $f(X)$ $h(X) \in \mathbb{F}[X]$，我们用 ($f(X)$ mod $h(X)$) 表示将 $f(X)$ 除以 $h(X)$ 所得的唯一余式。我们还称 $f(X)$ 与 $g(X)$ 模 $h(X)$ 同余（记作 ($f(X) \equiv g(X)$ mod $h(X)$），当且仅当 ($f(X) - g(X)$) 可被 $h(X)$ 整除。

2.2.2 多元多项式

上述定义的概念也可以推广到多元多项式的情形。具体而言，对于域 $\mathbb{F}$ 和正整数 m，我们用 $\mathbb{F}[X_1, \ldots, X_m]$ 表示 m 元多项式在 $\mathbb{F}$ 上构成的环，并用 $\mathbb{F}(X_1, \ldots, X_m)$ 表示 $\mathbb{F}$ 上关于不定元 $X_1, \ldots, X_m$ 的有理函数域。为方便记号，我们令 $\mathbf{X} := (X_1, X_2, \ldots)$；在本综述中，我们还约定用粗体字母 $\mathbf{a}$,$\mathbf{b}$ ... 表示 $\mathbb{F}$ 上的向量。对于 $\mathbf{i} = (i_1, \ldots, i_m) \in \mathbb{N}^m$，我们用 $\mathbf{X^i}$ 表示单项式 $\mathbf{X^i} := X_1^{i_1} \cdots X_m^{i_m}$。

多项式 $f(\mathbf{X}) = \sum_{\mathbf{i}} f_{\mathbf{i}} \mathbf{X^i} \in \mathbb{F}[\mathbf{X}]$ 的（总）次数 $\deg(f)$，是满足 $f_{\mathbf{i}} \neq 0$ 的 $\mathbf{i}$ 的最大权重 $\mathrm{wt}(\mathbf{i}) = \sum_j \mathbf{i}_j$。与之前一样，我们用 $\mathbb{F}_{<d}[X_1, \ldots, X_m]$（分别用 $\mathbb{F}_{\leq d}[X_1, \ldots, X_m]$）表示所有 m 元多项式构成的线性空间，这些多项式定义在 $\mathbb{F}$ 上，且（总）次数小于 d（至多为 d）。在多元情形下，我们有时也会用到加权次数的概念。具体而言，对于向量 $\mathbf{b} \in \mathbb{N}^m$，多项式 $f(\mathbf{X}) = \sum_{\mathbf{i}} f_{\mathbf{i}} \mathbf{X^i} \in \mathbb{F}[\mathbf{X}]$ 的 $\mathbf{b}$-加权次数 $\deg_{\mathbf{b}}(f)$，是满足 $f_{\mathbf{i}} \neq 0$ 的 $\mathbf{i}$ 的最大加权和 $\sum_j \mathbf{b}_j \cdot \mathbf{i}_j$。

与单变量情形一样，我们将多项式 $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ 的根定义为点 $\mathbf{a}$，使得 $f(\mathbf{a}) = 0$。以下著名的 Schwartz-Zippel 引理 将低次单变量多项式的根的数量上界推广到了多元情形。

引理 2.5 ([Sch80, Zip79, DL78])。设 $f(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ 是有限域 $\mathbb{F}$ 上的一个非零 m 元多项式，其（总）次数为 d。则 f 在 $\mathbb{F}^m$ 中至多有 $d \cdot |\mathbb{F}|^{m-1}$ 个根。

Hasse 导数的概念也可以按如下方式推广到多元情形。设$f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ 是域 $\mathbb{F}$ 上的一个非零 m 元多项式。对于向量 $\mathbf{i} \in \mathbb{N}^m$，我们将 $\mathbf{i}$ 阶（Hasse）导数 $f^{(\mathbf{i})}(\mathbf{X})$ 定义为展开式中 $\mathbf{Z^i}$ 的系数

$$f(\mathbf{X} + \mathbf{Z}) = \sum_{\mathbf{i} \in \mathbb{N}^m} f^{(\mathbf{i})}(\mathbf{X}) \mathbf{Z^i}.$$

我们将 f 在点 $\mathbf{a} \in \mathbb{F}^m$处的重数 定义为记作 $\mathrm{mult}(f, \mathbf{a})$ 的最大整数 s，使得对于任意满足 $\mathrm{wt}(\mathbf{i}) < s$ 的 $\mathbf{i} \in \mathbb{N}^m$，都有 $f^{(\mathbf{i})}(\mathbf{a}) = 0$。

下面的定理将上述引理 2.5 推广到同时考虑根的重数。

定理 2.6 ([DKSS13], 引理 2.7)。设 $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ 是有限域 $\mathbb{F}$上的一个非零 m元多项式，其（总）次数为 d。那么

$$\sum_{\mathbf{a} \in \mathbb{F}^m} \mathrm{mult}(f, \mathbf{a}) \leq d \cdot |\mathbb{F}|^{m-1}.$$

特别地，对于 任意正整数 s，对于至多占点集$\mathrm{mult}(f, \mathbf{a}) \geq s$的 $\frac{d}{s|\mathbb{F}|}$ 比例的点$\mathbf{a} \in \mathbb{F}^m$。

请注意，上述定理的 $m = 1$ 情形对应于上述事实 2.3，而“特别是”部分的 $s = 1$ 情形对应于上述引理 2.5。

我们还有如下对引理 2.4 的推广。

引理 2.7. 对任意域 $\mathbb{F}$、m元多项式 $f(\mathbf{X})$ $g(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$, 以及 $\mathbf{i}$、$\mathbf{j} \in \mathbb{N}^m$，下列结论成立：

1.（线性性）$(f(X) + g(X))^{(\mathbf{i})} = f^{(\mathbf{i})}(X) + g^{(\mathbf{i})}(X)$。*2.*（乘积法则）$(f(X) \cdot g(X))^{(\mathbf{i})} = \sum_{r,k\,:\, r+k=i} f^{(\mathbf{r})}(X) \cdot g^{(\mathbf{k})}(X)$。*3.*（迭代应用）$(f^{(\mathbf{i})}(X))^{(\mathbf{j})} = \binom{\mathbf{i+j}}{i} \cdot f^{(i+j)}(X)$。

2.3 多项式码的若干族

接下来我们介绍本综述将重点讨论的若干族多项式码。所有码都定义在含有 q 个元素的有限域 $\mathbb{F}_q$ 上，其中 q 为某个素数幂。我们从最基本的一族里德-所罗门码开始。

Reed-Solomon（RS）码。令 $a_1, \ldots, a_n$ 是 $\mathbb{F}_q$ 中互不相同的点（称为求值点），并令 $k < n$ 为正整数（即次数参数）。Reed-Solomon（RS）码 $\mathrm{RS}_q(a_1, \ldots, a_n;\, k)$ 是一种码，它将每个次数小于 k 的一元多项式 $f(X) \in \mathbb{F}_q[X]$ 映射为码字 $(f(a_1) \ldots, f(a_n)) \in \mathbb{F}_q^n$.。在 $n = q$ 的特殊情形下，我们令 $\mathrm{RS}_q(k) := \mathrm{RS}_q(a_1, \ldots, a_n;\, k)$。

根据定义，Reed-Solomon 码 $\mathrm{RS}_q(a_1, \ldots, a_n;\, k)$ 是码率为 $\frac{k}{n}$ 的线性码。此外，由于任意两个次数–小于 k 的不同一元多项式在 $\mathbb{F}_q$ 中至多有 $k-1$ 个点取值相同（因为它们的差是一个非零的、次数小于 k 的一元多项式，因此在 $\mathbb{F}_q$ 中至多有 $k-1$ 个根），可知 $\mathrm{RS}_q(a_1, \ldots, a_n;\, k)$ 的距离至少为 $n - k + 1$，相对距离至少为 $1 - \frac{k}{n}$。因此，Reed-Solomon 码达到了 Singleton界（所以它是最大距离可分码）。

本综述重点讨论的另一类多项式码是重数码，它通过同时计算多项式的导数 扩展了 Reed-Solomon 码。

重数码。与之前一样，设 $a_1, \ldots, a_n$ 是 $\mathbb{F}_q$ 中互不相同的求值点，并设 s 为正整数（重数参数）。将重数参数 s 设得较大，可以使我们选择一个大于码长的次数参数。具体而言，我们可以选择任意满足 $k < sn$ 的正整数作为次数参数 k。单变量重数码 $\mathrm{MULT}_q^{(s)}(a_1, \ldots, a_n;\, k)$ 的定义与相应的 Reed-Solomon 码 $\mathrm{RS}_q(a_1, \ldots, a_n;\, k)$ 类似，不同之处在于，形式为 $(f(a_1) \ldots, f(a_n))$ 的每个码字现在替换为码字 $\left(f^{(<s)}(a_1) \ldots, f^{(<s)}(a_n)\right)$；其中，对于 $a \in \mathbb{F}_q$，我们用 $f^{(<s)}(a) \in \mathbb{F}_q^s$ 表示一个向量，该向量包含 f 在 a 处所有阶数小于 s 的（哈斯）导数，即 $f^{(<s)}(a) = (f(a)\ f^{(1)}(a) \ldots, f^{(s-1)}(a)$。

根据定义，重数码 $\mathrm{MULT}_q^{(s)}(a_1、\ldots\ldots、a_n;\, k)$ 是字母表为 $\mathbb{F}_q^s$、码率为 $\frac{k}{sn}$ 的 $\mathbb{F}_q$-线性码。此外，根据事实 2.3，$\mathrm{MULT}_q^{(s)}(a_1、\ldots\ldots、a_n;\, k)$ 的距离至少为 $n - \frac{k-1}{s}$，相对距离至少为 $1 - \frac{k}{sn}$。最后请注意，里德-所罗门码对应于重数参数为 $s = 1$ 的特殊情形。

接下来，我们介绍上述码的多变量扩展。第一种此类扩展是*Reed-Muller*码，它将里德-所罗门码扩展到多变量多项式的情形。

Reed-Muller（RM）码。为简单起见，我们在此仅给出在整个域上求值的Reed-Muller码的定义。更具体地说，与里德-所罗门码的情形一样，设 k 为次数参数，使得 $k < q$，并设 m 为正整数。Reed-Muller（RM）码里德-穆勒码$_{q,m}(k)$是一个码，它将任意次数小于k 的 m元多项式 $f(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ 与一个码字$(f(\mathbf{a}))_{\mathbf{a}\in\mathbb{F}_q^m}$相关联

根据定义，Reed-Muller 码 RM$_{q,\ m}(k)$ 是一种码长为 q^m 的线性码。其维数等于 m 个变量中次数小于 k 的单项式数量，即 $\binom{m+k-1}{m}$，因此该码的码率为 $\binom{m+k-1}{m}/q^m$。此外，根据 Schwartz-Zippel 引理（引理 2.5），RM$_{q,\ m}(k)$ 的相对距离至少为 $1 - \frac{k}{q}$。还需注意，上述 Reed-Muller 码在 $m = 1$ 情形下对应于在整个域上取值的 Reed-Solomon 码 RS$_q(k)$。

最后，我们还介绍将重数码推广到多元情形。

多变量重数码。再一次，为简便起见，这里只给出在整个域上取值的多变量重数码的定义。与单变量重数码的情形一样，设 k 为次数参数，s 为重数参数，使得 $k < s \cdot q$；与 Reed-Muller 码的情形一样，设 m 为正整数。多变量重数码 MULT$_q^{(s)}$,$_m(k)$ 的定义与相应的 Reed-Muller 码 RM$_{q,m}(k)$ 类似，不同之处在于，形如 $(f(\mathbf{a}))_{\mathbf{a}\in\mathbb{F}_q^m}$ 的每个码字现在都替换为码字 $(f^{(<s)}(\mathbf{a}))_{\mathbf{a}\in\mathbb{F}_q^m}$；与单变量重数码的情形类似，我们令$f^{(<s)}(\mathbf{a})$ 表示一个向量，该向量包含 m 元函数 f 在 a 处所有阶数小于 s 的（哈斯）导数，即 $f^{(<s)}(\mathbf{a}) = (f^{(\mathbf{i})}(\mathbf{a}))_{\mathbf{i}\in\mathbb{N}^m:\ \mathrm{wt}(\mathbf{i})<s}$。注意，该向量的长度等于权重小于 s 的向量 $\mathbf{i} \in \mathbb{N}^m$ 的数量，即 $\binom{m+s-1}{m}$。

根据定义，多变量重数码 MULT$_q^{(s)}$、$_m(k)$ 是一个 $\mathbb{F}_q$-线性码，其字母表为 $\mathbb{F}_q^{\binom{m+s-1}{m}}$，维数为 $\binom{m+k-1}{m}$，因此码率为 $\binom{m+k-1}{m}/\binom{m+s-1}{m} \cdot q^m$。此外，根据定理 2.6，MULT$_q^{(s)}$、$_m(k)$ 的相对距离至少为 $1 - \frac{k}{sq}$。

2.4 文献注记

列表译码。列表译码的模型最早由 Elias [Eli57] 和 Wozencraft [Woz57] 引入。Johnson界 是编码理论中的经典界，而与定理 2.1 中所述界具有类似形式的一个界，曾在 [GRS00 第 4 节 1] 的列表译码背景下出现。我们对定理 2.1 的证明遵循 [Gur06b 第 3 定理 1] 中的证明；该证明在其中归于 Radhakrishnan。Singleton界 是编码理论中的另一个经典界，归于 Singleton [Sin64], ，但此前也曾出现在 [Jos58] 中。广义辛格尔顿界 由 Shangguan 和 Tamo [ST20], 于较近时期提出并证明，随后 Roth[Rot22] 以及 Goldberg、Shangguan 和 Tamo [GST24] 又对这一界给出了进一步的改进和推广。

本节仅陈述并证明了 Johnson 界和广义辛格尔顿界的简化依赖字母表的版本，因为本综述聚焦于定义在大字母表上、并达到最佳列表译码半径的基于多项式的码。Johnson 界的依赖字母表版本可见 [Gur06b，第 3 节1]。此外，已知在一个 q 元字母表上，列表译码容量（即码率为 R 的码所能达到的最佳列表译码半径）为

$H_q^{-1}(1-R)$，其中

$$H_q(\alpha) = \alpha \log_q(q-1) + \alpha \log_q\left(\frac{1}{\alpha}\right) + (1-\alpha)\log_q\left(\frac{1}{1-\alpha}\right)$$

表示 q元熵函数 （例如参见 [Gur06b，第 3.2] 节）。可以验证，随着字母表增大， $H_q^{-1}(1-R)$ 趋近于 $1-R$。

基于多项式的码。 定理 2.6 给出了低次多项式根的数量上界，并按重数计数；该定理由 Dvir、Kopparty、Saraf 和 Sudan [DKSS13] 陈述并证明。这个上界扩展了引理 2.5 中关于不计重数的根的数量的经典上界；该上界由 Schwartz [Sch80], Zippel [Zip79], 以及 DeMillo 和 Lipton [DL78]分别独立证明。

里德-所罗门码 是由 Reed 和 Solomon [RS60], 提出的经典码，而Reed-Muller码 由 Muller [Mul54], 提出，Reed [Ree54]则提出了这些码的快速译码器。单变量重数码 由 Rosenbloom 和 Tsfasman[RT97], 提出，而其多变量扩展则是最近由 Kopparty、Saraf 和 Yekhanin[KSY14]提出的。

3 超越 Johnson界的列表译码算法

本节聚焦于最基本的一类*Reed-Solomon* (RS)码，并说明如何高效地对这些码进行列表译码，使其超越唯一译码半径，达到*Johnson*界（参见定理 2.1）。请注意，在此界限以内，列表大小保证为常数，因此问题仅在于计算，也就是设计高效的列表译码算法：给定一个接收字，输出与之距离较近的码字列表。

作为预热，我们首先在下文第 3.1 节介绍一种高效的（多项式时间）算法，用于对 Reed-Solomon 码进行唯一译码，译码半径可达其最小距离的一半。随后，在第 3.2 节中，我们介绍一种高效算法，用于对 Reed-Solomon 码进行列表译码，使其超越最小距离的一半；而在第 3.3 节中，我们将说明如何把该算法扩展至*Johnson*界。最后，我们在第 节中给出 Reed-Solomon 码列表大小的组合下界，该下界适用于超越 Johnson界的情形，并特别意味着不存在能够对一般 Reed-Solomon 码进行远超 Johnson界的高效列表译码算法。

3.1 Reed-Solomon 码的唯一译码

本节首先作为热身，介绍一种高效的（多项式时间）算法，用于对 Reed-Solomon 码进行唯一译码，可达其最小距离的一半。

更具体地说，固定一个素数幂 q、互不相同的求值点 $a_1, \ldots, a_n \in \mathbb{F}_q$，以及一个正整数$k < n$。回顾一下，Reed-Solomon（RS）码 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 是这样一种码：它将每个次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$ 映射为码字 $(f(a_1) \ldots, f(a_n)) \in \mathbb{F}_q^n$.。为避免令人烦恼的取整问题，以下为简单起见，假设 k, n 的奇偶性相同。设 $w \in \mathbb{F}_q^n$ 是一个接收字，并假设存在一个（唯一的）次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$，使得对于至多 $e := \frac{n-k}{2}$ 个指标 $i \in [n]$，$f(a_i) \neq w_i$。也就是说，对于至少 $t := n - e = \frac{n+k}{2}$ 个指标 $i \in [n]$，$f(a_i) = w_i$。下面我们将介绍一种求出 $f(X)$ 的算法（从而也能求出相应的码字 $(f(a_1)\ f(a_2) \ldots, f(a_n))$）。特别地，若令 $R := \frac{k}{n}$ 表示 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 码的码率，则该算法能够纠正比例为 $\frac{1-R}{2}$ 的错误。

概述。 通常，解码算法分为两个主要步骤。第一步是插值 步骤，在此步骤中，我们求出一个非零低次二元多项式 $Q(X,Y) \in \mathbb{F}_q[X,Y]$，使得对于任意 $i \in [n]$，$Q(a_i, w_i) = 0$。第二步是求根 步骤，在此步骤中，我们求出一个满足 $Q(X, g(X)) = 0$ 的一元多项式 $g(X) \in \mathbb{F}_q[X]$。为证明正确性，我们需要证明这样的非零低次多项式 Q 存在，并且 $g(X) = f(X)$。我们还需要确保这两个步骤都能高效执行（运行时间关于 n 和 $\log(q)$ 为多项式）。下面我们将分别介绍这两个步骤，并分析其正确性和效率。

步骤 1：插值。我们先介绍插值的第一步，其中我们希望求一个非零的低次二元多项式 $Q(X,Y) \in \mathbb{F}_q[X,Y]$，使得对任意 $i \in [n]$，都有 $Q(a_i, w_i) = 0$。

如何求得这样的多项式 Q？令

$$E(X) := \prod_{i: f(a_i) \neq w_i} (X - a_i)$$

表示其根为所有错误位置（即所有满足 $f(a_i) \neq w_i$ 的求值点 a_i）的错误定位多项式。

主要观察是，若令

$$Q(X,Y) = E(X) \cdot f(X) - E(X) \cdot Y,$$

那么对任意 $i \in [n]$，都有

$$Q(a_i, w_i) = E(a_i) \cdot f(a_i) - E(a_i) \cdot w_i = 0.$$

要说明上述结论确实成立，请注意，如果 $f(a_i) = w_i$，那么显然有 $Q(a_i, w_i) = 0$；而如果 $f(a_i) \neq w_i$，那么根据 E 的定义，$E(a_i) = 0$，因此在这种情况下也显然有 $Q(a_i, w_i) = 0$。

受上述结果启发，我们希望寻找一个具有如下形式的非零二元多项式 $Q(X, Y)$，其系数属于 $\mathbb{F}_q$

$$Q(X,Y) = A(X) + B(X) \cdot Y,$$

其中 $A(X)$ 的次数至多为 $e + k - 1 = \frac{n+k}{2} - 1$，$B(X)$ 的次数至多为 $e = \frac{n-k}{2}$，并且满足：对于任意 $i \in [n]$，$Q(a_i, w_i) = 0$。根据上述结果，由 $A(X) = E(X) \cdot f(X)$ 和 $B(X) = -E(X)$ 的选取可知，这样的非零多项式 $Q(X, Y)$ 存在。接下来，我们将用另一种线性代数论证证明 Q 的存在性；在之后尝试将唯一解码算法扩展到列表译码时，这种论证将很有用。

引理 3.1。 存在一个非零二元多项式 $Q(X, Y)$，其系数属于 $\mathbb{F}_q$，且具有如下形式

$$Q(X,Y) = A(X) + B(X) \cdot Y,$$

其中 $A(X)$ 的次数至多为 $\frac{n+k}{2} - 1$，$B(X)$ 的次数至多为 $\frac{n-k}{2}$，并且满足：对于任意 $i \in [n]$，$Q(a_i, w_i) = 0$。

此外，通过求解一个线性方程组可以找到这样的多项式 $Q(X,Y)$。该方程组的构造方法是：将 $A(X)$ 和 $B(X)$ 中单项式的系数视为未知数，并将每个形如 $Q(a_i, w_i) = A(a_i) + B(a_i) \cdot w_i = 0$ 的要求视为关于这些未知数的齐次线性约束。

证明。 如果将 $A(X)$ 和 $B(X)$ 中单项式的系数视为未知数，那么每个形如 $Q(a_i, w_i) = A(a_i) + B(a_i) \cdot w_i = 0$ 的要求都会对这些未知数施加一个齐次线性约束。还要注意，未知数的数量为 $(\deg(A) + 1) + (\deg(B) + 1) = n + 1$，而线性约束的数量为 n，因此这个线性系统有一个非零解。 □

步骤 2：求根。 在此步骤中，我们希望找到一个一元多项式 $g(X) \in \mathbb{F}_q[X]$，使其满足 $Q(X, g(X)) = 0$，并希望证明 $g(X) = f(X)$。为此，我们首先证明 $Q(X, f(X)) = 0$。只需证明一元多项式 $P_f(X) := Q(X, f(X))$ 的根的数量多于其次数即可。

引理3.2。 设 $Q(X, Y)$ 是 $\mathbb{F}_q$ 上的一个非零二元多项式，其形式为

$$Q(X, Y) = A(X) + B(X) \cdot Y,$$

其中 $A(X)$ 的次数至多为 $\binom{n+k}{2} - 1$，而 $B(X)$ 的次数至多为 $\binom{n-k}{2}$，并且对任意 $i \in [n]$，满足 $Q(a_i, w_i) = 0$。设 $f(X) \in \mathbb{F}_q[X]$ 是一个次数小于 k 的一元多项式，使得对于至少 $\binom{n+k}{2}$ 个指标 $i \in [n]$，有 $f(a_i) = w_i$。则 $Q(X, f(X)) \equiv 0$。

证明。 多项式 $P_f(X) := Q(X, f(X)) \in \mathbb{F}_q[X]$ 是次数至多为 $\binom{n+k}{2} - 1$ 的一元多项式，并且满足：对于任意满足 $f(a_i) = w_i$ 的 $i \in [n]$，都有 $P_f(a_i) = Q(a_i, f(a_i)) = Q(a_i, w_i) = 0$。因此，$P_f(X)$ 是次数至多为 $\binom{n+k}{2} - 1$ 且至少有 $\binom{n+k}{2}$ 个根的一元多项式，所以它必定是零多项式。 □

The 下一个引理表明，$f(X)$ 是满足 $Q(X, f(X)) = 0$ 的唯一多项式 .

引理3.3。 设 $Q(X, Y)$ 是 $\mathbb{F}_q$ 上的一个非零二元多项式，其形式为

$$Q(X, Y) = A(X) + B(X) \cdot Y.$$

至多存在一个一元多项式 $f(X) \in \mathbb{F}_q[X]$，使得 $Q(X, f(X)) = 0$。此外，若 $Q(X, f(X)) = 0$，则 $B(X) \neq 0$ 且 $f(X) = -\frac{A(X)}{B(X)}$。

证明。假设对某个一元多项式 $f(X) \in \mathbb{F}_q[X]$，有 $Q(X, f(X)) = 0$。我们首先证明 $B(X) \neq 0$。反设 $B(X) = 0$。则由我们的假设，同样有 $0 = Q(X, f(X)) = A(X)$，这进而蕴含 $Q(X, Y) = A(X) + B(X) \cdot Y = 0$，与 $Q(X, Y)$ 非零的假设矛盾。由假设 $0 = Q(X, f(X)) = A(X) + B(X) \cdot f(X)$，这进而蕴含 $f(X) = -\frac{A(X)}{B(X)}$，因此 $f(X)$ 被唯一确定。特别地，至多存在一个一元多项式 $f(X) \in \mathbb{F}_q[X]$，使得 $Q(X, f(X)) = 0$。 □

算法的完整描述见下方图1，随后是正确性与效率分析。

正确性。 假设 $f(X) \in \mathbb{F}_q[X]$ 是一个次数小于 k 的单变量多项式，使得 $f(a_i) = w_i$ 对至少 $t := \binom{n+k}{2}$ 个指标 $i \in [n]$ 成立。根据引理 3.1，存在一个非零二元多项式 $Q(X, Y)$，满足步骤 1 的要求。根据引理3.2，我们有 $Q(X, f(X)) = 0$；而由引理3.3可知，进而有 $B(X) \neq 0$ 且 $f(X) = -\frac{A(X)}{B(X)}$，因此算法将在步骤 2 中计算出正确的 $f(X)$。显然，$f(X)$ 也会通过步骤 3 的检查，因此算法将按要求返回 $f(X)$。

$\mathrm{RS}_q(a_1,\ldots,a_n;\,k)$**的唯一译码：**

▷ 为简单起见，假设 n，k 具有相同的奇偶性。

- **输入：** $w \in \mathbb{F}_q^n$。
- **输出：** 一个次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$，使得对于至少 $\frac{n+k}{2}$ 个指标 $i \in [n]$，$f(a_i) = w_i$；若存在这样的多项式，则返回该多项式，否则返回 $\perp$。

1. 求一个非零二元多项式 $Q(X, Y)$，其系数取自 $\mathbb{F}_q$，形式如下

$$Q(X,Y) = A(X) + B(X) \cdot Y,$$

其中，$A(X)$ 的次数至多为 $\frac{n+k}{2} - 1$，$B(X)$ 的次数至多为 $\frac{n-k}{2}$，并且满足对任意 $i \in [n]$，$Q(a_i, w_i) = 0$。这样的多项式 $Q(X, Y)$ 可通过求解一个线性方程组得到：将 $A(X)$ 和 $B(X)$ 中单项式的系数视为未知数，并将每个形如 $Q(a_i, w_i) = A(a_i) + B(a_i) \cdot w_i = 0$ 的要求视为关于这些未知数的齐次线性约束。2. 如果 $B(X) = 0$，则返回 $\perp$；否则，求一个一元多项式 $f(X)$，使得 $Q(X, f(X)) = 0$，方法是令 $f(X) := -\frac{A}{B}(X)$。3. 如果 $f(X)$ 是一个次数小于 k 的多项式，且对于至少 $\frac{n+k}{2}$ 个指标 $i \in [n]$，$f(a_i) = w_i$，则返回 $(f(a_1), f(a_2), \ldots, f(a_n))$；否则，返回 $\perp$。

图1：Reed-Solomon 码的唯一译码

效率。 步骤 1 可通过高斯消元求解一个包含 n 个线性方程和 $n+1$ 个变量的方程组，在 poly(n,log(q)) 时间内完成。步骤 2 可通过使用欧几里得算法进行多项式除法，在 poly(n,log(q)) 时间内完成。显然，步骤 3 也可在 poly(n,log(q)) 时间内完成。

3.2 超越唯一译码半径的 Reed-Solomon 码列表译码 s

本节将介绍一种高效算法，用于对超出其最小距离一半的 Reed-Solomon 码进行列表译码。

与之前一样，固定一个素数幂 q、互不相同的求值点 $a_1, \ldots, a_n \in \mathbb{F}_q$ 和一个正整数 $k < n$，并令 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 为相应的 Reed-Solomon 码。设 $w \in \mathbb{F}_q^n$ 是一个接收字。我们的目标是计算所有多项式 $f(X) \in \mathbb{F}_q[X]$ 的列表，这些多项式的次数小于 k，且满足 $f(a_i) \neq w_i$ 对至多 $e := n - \sqrt{2kn} - 1$ 个指标 $i \in [n]$ 成立。也就是说，$f(a_i) = w_i$ 对至少 $t := n - e = \sqrt{2kn} + 1$ 个指标 $i \in [n]$ 成立。

特别地，如果令 $R := \frac{k}{n}$ 表示 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 码的码率，那么该算法最多能够从大约 $(1 - \sqrt{2R})$ 比例的错误中进行列表译码。可以验证，当码率 R 小于 0。17 时，这一译码半径严格大于 $\frac{1-R}{2}$ 的唯一译码半径。

概述。 回顾一下，在唯一译码设定中，译码算法分为两个主要步骤：插值步骤中，我们求一个非零的低次二元多项式 $Q(X, Y) \in \mathbb{F}_q[X, Y]$，其形式为 $Q(X, Y) = A(X) + B(X) \cdot Y$，使得对于任意 $i \in [n]$，都有 $Q(a_i, w_i) = 0$；以及求根步骤中，我们求满足以下条件的（唯一）一元多项式 $f(X) \in \mathbb{F}_q[X]$：

$Q(X, f(X)) = 0$。

审视引理 3.1 和引理 3.2 的证明，我们观察到，我们从 Q中所需的主要性质是： Q 中未知系数的个数大于形如$Q(a_i, w_i) = 0$的约束个数 n ，并且 Q 的 $(1, k)$-加权次数 $\deg^{(1,k)}(Q)$ 小于一致参数 t。[2]第一个性质保证了非零 Q 的存在。第二个性质保证：对于任意次数小于 k的一元多项式 $f(X) \in \mathbb{F}_q[X]$，若 $f(a_i) = w_i$对至少 t个指标$i \in [n]$成立，则 $P_f(X) := Q(X, f(X))$ 是一个次数小于 t且至少有 t个根的一元多项式，从而 $P_f(X) = Q(X, f(X)) = 0$。

在列表译码设定中，一致参数 t 更小，这意味着 Q 的 $(1, k)$-加权次数也必须更小。因此， Q 可能含有少于 n 个单项式，从而我们可能无法论证非零多项式 Q的存在。为应对这一点，我们现在不再要求 Q 具有特殊形式 $Q(X, Y) = A(X) + B(X) \cdot Y$，而只要求 Q具有较低的 $(1, k)$-加权次数，这有可能增加 Q中单项式的个数。事实证明，这一改变确实足以使一致参数 t 显著小于唯一译码设定中的取值。我们还需要确保，当 Q 具有这种一般形式时，求根步骤能够高效执行。

接下来，我们分别介绍插值步骤和求根步骤所做的改动，并分析其正确性和效率。

步骤 1：插值。 在这一步中，我们现在希望求出一个非零二元多项式 $Q(X, Y) \in \mathbb{F}_q[X, Y]$，其 $(1, k)$-加权次数较低，并且对任意 $i \in [n]$，都有 $Q(a_i, w_i) = 0$。与唯一译码设定不同，现在我们不对 Q 施加任何额外的结构要求，只要求它满足加权次数限制。下面的引理表明，存在这样一个非零多项式 Q ，其 $(1, k)$-加权次数远小于唯一译码设定中的次数。

引理 3.4。 存在一个定义在 $\mathbb{F}_q$ 上的非零二元多项式 $Q(X, Y)$，其 $(1, k)$-加权次数至多为 $\sqrt{2kn}$，并且对任意 $i \in [n]$，都满足 $Q(a_i, w_i) = 0$ 。此外，可以通过求解一个线性方程组找到这样的多项式$Q(X, Y)$：将 $Q(X, Y)$ 中单项式的系数视为未知数，并将形如 $Q(a_i, w_i) = 0$ 的每个要求视为关于这些未知数的齐次线性约束。

证明。 如果我们将 Q 中单项式的系数视为未知数，那么每个形如 $Q(a_i, w_i) = 0$ 的要求都会对这些未知数施加一个齐次线性约束。因此，只需证明 Q 中单项式的数量大于线性约束 n 的数量，这样该线性系统就有非零解。

令 M 表示 $Q(X, Y)$ 中单项式的数量，并为简单起见，假设 $\ell := \sqrt{2n/k}$ 是整数。首先注意， 根据我们对 $\deg^{(1,k)}(Q) \le \ell \cdot k$ 的要求， $Q(X, Y)$ 中 Y 变量的次数可以是任意 $j \in \{0, 1, \ldots, \ell\}$；对于其中 Y 变量的次数为 j 的任意单项式， X 变量的次数可以是任意 $i \in \{0, 1, \ldots, k(\ell - j)\}$。因此我们有

$$M = \sum_{j=0}^{\ell} (k\ell - kj + 1) = \left(\frac{k\ell}{2} + 1\right) \cdot (\ell + 1) > \frac{k\ell^2}{2} = n.$$

我们得出结论： Q 中的未知系数数量多于线性约束的数量n，因此存在一个满足该引理要求的非零多项式 Q。 □

[2]回顾一下，对于向量 $\mathbf{b} \in \mathbb{N}^m$，多项式 $f(\mathbf{X}) = \sum_{\mathbf{i}} f_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathbb{F}[\mathbf{X}]$ 的 $\mathbf{b}$-加权次数 $\deg_{\mathbf{b}}(f)$ 是满足 $f_{\mathbf{i}} \neq 0$ 的各个 $\mathbf{i}$ 对应的加权和 $\sum_j \mathbf{b}_j \cdot \mathbf{i}_j$ 中的最大值。

步骤 2：求根。 在这一步中，我们希望求出所有满足 $Q(X, f(X)) = 0$ 的单变量多项式 $f(X) \in \mathbb{F}_q[X]$；并且希望证明，任何次数小于 k 且满足 $f(a_i) = w_i$ 的单变量多项式 $f(X) \in \mathbb{F}_q[X]$，只要其满足条件的指标至少有 $t = \sqrt{2kn} + 1$ 个 $i \in [n]$，就满足 $Q(X, f(X)) = 0$。

引理 *3.5.* 假设 $Q(X, Y)$ 是 $\mathbb{F}_q$ 上的非零二元多项式，且满足 $\deg^{(1,k)}(Q) \leq \sqrt{2kn}$，并且对任意 $i \in [n]$ 都有 $Q(a_i, w_i) = 0$。设 $f(X) \in \mathbb{F}_q[X]$ 是次数小于 k 的一元多项式，使得对至少 $\sqrt{2kn} + 1$ 个指标 $i \in [n]$，都有 $f(a_i) = w_i$。那么 $Q(X, f(X)) = 0$。

证明。 根据假设 $\deg^{(1,k)}(Q) \leq \sqrt{2kn}$，多项式 $P_f(X) := Q(X, f(X)) \in \mathbb{F}_q[X]$ 是一个次数至多为 $\sqrt{2kn}$ 的一元多项式。此外，对于满足 $f(a_i) = w_i$ 的任意 $i \in [n]$，它还满足 $Q(a_i, f(a_i)) = Q(a_i, w_i) = 0$。因此，$P_f(X)$ 是一个次数至多为 $\sqrt{2kn}$、至少有 $\sqrt{2kn} + 1$ 个根的一元多项式，所以它必定是零多项式。 □

为确保当 Q 具有一般形式时，能够高效地执行求根步骤，我们需要证明，满足 $Q(X, f(X)) = 0$ 的次数小于 k 的多项式 $f(X)$ 数量不多，并且能够高效地找到这些多项式。为此，我们注意到以下事实。

引理 3.6. 设 $Q(X, Y)$ 是 $\mathbb{F}_q$ 上的一个非零二元多项式，且 $f(X) \in \mathbb{F}_q[X]$ 是一个一元多项式，使得 $Q(X, f(X)) = 0$。那么，在双变量多项式环 $\mathbb{F}_q[X, Y]$ 中，$Y - f(X)$ 整除 $Q(X, Y)$。

证明。 令 D 为 Q 中 Y 的次数。因此，我们可以将 Q 写成 $Q(X, Y) = \sum_{i=0}^{D} Q_i(X) Y^i$。显然，$Q(X, f(X))$ 等于 $\sum_{i=0}^{D} Q_i(X)(f(X))^i$。因此，

$$Q(X, Y) - Q(X, f(X)) = \sum_{i=1}^{D} Q_i(X)(Y^i - f(X)^i)\,.$$

对于每个正整数 i，我们注意到 $(Y^i - f(X)^i)$ 可分解为 $(Y - f(X))(Y^{i-1} + Y^{i-2} f(X) + \cdots + Y f(X)^{i-2} + f(X)^{i-1})$。换句话说，和式 $\sum_{i=1}^{D} Q_i(X)(Y^i - f(X)^i)$ 中的每一项都可被 $(Y - f(X))$ 整除，而且商是关于 $\mathbb{F}_q[X, Y]$ 的多项式。因此，$Q(X, Y) - Q(X, f(X))$ 在 $\mathbb{F}_q[X, Y]$ 上可被 $(Y - f(X))$ 整除。所以，若 $f(X)$ 满足 $Q(X, f(X))$ 为零，则可得 $Q(X, Y)$ 在 $\mathbb{F}_q[X, Y]$ 上可被 $(Y - f(X))$ 整除。 □

因此，为了求出所有满足 $Q(X, f(X)) = 0$ 的一元多项式 $f(X) \in \mathbb{F}_q[X]$，只需对 $Q(X, Y)$ 进行因式分解；利用已知的二元/多元多项式因式分解算法，可以在多项式时间内完成此操作。我们在以下定理中概述所需的结果，并请参阅文献及 [Gur06b，第 4 节5]，了解该算法的描述。

定理3.7（二元因式分解 [Kal85, Len85]）。设 $\mathbb{F}$ 是任意有限域。那么，存在一种随机算法，以二元多项式 $Q(X, Y) \in \mathbb{F}[X, Y]$ 为输入，并输出其所有形如 $Y - f(X)$ 的因子，其中 $f \in \mathbb{F}[X]$，运行时间为 $\mathrm{poly}(\log(|\mathbb{F}|), \deg(Q))$。

算法的完整描述如下图 2 所示，随后是正确性和效率分析。

$\mathrm{RS}_q(a_1, \ldots\ldots, a_n; k)$**的列表译码：**

• **输入：** $w \in \mathbb{F}_q^n$。

•输出：所有次数小于 k 的多项式 $f(X)$ 的列表 $\mathcal{L}$，使得对于至少 $\sqrt{2kn+1}$ 个指标 $i \in [n]$，$f(a_i) = w_i$。1. 求一个非零二元多项式 $Q(X,Y)$，其系数属于 $\mathbb{F}_q$，且 $(1,k)$-加权次数至多为 $\sqrt{2nk}$，并满足：对于任意 $i \in [n]$，$Q(a_i, w_i) = 0$。可以通过求解一个线性方程组来求得这样的多项式 $Q(X,Y)$：将 $Q(X,Y)$ 中单项式的系数视为未知数，并将每个形如 $Q(a_i, w_i) = 0$ 的要求视为关于这些未知数的齐次线性约束。2. 求所有一元多项式 $f(X)$ 的列表 $\mathcal{L}'$，使得 $Q(X, f(X)) = 0$。具体做法是使用定理3.7中的算法对 $Q(X,Y)$ 进行因式分解，并将所有满足 $Y - f(X)$ 是 $Q(X,Y)$ 的因子的单变量多项式 $f(X)$ 加入 $\mathcal{L}'$。3. 输出所有对应于一元多项式 $f(X)$ 的码字（$f(a_1)$ $f(a_2)$.....，$f(a_n)$）的列表 $\mathcal{L}$。这些多项式的次数小于 k（$\in \mathcal{L}'$），并且对于至少 $\sqrt{2nk+1}$ 个指标 $i \in [n]$，满足 $f(a_i) = w_i$。

图 2：里德-所罗门码的列表译码

正确性。 假设 $f(X) \in \mathbb{F}_q[X]$ 是一个次数小于 k 的一元多项式，使得对于至少 $\sqrt{2nk+1}$ 个指标 $i \in [n]$，$f(a_i) = w_i$，我们将证明 $f(X) \in \mathcal{L}$。根据引理 3.4，存在一个非零二元多项式 $Q(X, Y)$，满足步骤 1 的要求。根据引理 3.5，我们有 $Q(X,\ f(X)) = 0$；而由引理 3.6 可知，进而 $Y - f(X)$ 整除 $Q(X,\ Y)$，因此 $f(X)$ 将被纳入步骤 2 的 $\mathcal{L}'$ 中。显然，$f(X)$ 也会通过步骤 3 的检查，因此 $f(X)$ 也会被纳入 $\mathcal{L}$。

效率。 步骤 1 可以通过高斯消元求解一个含有 $O(n)$ 个变量的 n 个线性方程组，在 poly(n，log(q)) 时间内完成。根据定理3.7中的算法，步骤 2 可以在 poly(n，log(q)) 时间内完成。显然，步骤 3 也可以在 poly(n，log(q)) 时间内完成。

3.3 Reed-Solomon 码的列表译码达到 Johnson界

本节将介绍一种高效算法，用于对 Reed-Solomon 码进行列表译码，使其达到 *Johnson*界（参见定理 2.1）。

再次设 q 为素数幂，$a_1, \ldots, a_n \in \mathbb{F}_q$ 为互不相同的求值点，$k < n$ 为正整数，并令 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 为相应的 Reed-Solomon 码。设 $w \in \mathbb{F}_q^n$ 是一个接收字。我们将说明如何计算满足以下条件的所有多项式 $f(X) \in \mathbb{F}_q[X]$ 的列表：其次数小于 k，且对于至多 $e := n - \sqrt{kn} - 1$ 个指标 $i \in [n]$，有 $f(a_i) \neq w_i$。也就是说，对于至少 $t := n - e = \sqrt{kn} + 1$ 个指标 $i \in [n]$，有 $f(a_i) = w_i$。

特别地，若令 $R := \frac{k}{n}$ 表示 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 码的码率，则该算法将能够从最多大约 $(1 - \sqrt{R})$ 的错误比例进行列表译码。这大致将上一节所讨论算法所需的一致削减了 $\sqrt{2}$ 倍，并与定理 2.1 的 Johnson 界相吻合（回顾到 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 码的相对距离 δ 满足

$R \leq 1-\delta$）。

概述。该算法建立在我们之前所见算法的思想之上，并为该框架增加了一项新的技术要素，即重数方法。为描述这一思想，我们首先简要回顾上一节中算法的高层概要。

图 2 中的算法本质上是通过求一个非零且次数较低（按某种适当的意义而言）的二元多项式 $Q(X, Y)$ 来实现的，该多项式具有以下性质：对于每个次数小于 k 的多项式 $f(X)$，如果接收字的 i^{th} 位置 w_i 满足 $w_i = f(a_i)$，那么一元多项式$P_f(X) := Q(X, f(X))$ 在 a_i 处有一个零点。因此，对于编码与接收字 w 接近的某个 f，一元多项式 P_f 有许多不同的零点；如果此类相符的数量超过 P_f 的次数（至多为 Q 的 $(1, k)$ 加权次数），那么 P_f 必定恒等于零；等价地，$f(X)$ 必定是 Q 的根（将 Q 视为关于不定元 Y 的一元多项式，其系数来自一元多项式环 $\mathbb{F}_q[X]$）。

多项式 Q 是通过求解关于其系数的适当线性系统得到的，该线性系统保证对于任意 i，都有 $Q(a_i, w_i) = 0$；同时，我们需要将 Q 的次数设得不能太低，以保证存在非零解。另一方面，Q 的次数也不能太高，这一点同样至关重要，因为该算法要奏效，所需的相符数量下限本质上比 P_f 的次数大一，因此 Q 的次数越低，容错能力就越高。这两项彼此牵制的要求决定了算法成功所需的定量界限。

从较高层面来看，使我们能够容忍更多错误的主要新想法，是在插值步骤中求得一个 $Q(X, Y)$，并赋予它更强的性质：如果多项式 $f(X)$ 与接收字 w 在某个位置 i 上相符，即 $f(a_i) = w_i$，那么一元多项式 $P_f(X)$ 在 a_i 处具有高重数零点，也就是说，对于足够大的参数 r，当 $j = 0$ 为 $0, \ldots, r-1$ 时，$P_f^{(j)}(a_i) = 0$，其中 $P^{(j)} f(X)$ 表示第 j 阶 Hasse 导数（参见第 2.2 节）。直观上，这似乎意味着，为了确保 $P_f(X)$ 恒等于零，我们现在只需要 f 与 w 之间更少的一致。为了得到满足这一性质的非零二元多项式 $Q(X, Y)$，其思路是强化插值步骤，寻找一个 $Q(X, Y)$，使它在每个点 (a_i, w_i) 处（实质上）都具有足够高的重数零点。由于这一过程中约束的数量增加了，为了使该方程组存在非零解，我们现在需要使用 $(1, k)$-加权次数稍高的二元多项式 $Q(X, Y)$。

再一次，这两个步骤彼此存在冲突——如果 Q 的 $(1, k)$-加权次数不是太低，插值步骤就很可能成功；而要使 $P_f(X)$ 对次数小于 k 且编码接近 w 的多项式 $f(X)$ 恒等于零，则有助于降低 P_f 的次数，而 P_f 的次数至多为 Q 的 $(1, k)$-加权次数。事先并不清楚，采用这种方法得到的定量界限是否会优于上一节所介绍的图 2 中算法所得的界限。然而，正如我们将看到的，事实确实如此，而且新算法的列表译码能力一直达到 Johnson界。

现在我们正式描述该算法的主要步骤。

步骤 1：插值。下面的引理是上一节引理 3.4 的高重数变体。

引理 3.8。存在一个非零二元多项式 $Q(X, Y)$，其系数属于 $\mathbb{F}_q$，且具有至多为 $\sqrt{kn}(r+1)r$ 的 $i \in [n]$，Q - 加权次数，使得对于每个 $i \in [n]$，Q，它在 (a_i, w_i) 处的重数至少为 r。此外，这样的多项式 $Q(X, Y)$ 可以通过求解一个线性方程组得到：将 $Q(X, Y)$ 中单项式的系数视为未知数，并将 Q 的每个 *Hasse* 导数的零点约束视为关于这些未知数的齐次线性约束。

证明。 证明过程与引理 3.4 的证明基本相同，后者对应于 $r = 1$ 情形。我们将 Q 的系数视为变量，并注意到 Q 的任意 Hasse 导数在 $(a_i,\ w_i)$ 处为零这一性质，恰好是关于 Q 的系数的齐次线性约束。因此，如果对参数进行设置，使未知数的数量多于约束的数量，那么该线性方程组必然存在非零解。因此，为完成证明，我们只需计算线性系统中的变量数和约束数。

次数小于 r 的二元多项式的Hasse导数个数，等于两个变量中总次数至多为$(r-1)$的单项式个数，该个数至多为 $\binom{r+1}{2}$。因此，对每个$i \in [n]$，我们有 $\binom{r+1}{2}$ 个齐次线性约束，总共得到 $n\binom{r+1}{2}$ 个约束。设 D 为一个参数（即将设定），它表示 $Q(X,Y)$的$(1,k)$-加权次数。若 D 足够大，使得 $(1,k)$-加权次数至多为 D 的二元单项式个数超过 $n\binom{r+1}{2}$，则上述齐次线性系统的变量数多于约束数，因而存在非零解。因此，按照与引理 3.4相同的计算（取$\ell = \frac{D}{k}$），只需选择 D 使得

$$\frac{(D+2)(D+k)}{2k} > n\binom{r+1}{2}.$$

令 D 等于 $\sqrt{kn(r+1)r}$（为简单起见，我们假设它是整数），即可满足此约束。

□

步骤 2：求根。 现在我们说明，任何次数小于 k 的多项式 $f(X)$，如果其编码与接收字 w 有较大的一致度，就满足 $Q(X, f(X))$ 恒等于零。为此，我们先观察到，如果 $Q(X,Y)$ 在点 $(a_i, f(a_i))$ 处以至少 r 重数为零，那么 $P_f(X) := Q(X, f(X))$ 在 a_i 处以至少 r 重数为零。

断言 3.9。设 $Q(X,Y) \in \mathbb{F}_q[X,Y]$ 和 $f(X) \in \mathbb{F}_q[X]$ 是多项式，并令 $P_f(X) := Q(X, f(X))$。假设 $Q(X,Y)$ 在某个点 $(a, f(a))$ 处为零，其中某个 $a \in \mathbb{F}_q$ 的重数至少为 r。那么 $P_f(X)$ 在 a 处的重数至少为 r。

证明。 该结论可由哈斯导数链式法则的标准应用得出。具体来说，回顾哈斯导数的定义可知

$$f(a+Z) = \sum_{i=0}^{k-1} f^{(i)}(a) Z^i = f(a) + Z \cdot \tilde{f}(Z),$$

对于某个 $\tilde{}$ 一元多项式 $f(Z)$。根据哈斯导数的定义，我们还可以得到

$$P_f(a+Z) = Q(a+Z, f(a) + Z\cdot\tilde{f}(Z)) = \sum_{u,v} Q^{(u,v)}(a, f(a)) Z^{u+v} \tilde{f}(Z)^v .$$

现在，根据假设，Q 在 $(a,\ f(a))$ 处所有阶数小于 r 的哈斯导数均为零，因此有

$$P_f(a+Z) = \sum_{u,v\in\mathbb{Z}_{\geq 0}: u+v\geq r} Q^{(u,v)}(a, f(a)) Z^{u+v} \tilde{f}(Z)^v .$$

因此，Z 中可能在 $P_f(a+Z)$里具有非零系数的单项式的最低次数至少为 r，从而根据重数的定义，我们得到 P_f 在 a 处的重数至少为 r。 □

下面的引理类似于上一节中的引理 3.5。

引理 *3.10*。设 $Q(X,Y)$是 $\mathbb{F}_q$ 上的一个非零二元多项式，满足对 $r = 2kn$有$\deg^{(1,k)}(Q) \leq \sqrt{kn(r+1)}r$。进一步设 Q 在每个点(a_i, w_i)（对$i \in [n]$）上以至少 r的重数消失。设 $f(X) \in \mathbb{F}_q[X]$ 是次数小于 k的一元多项式，使得对至少$\sqrt{nk}+1$ 个指标 $i \in [n]$有 $f(a_i) = w_i$。则 $Q(X, f(X)) = 0$。

证明。由 Q 的 $(1,k)$-加权次数上界可知， $P_f(X) := Q(X, f(X))$ 是一个次数至多为 $D := \sqrt{kn(r+1)}r$ 的一元多项式。由断言 3.9 可知，对任意 $i \in [n]$，若 $f(a_i) = w_i$，则 P_f 在 a_i 处具有重数至少为 r 的零点。因此，若 f 与 w 在多于 $\frac{D}{r} = \frac{\sqrt{kn(r+1)}r}{r} = \sqrt{nk}(1+\frac{1}{r})$ 个互异的 a_i 上一致，则由事实 2.3 可知 P_f 必恒为零。对于充分大的 r，例如 $r \geq kn$，我们有 $\sqrt{nk}(1+\frac{1}{r}) < \sqrt{nk}+1$。因此，通过选取足够大的 r （例如 $r = 2kn$），可得多于 $\sqrt{nk}$ 个相符便足以使 P_f 恒为零。 □

因此，与上一节一样，我们得到：任何次数小于 k 且与 w 有较高一致度的一元多项式，都是 $Q(X, Y)$的一个根，并可利用定理3.7恢复。再一次，列表译码算法的时间复杂度关于输入规模是多项式有界的，因为主要步骤仅涉及求解一个规模为多项式有界的线性系统，以及一种特殊情形的二元多项式因式分解。该算法的完整描述见下方图 9。

对$\mathrm{RS}_q(a_1, \ldots\ldots, a_n; k)$**进行列表译码至Johnson界：**

令 $r := 2nk$。

- **输入：** $w \in \mathbb{F}_q^n$。

•输出：列表 $\mathcal{L}$，包含所有次数小于 k的多项式 $f(X) \in \mathbb{F}_q[X]$，使得 $f(a_i) = w_i$对至少$\sqrt{nk}+1$ 个指标 $i \in [n]$成立。1. 求一个非零二元多项式 $Q(X,Y)$，其系数属于 $\mathbb{F}_q$，$(1,k)$-加权次数至多为 $\sqrt{nk}(r+1)r$，且满足：对于任意 $i \in [n]$以及任意满足 $u+v<r$的 $u, v \in \mathbb{N}$，都有 $Q_{(u,v)}(a_i, w_i) = 0$。这样的多项式 $Q(X,Y)$可通过求解一个线性方程组得到：将 $Q(X,Y)$中单项式的系数视为未知数，并将形如 $Q_{(u,v)}(a_i, w_i) = 0$ 的每个条件视为关于这些未知数的齐次线性约束。2. 求列表 $\mathcal{L}'$，其中包含所有满足 $Q(X, f(X)) = 0$ 的一元多项式 $f(X)$：使用定理3.7中的算法对 $Q(X,Y)$进行因式分解，并将所有满足 $Y - f(X)$是 $Q(X,Y)$的一个因子的单变量多项式 $f(X)$纳入 $\mathcal{L}'$。3. 输出列表 $\mathcal{L}$，其中包含与满足 $f(a_i) = w_i$ 对至少$\sqrt{nk}+1$ 个指标 $i \in [n]$成立的次数小于 k 的单变量多项式 $f(X) \in \mathcal{L}'$ 相对应的所有码字$(f(a_1)\ f(a_2)\ldots\ldots,\ f(a_n))$。

图3：里德-所罗门码的列表译码可达 Johnson 界

3.4 Johnson 界之外里德-所罗门码列表译码的局限性

在上一节中，我们证明了 Reed-Solomon 码可以高效地列表译码至 Johnson界。也就是说，我们给出了一种算法，可以高效地输出所有次数小于 k的多项式

这些多项式的编码与接收字在至少 $\sqrt{R}n$个点上一致。本节将给出 Reed-Solomon 码列表大小的一个组合下界，该下界表明，通常情况下，Reed-Solomon 码对于一致度略低的 $R^{\frac{1}{2}+\epsilon}n$是不可列表可译码的，且列表大小关于 n是多项式级的。这进而意味着，不存在能够将 Reed-Solomon 码列表译码至这一一致度的多项式时间算法，特别是无法从任意接近 R的一致度进行列表译码。该界是以下定理的推论。

定理 3.11。 对于任意的 $\gamma \in (0,\ 1)$、$\beta \in (\gamma,\ \sqrt{\gamma})$、充分大的整数 m 以及 $n = 2^m$，存在一个字 $w \in (\mathbb{F}_n)^n$，使得在 $\mathrm{RS}_n(n^\gamma)$ 中，至少有 $n^{(\gamma-\beta^2)\log(n)}$ 个码字与 w 在至少 n^β 个位置上相同。

在上述引理中设 $\gamma := 1 - \epsilon$，且 $\beta := (\frac{1}{2} - \epsilon) + \gamma(\frac{1}{2} + \epsilon)$（注意 $\beta \in (\gamma, \sqrt{\gamma})$），可知对于无穷多个 n，存在一个字 $w \in (\mathbb{F}_n)^n$，使得 $\mathrm{RS}_n(k)$ 中存在超多项式数量的码字与 w 在至少 $n^{\frac{1}{2}-\epsilon}k^{\frac{1}{2}+\epsilon} = R^{\frac{1}{2}+\epsilon}n$ 个位置上相同，其中 $k = n^{1-\epsilon}$。

上述定理 3.11 的证明基于子空间多项式，其定义如下。

定义 3.12（子空间多项式）。 令 $V \subseteq \mathbb{F}_{2^m}$ 为 $\mathbb{F}_{2^m}$的一个 $\mathbb{F}_2$-线性子空间。V的子空间多项式 定义为 $P_V(X) := \prod_{v \in V}(X - v)$。

我们将使用子空间多项式的两个主要性质：一方面，它们有相对较多的根（整个子空间V）；另一方面，这些多项式相当稀疏，如下面的断言所示。

断言 3.13 $V \subseteq \mathbb{F}_{2^m}$ $\mathbb{F}_2$ $\mathbb{F}_{2^m}$ d $b_0\ b_1\ \ldots\ b_{d-1} \in$。。设是的一个线性子 $\mathbb{F}_{2^m}$ $P_V\ X = X^{2^d} + \sum_{i=0}^{d-1} b_i X^{2^i}$. 空间，其维数为。那么存在、、，使得()

证明。对于一个非负整数 i，令 $f_i(X) : V \to \mathbb{F}_{2^m}$表示由 $f_i(v) := v^{2^i}$给出的 $\mathbb{F}_2$-线性函数，其中 $v \in V$。接下来注意，从 V到 $\mathbb{F}_{2^m}$ 的 $\mathbb{F}_2$-线性函数构成一个维数为 d的 $\mathbb{F}_{2^m}$-线性子空间，因此 f_0、f_1、…、f_d必定线性依赖且不全为零。也就是说，存在标量 b_0、b_1、…、$b_d \in \mathbb{F}_{2^m}$，它们不全为零，使得 $P(X) := \sum_{i=0}^{d} b_i f_i(X) = \sum_{i=0}^{d} b_i X^{2^i}$ 在任意 $v \in V$ 上取值均为零。此外，由于 V 有 2^d 个元素，我们必有 $\deg(P(X)) = 2^d$，并且还可以假设 $P(X)$是首一多项式。因此，$P(X)$和 $P_V(X)$是两个次数为 2^d且在 V的全部 2^d个元素上都取值为零的首一多项式，所以必有 $P_V(X) = P(X) = X^{2^d} + \sum_{i=0}^{d-1} b_i X^{2^i}$（因为 $P(X) - P_V(X)$是一个次数小于 2^d且至少有 2^d个根的多项式，因此必定是零多项式）。

□

现在我们转向上述定理 3.11 的证明。

定理 *3.11* 的证明。 令 $\gamma \in (0, 1)$，$\beta \in (\gamma, \sqrt{\gamma})$，设 m为充分大的整数。令 $\mathcal{V}$为由维数为 βm的 $\mathbb{F}_2$-线性子空间 $V \subseteq \mathbb{F}_{2^m}$ 构成的集合。那么 $\mathcal{V}$ 的大小为 $\prod_{i=0}^{\beta m-1} \frac{2^m - 2^i}{2^{\beta m} - 2^i} \geq 2^{\beta(1-\beta)m^2}$（因为要在 ~~$\mathbb{F}_{2^m}$~~中选取一个维数为 d的子空间 V，对于每个 $i = 0, 1, \ldots, d-1$，我们都需要选取一个不属于此前所有 i 个向量的线性张成空间的向量；此外，还需要除以在 V中选取 d个线性无关向量的选项数）。此外，根据断言 3.13，对于每个$V \in \mathcal{V}$，存在 $b_0, b_1, \ldots, b_{\beta m-1} \in \mathbb{F}_{2^m}$，使得 $P_V(X) = X^{2^{\beta m}} + \sum_{i=0}^{\beta m-1} b_i X^{2^i}$。

根据鸽巢原理，存在 $b_{\gamma m+1}, b_{\gamma m+2}, \ldots, b_{\beta m-1} \in \mathbb{F}_{2^m}$，使得对于 $i = \gamma m+1, \ldots, \beta m-1$，满足其系数为 b_i 的子空间多项式 $P_V(X)$ 的数量至少为 $2^{\beta(1-\beta)m^2}/2^{(\beta-\gamma)m^2} \geq 2^{(\gamma-\beta^2)m^2}$。令 $\mathcal{V}' \subseteq \mathcal{V}$ 表示满足 $P_V(X)$ 具有此性质的子空间 $V \in \mathcal{V}$ 的子空间族。

令 $P(X) := \sum_{i=\gamma m+1}^{\beta m-1} b_i X^{2^i}$，并令 $w \in (\mathbb{F}_n)^n$ 为 $P(X)$ 在 $\mathbb{F}_{2^m}$ 上的求值表，其中 $n = 2^m$。对于 $V \in \mathcal{V}'$，令 $P'_V(X) = P_V(X) + P(X)$。那么，对于 $V \in \mathcal{V}'$，多项式 $P'_V(X)$ 构成一个包含 $2^{(\gamma-\beta^2)m^2} = n^{(\gamma-\beta^2)} \log(n)$ 个不同多项式的族，其次数至多为 $2^{\gamma m} = n^{\gamma}$。此外，对于每个 $V \in \mathcal{V}'$，$P'_V(X)$ 在 V 的所有 $2^{\beta m} = n^{\beta}$ 个元素上都与 $P(X)$ 一致。由此可得，$\mathrm{RS}_n(n^{\gamma})$ 中至少有 $n^{(\gamma-\beta^2)} \log(n)$ 个码字（即对于 $V \in \mathcal{V}'$，$P'_V(X)$ 在 $\mathbb{F}_{2^m}$ 上的求值），它们在至少 n^{β} 个位置上与 w 一致。□

3.5 文献注记

最早的高效 Reed-Solomon 码唯一译码算法由 Peterson [Pet60],Gorenstein 和 Zierler [GZ61], Berlekamp [Ber68b], 以及 Massey [Mas69]提出。第 3.1 节所述的 Reed-Solomon 码唯一译码算法归功于 Berlekamp 和 Welch [BW87],，其讲解基于 Gemmell 和 Sudan [GS92] 的论述（另见 [GRS，第 12.1] 节）。第 3.2 节所述的超出唯一译码半径的 Reed-Solomon 码列表译码算法归功于 Sudan [Sud97],，而达到 Johnson 界的 Reed-Solomon 码列表译码算法则归功于 Guruswami 和 Sudan [GS99]（另见 [Gur06b，第 4] 节，以及 [GRS，第 12.2] 节）。

列表译码 Reed-Solomon 码所用的求根算法（定理3.7）源自更一般的双变量（及多变量）多项式因式分解算法，例如 Kaltofen [Kal85] 和 Lenstra [Len85]的相关研究。

第 3.4 节介绍了 Reed-Solomon 码在 Johnson 界之外进行列表译码的局限性，这一局限性由 Ben-Sasson、Kopparty 和 Radhakrishnan [BKR10] 发现。

4 达到容量的算法列表译码

在上一节中，我们介绍了用于对 Reed-Solomon 码进行列表译码的高效（多项式时间）算法，其译码范围达到 *Johnson* 界；我们还指出，通常 Reed-Solomon 码无法在远超 Johnson 界的范围内进行列表译码，尤其无法达到容量。

本节介绍对 Reed-Solomon 码的变体进行列表译码的算法，其译码范围达到容量。具体而言，在第 4.1 节和第 4.2 节中，我们介绍了对重数码进行列表译码直至达到容量的高效算法；在第 4.3 节中，我们还将证明，类似的算法可用于对采用子域求值点的 Reed-Solomon 码进行列表译码，且所需时间为稍具实质意义的次指数时间。特别是，这些算法表明，重数码在容量处的列表大小至多为码长的多项式级，而采用子域求值点的 Reed-Solomon 码的列表大小至多为码长的次指数级。在第 5 节中，我们将介绍这些码的列表大小的组合上界，从而有效地将列表大小降至一个与码长无关的常数。

4.1 超越唯一译码半径的重数码列表译码

接下来，我们将介绍针对 重数码族进行列表译码的高效（多项式时间）算法。这类码通过对多项式求值并计算其导数 来扩展 Reed-Solomon 码，且可达到容量。为此，本节先介绍一个简单的列表译码算法作为热身。该算法类似于第 3.1 节中针对 Reed-Solomon 码的唯一译码 算法，可对重数码进行超出唯一译码半径的列表译码。然后，在第 4.2 节中，我们将证明，为该算法加入重数（与第 3.3 节中介绍的、针对 Reed-Solomon 码的达到 *Johnson*界的列表译码算法类似），便可得到一个能够对重数码进行达到容量的列表译码算法。

下文中，固定一个素数幂 q、互不相同的求值点 $a_1, \ldots, a_n \in \mathbb{F}_q$，以及正整数$s, k$，使得 $k < sn$。回顾一下，重数码 $\mathrm{MULT}_q^{(s)}(a_1, \ldots, a_n; k)$ 是这样一种码：它将每个次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$ 关联到一个码字 $(f^{(<s)}(a_1) \ldots, f^{(<s)}(a_n)) \in (\mathbb{F}_q^s)^n$；其中，对于 $a \in \mathbb{F}_q$, $f^{(<s)}(a) = (f(a)\ f^{(1)}(a) \ldots, f^{(s-1)}(a))$。为简便起见，下文假设 $\max\{k, s\} \leq \mathrm{char}(\mathbb{F}_q)$。设 $w \in (\mathbb{F}_q^s)^n$ 是一个接收字，其中对于任意 $i \in [n]$, $w_i = (w_{i,0}, \ldots, w_{i,s-1}) \in \mathbb{F}_q^s$。我们将给出一个运行时间约为 q^s 的算法，用于计算所有次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$ 的列表，使得对于至多 $e := s \cdot (n-k+1)_{s+1}$ 个指标 $i \in [n]$，有 $f^{(<s)}(a_i) \neq w_i$。也就是说，对于至少 $t := n - e = \frac{n+s}{s+1}(k-1+1)$ 个指标$i \in [n]$，有 $f^{(<s)}(a_i) = w_i$。

注意，$s = 1$ 的特殊情形对应于第 3.1 节中介绍的 Reed-Solomon 码唯一解码算法。此外，若令 $R := \frac{k}{s \cdot n}$ 表示 $\mathrm{mult}_q^{(s)}(a_1, \ldots..., a_n; k)$ 码的码率,那么该算法能够在大约 q^s 的时间内，对错误比例最高约为 $\frac{s}{s+1}(1 - s \cdot R)$ 的情形进行列表译码。可以验证，对于任意 $s > 1$ 和 $R \leq \frac{1}{3s}$，这都严格大于 $\frac{1-R}{2}$ 的唯一译码半径。此外，对于任意常数 s 和 $q = \mathrm{poly}(n)$，运行时间（以及列表大小）都是码长的多项式。

概述。回顾里德-所罗门码的唯一解码算法（算法 1），其中解码算法分为两个主要步骤：插值步骤中，我们寻找一个非零的低次二元多项式 $Q(X, Y) \in \mathbb{F}_q[X, Y]$，其形式为 $Q(X, Y) = A(X) + B(X) \cdot Y$，使得对于任意 $i \in [n]$，都有 $Q(a_i, w_i) = 0$；而求根步骤中，我们寻找满足 $Q(X, f(X)) = 0$ 的一元多项式 $f(X) \in \mathbb{F}_q[X]$。

此外，我们从 Q 中所需的主要性质是：Q 中的未知系数数量大于形如 $Q(a_i, w_i) = 0$的约束数量 n；并且 Q 的 $(1, k)$ 加权次数 $\deg^{(1,k)}(Q)$ 小于一致参数 t。第一个性质保证存在一个非零 Q;第二个性质则保证，对于任意次数小于 k的一元多项式 $f(X) \in \mathbb{F}_q[X]$，只要它对至少 t 个指标 $i \in [n]$满足 $f(a_i) = w_i$，那么 $Q(X, f(X))$ 是一个次数小于 t的一元多项式，它至少有 t 个根，因此 $Q(X, f(X)) = 0$。

在列表译码的设定中，我们希望一致参数 t 更小，这意味着要求 Q 的 $(1, k)$ 加权次数更小。因此，Q 可能包含少于n 个单项式，所以我们或许无法证明非零多项式 Q的存在。在超越唯一译码半径的 Reed-Solomon 码列表译码算法（算法 2）中，我们通过不再要求 Q 具有 $Q(X, Y) = A(X) + B(X) \cdot Y$的形式来解决这一问题，因为这种形式关于 Y是线性的，而放宽这一要求有可能增加 Q中的单项式数量。对于超越唯一译码半径的重数码列表译码，我们采用不同的方法:令 Q 为一个低次（$s+1$）元多项式 $Q(X, Y_0, \ldots, Y_{s-1})$，它关于 $Y_0, \ldots, Y_{s-1}$是线性的，这也有可能增加 Q中的单项式数量。

更具体地说，在插值步骤中，我们寻找一个非零的$(s+1)$元多项式$Q(X, Y_0, \ldots, Y_{s-1}) \in \mathbb{F}_q[X, Y_0, \ldots, Y_{s-1}]$，其形式为

$$Q(X, Y_0, \ldots, Y_{s-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{s-1}(X) \cdot Y_{s-1},$$

其$(1, k, \ldots, k)$-加权次数小于 t，使得 $Q(a_i, w_i) = 0$对任意 $i \in [n]$成立（其中我们将$w_i = (w_{i,0}, \ldots, w_{i,s-1}) \in \mathbb{F}_q^s$视为对$\mathbb{F}_q$中 s 个变量的赋值）。然后，在求根步骤中，我们寻找所有单变量多项式 $f(X) \in \mathbb{F}_q[X]$，使其满足 $Q(X, f(X)\ f_{(1)}(X) \ldots, f_{(s-1)}(X)) = 0$。

该分析类似于 Reed-Solomon 码唯一译码的算法，但证明中利用的一个关键点是，求解该微分方程的多项式 $f(X)$ 并不太多

$Q(X,\ f(X)\ f_{(1)}(X)\ldots,\ f^{(s-1)}(X))\ =0$。下面我们将分别描述插值和求根步骤，并分析其正确性和效率。

步骤 1：插值。在此步骤中，我们寻找一个非零的低次数 $(s+1)$ 元多项式$Q(X,Y_0,\ldots,Y_{s-1})$，使得对任意 $i\in[n]$ 都有 $Q(a_i,w_i)\ =0$。

引理 4.1. 设 $t=\frac{n+s}{s+1}$。则存在一个定义在 $\mathbb{F}_q$ 上、形如下式的非零 $(s+1)$ 元多项式 $Q(X,Y_0,\ldots,Y_{s-1})$

$$Q(X,Y_0,\ldots,Y_{s-1})=A(X)+B_0(X)\cdot Y_0+\cdots+B_{s-1}(X)\cdot Y_{s-1},$$

其中 $A(X)$ 的次数小于 t，且每个 $B_\ell(X)$ 的次数小于 $t-k+1$，并且满足对任意 $i\in[n]$ 都有 $Q(a_i,w_i)\ =0$（其中我们将 $w_i=(w_{i,0},\ldots,w_{i,s-1})\ \in\mathbb{F}_q^s$视为对 $\mathbb{F}_q$中 s 个变量的赋值）。

此外，这样的多项式 $Q(X,Y_0,\ldots,Y_{s-1})$ 可以通过求解一个线性方程组得到，该线性方程组是通过将 $A(X)\ B_0(X)\ldots,B_{s-1}(X)$ 中单项式的系数视为未知数，并将每个形如 $Q(a_i,w_i)$ 的要求视为对这些未知数的齐次线性约束而得到的。

证明。若将 $A(X)\ B_0(X)\ldots,B_{s-1}(X)$ 中各单项式的系数视为未知数，那么每个形如 $Q(a_i,w_i)\ =0$ 的条件都会对这些未知数施加一个齐次线性约束。还要注意，未知数的数量为

$$t+s\cdot(t-k+1)=(s+1)\cdot t-s\cdot(k-1)=n+1,$$

而线性约束的数量为 n，因此该线性系统存在非零解。 □

步骤 2：求根。在此步骤中，我们寻找所有次数小于 k 且满足微分方程的一元多项式 $f(X)\ \in\mathbb{F}_q[X]$

$$Q\left(X,f(X),f^{(1)}(X),\ldots,f^{(s-1)}(X)\right)=0,$$

我们希望证明，任何次数小于 k 且对于至少 t 个指标 $i\in[n]$，满足$f^{(<s)}(a_i)\ =w_i$ 的一元多项式 $f(X)\ \in\mathbb{F}_q[X]$，都满足上述微分方程。我们先从后者着手。

引理 4.2. 假设　设 $Q(X,Y_0,\ldots,Y_{s-1})$ 是一个形如以下形式的非零 $s+1)$ 元多项式，定义在 $\mathbb{F}_q$ 上

$$Q(X,Y_0,\ldots,Y_{s-1})=A(X)+B_0(X)\cdot Y_0+\cdots+B_{s-1}(X)\cdot Y_{s-1},$$

其中 $A(X)$ 的次数小于 t，且每个 $B_\ell(X)$ 的次数小于 $t-k+1$，并且满足对任意 $i\in[n]$ 有 $Q(a_i,w_i)\ =0$（其中我们将 $w_i=(w_{i,0},\ldots,w_{i,s-1})\ \in\mathbb{F}_q^s$视为对 $\mathbb{F}_q$ 中 s 个变量的赋值）。设 $f(X)\ \in\mathbb{F}_q[X]$ 是次数小于 k 的一元多项式，使得对至少 t 个指标 $i\in[n]$有 $f^{(<s)}(a_i)\ =w_i$。则

$$Q(X,f(X),f^{(1)}(X),\ldots,f^{(s-1)}(X))=0.$$

证明。多项式 $P_f(X):=\ Q(X,f(X)\ f_{(1)}(X)\ldots,f_{(s-1)}(X))$ 是次数小于 t的一元多项式，它满足

$$P_f(a_i)=Q(a_i,f(a_i),f^{(1)}(a_i),\ldots,f^{(s-1)}(a_i))=Q(a_i,w_i)=0$$

对于任意满足 $f^{(<s)}(a_i)\ =w_i$ 的 $i\in[n]$。因此，$P_f(X)$ 是次数小于 t 且至少有 t 个根的一元多项式，所以它必定是零多项式。 □

重数码列表译码算法中的一个主要新要素是下面这个引理，它给出了满足该微分方程的一元多项式 $f(X) \in \mathbb{F}_q[X]$ 的数量上界。

引理 4.3. 设 $Q(X, Y_0, \ldots, Y_{s-1})$ 是一个形如下式的、定义在 $\mathbb{F}_q$ 上的非零$(s+1)$元多项式

$$Q(X, Y_0, \ldots, Y_{s-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{s-1}(X) \cdot Y_{s-1},$$

并设 $\mathcal{L}$ 是由所有次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$ 组成的列表，使得

$$Q(X, f(X), f^{(1)}(X), \ldots, f^{(s-1)}(X)) = 0.$$

那么，若 $\max\{k, s\} \le \mathrm{char}(\mathbb{F}_q)$，则 $|\mathcal{L}| \le q^{s-1}$。

此外，$\mathcal{L}$ 构成 $\mathbb{F}_q$ 上一个维数至多为 $s-1$ 的仿射子空间。该子空间的一组基可以通过求解线性方程组得到：将 $f(X)$ 的系数视为未知数，并将要求 $Q(X, f(X)\ f^{(1)}(X) \ldots, f_{(s-1)}(X))$的每个系数均为零，视为关于这些未知数的（非齐次）线性约束。

证明。首先注意，若不存在满足 $Q(X, f(X)\ f(1)(X) \ldots, f(s-1)(X)) = 0$ 的多项式 $f(X) \in \mathbb{F}_q[X]$，则结论成立。因此，我们可以假设存在满足$Q(X, f(X)\ f(1)(X) \ldots, f^{(s-1)}(X)) = 0.$的多项式 $f(X) \in \mathbb{F}_q[X]$ 。接下来我们注意到，在这种情况下，$B_0(X) \ldots, B_{s-1}(X)$ 并非全为零。为此，反设 $B_0(X) \ldots, B_{s-1}(X)$ 全为零。那么根据假设 $Q(X, f(X)\ f(1)(X) \ldots, f^{(s-1)}(X)) = A(X) + \sum_{\ell=0}^{s-1} B_\ell(X) \cdot f(\ell)(X) = 0$，我们也有 $A(X) = 0$，进而推出 $Q(X, Y_0, \ldots, Y_{s-1}) = A(X) + \sum_{\ell=0}^{s-1} B_\ell(X) \cdot Y_\ell = 0$，这与 $Q(X, Y_0, \ldots, Y_{s-1})$ 非零的假设矛盾。不失一般性，我们还可以假设$B_{s-1}(X) \neq 0$；否则，我们就对使 $B_{s'}(X) \neq 0$ 成立的最大值 $s' < s$ 证明该结论，这也就推出了该结论对 s 成立。最后，由于 $B_{s-1}(X)$ 是定义在 $\mathbb{F}_q$ 上的非零多项式，存在一个元素 $a \in \mathbb{F}_q$，使得 $B_{s-1}(a) \neq 0$。关键观察如下。

断言 4.4。对于任意 $u \in \mathbb{F}_q^{s-1}$，存在唯一的次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$，使得$f_{(<s-1)}(a) = u$，且 $Q(X, f(X)\ f^{(1)}(X) \ldots, f_{(s-1)}(X)) = 0$。

证明。为证明这一点，固定 $u \in \mathbb{F}_q^{s-1}$，并令 $f(X) \in \mathbb{F}_q[X]$ 为一个次数小于 k 的多项式，使得 $f^{(<s-1)}(a) = u$，且

$$P_f(X) := Q(X, f(X), f^{(1)}(X), \ldots, f^{(s-1)}(X)) = A(X) + \sum_{\ell=0}^{s-1} B_\ell(X) \cdot f^{(\ell)}(X) = 0.$$

根据 Hasse 导数的定义，我们可以写成 $f(X) = \sum_{i=0}^{k-1} f_{(i)}(a) \cdot (X-a)^i$。因此，只需证明 $f_{(<s-1)}(a)$ 的取值可以确定其余导数 $f_{(s-1)}(a) \ldots, f_{(k-1)}(a)$。

为证明上述结论，我们首先计算 $P_f(X)$ 的导数。根据 Hasse 导数的性质（引理 2.4），对于任意 $j \in \mathbb{N}$，我们有：

$$\begin{aligned}
P_f^{(j)}(X) &= A^{(j)}(X) + \sum_{\ell=0}^{s-1} (B_\ell(X) \cdot f^{(\ell)}(X))^{(j)} \\
&= A^{(j)}(X) + \sum_{\ell=0}^{s-1} \sum_{h=0}^{j} B_\ell^{(j-h)}(X) \cdot (f^{(\ell)})^{(h)}(X) \\
&= A^{(j)}(X) + \sum_{\ell=0}^{s-1} \sum_{h=0}^{j} \binom{h+\ell}{\ell} B_\ell^{(j-h)}(X) \cdot f^{(h+\ell)}(X). \qquad (4)
\end{aligned}$$

固定 $j \in \{0, 1, \ldots, k-s\}$。由于 $P_f(X)$ 是零多项式，我们有 $P_{(j)}f(a) = 0$，因此根据上述结果，

$$A^{(j)}(a) + \sum_{\ell=0}^{s-1} \sum_{h=0}^{j} \binom{h+\ell}{\ell} B_\ell^{(j-h)}(a) \cdot f^{(h+\ell)}(a) = 0.$$

观察上述表达式，我们看到其中出现的 f 的最高阶导数是 $f^{(j+s-1)}(a)$，它仅在选取 $\ell = s-1$ 与 $h = j$ 时得到。此外，乘以 $f^{(j+s-1)}(a)$ 的系数是 $\binom{j+s-1}{s-1} B_{s-1}(a)$，根据假设 $\max\{k, s\} \leq$ 特征 $(\mathbb{F}_q)$ 以及 $B_{s-1}(a) \neq 0$，该系数非零。因此，导数 $f^{(j+s-1)}(a)$ 是较低阶导数 $f_{(<j+s-1)}(a)$ 的线性组合。特别地，$f_{(s-1)}(a) \ldots, f_{(k-1)}(a)$，以及多项式 $f(X)$，均由 $f^{(<s-1)}(a) = u$ 唯一确定。

□

根据上述断言，我们显然有 $|\mathcal{L}| \leq q^{s-1}$。此外的部分则由 Q 的线性结构得出。

□

该算法的完整描述见下方图 4，随后给出正确性和效率分析。

对多重 $\mathrm{RS}_q^{(s)}(a_1, \ldots, a_n; k)$ **进行列表译码：**

- **输入：** $w \in (\mathbb{F}_q^s)^n$，其中 $w_i = (w_{i,0}, \ldots, w_{i,s-1}) \in \mathbb{F}_q^s$ 对每个 $i \in [n]$ 均成立。
- **输出：** 列表 $\mathcal{L}$ 包含所有次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$，使得 $f_{(<s)}(a_i) = w_i$ 对至少 $t = \frac{n+s}{(k-1+1)_{s+1}}$ 个指标 ~~$i \in [n]$~~ 成立。

1. 求一个非零的（$s+1$）元多项式 $Q(X, Y_0, \ldots, Y_{s-1})$，其定义在 $\mathbb{F}_q$ 上，形式如下：

$$Q(X, Y_0, \ldots, Y_{s-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{s-1}(X) \cdot Y_{s-1},$$

其中 $A(X)$ 的次数小于 t，每个 $B_\ell(X)$ 的次数小于 $t - k + 1$，且满足：对任意 $i \in [n]$，$Q(a_i, w_i) = 0$ 均成立（其中我们将 $w_i = (w_{i,0}, \ldots, w_{i,s-1}) \in \mathbb{F}_q^s$ 视为对 $\mathbb{F}_q$ 中 s 个变量的赋值）。

通过求解一个线性方程组，可以找到这样的多项式 $Q(X, Y_0, \ldots, Y_{s-1})$。该方程组通过将 Q 中单项式的系数视为未知数，并将每个形如 $Q(a_i, w_i) = 0$ 的要求视为关于这些未知数的齐次线性约束而得到。

2. 求列表 $\mathcal{L}'$ 的一个基，其中包含所有次数小于 k 的一元多项式 $f(X)$，使得

$$Q(X, f(X), f^{(1)}(X), \ldots, f^{(s-1)}(X)) = 0.$$

通过求解一个线性方程组，可以找到这个基。该方程组通过将 $f(X)$ 的 k 系数视为未知数，并将要求 $Q(X, f(X)\ f_{(1)}(X) \ldots, f^{(s-1)}(X))$ 的每个 t 系数为零，视为关于这些未知数的 t（非齐次）线性约束而得到。

3. 输出满足以下条件的所有一元多项式 $f(X)$ 的码字列表 $\mathcal{L}$：其次数小于 k，且 $f^{(<s)}(a_i) = w_i$ 对至少 t 个指标 $i \in [n]$ 成立，即 $f(a_1)\ f(a_2) \ldots, f(a_n)$。

图 4：重数码的列表译码

正确性。设 $f(X) \in \mathbb{F}_q[X]$ 是一个次数小于 k 的一元多项式，且对于至少 t 个指标 $i \in [n]$，$f^{(<s)}(a_i) = w_i$ 成立。我们将证明 $f(X) \in \mathcal{L}$。根据引理 4.1，存在一个非零的 $(s+1)$ 元多项式 $Q(X, Y_0, \ldots, Y_{s-1})$，满足步骤 1 的要求。根据引理 4.2，有 $Q(X, f(X)\ f(1)(X) \cdots, f(s-1)(X)) = 0$，因此 $f(X)$ 将被列入步骤 2 的 $\mathcal{L}'$ 中。显然，$f(X)$ 也将通过步骤 3 的检查，因此 $f(X)$ 也将被列入 $\mathcal{L}$。

效率。步骤 1 可通过高斯消元求解一个含有 $n+1$ 个变量的 n 个线性方程组成的方程组，在 poly$(n, s, \log(q))$ 时间内完成。步骤 2 可通过求解一个含有 k 个变量的 t 个线性方程组成的方程组，在 poly$(n, s, \log(q))$ 时间内完成。根据引理 4.3，步骤 3 可在时间 $|\mathcal{L}| \cdot \text{poly}(n, s, \log(q)) \le q^s \cdot \text{poly}(n, s, \log(q))$ 内完成，其中后一个界在参数 s 为常数且 $q = \text{poly}(n)$ 时关于码长是多项式的。

4.2 将重数码列表译码至容量

现在我们将说明如何把上一节的列表译码算法扩展为一种算法，使其能够将重数码列表译码至容量。

与之前一样，令 $\text{mult}_q^{(s)}(a_1, \ldots, a_n; k)$ 表示重数码，其中 q 是一个素数幂，a_1、a_2、…、a_n 是 $\mathbb{F}_q$ 中互不相同的点，且 s、k 是正整数，使得 $k < sn$ 且 $\max\{k, s\} \le \text{char}(\mathbb{F}_q)$。此外，假设 $w \in (\mathbb{F}_q^s)^n$ 是一个接收字，其中对于任意 $i \in [n]$，$w_i = (w_{i,0}, \ldots w_{i,s-1}) \in \mathbb{F}_q^s$。令 $r \in \{1, 2, \ldots, s\}$ 为一个稍后确定的参数。我们将说明如何计算所有次数小于 k 的多项式 $f(X) \in \mathbb{F}_q[X]$ 的列表，使得对于至多 $e := (s-r+1)rn - r(k-1) - 1$ $(s-r+1)(r+1)$ 个指标 $i \in [n]$，有 $f^{(<s)}(a_i) \ne w_i$。也就是说，对于至少 $t := n - e = (s-r+1)n + r(k-1) + 1 - (s-r+1)(r+1)$ 个指标 $i \in [n]$，有 $f^{(<s)}(a_i) = w_i$。

注意，上一节中的算法对应于 $r = s$ 这一特殊情形。此外，若令 $R := \frac{k}{s \cdot n}$ 表示 $\text{mult}_q^{(s)}(a_1, \ldots, a_n; k)$ 码的码率，则该算法能够在大约 q^r 的时间内，对至多大约 $\frac{r}{r+1}\left(1 - \frac{s}{s-r+1} \cdot R\right)$ 的错误比例进行列表译码。因此，对任意 $\epsilon > 0$，我们可以选择 $r = \Theta(1/\epsilon)$ 与 $s = \Theta(1/\epsilon^2)$，使得错误比例至少为 $1 - R - \epsilon$，且运行时间（以及列表大小）大约为 $q^r = q^{1/\epsilon}$；当 $q = \text{poly}(n)$ 时，该量关于码长是多项式的。稍后，在第 5.2 节中，我们将证明列表大小实际上是一个与码长无关的常数（甚至达到广义 Singleton 界）。

概述。改进后的算法基于重数法，与第 3.3 节中介绍的、用于达到Johnson界的Reed-Solomon码列表译码的算法改进第 3.2 节中介绍的算法的方式类似。

更具体地说，回顾一下，在之前用于重数码列表译码的算法 4 中，在插值步骤中，我们寻找一个非零的低次数 $s+1$-元多项式 $Q(X, Y_0, \ldots, Y_{s-1}) = A(X) + \sum_{\ell=0}^{s-1} B_\ell(X) Y_\ell$，使得对于任意 $i \in [n]$，都有 $Q(a_i, w_i) = 0$；在求根步骤中，我们寻找所有次数小于 k、满足微分方程 $Q(X, f(X)\ f^{(1)}(X) \cdots, f^{(s-1)}(X)) = 0$ 的单变量多项式 $f(X) \in \mathbb{F}_q[X]$。

此外，我们需要从 Q 获得的主要性质是：Q 中的未知系数数量大于形如 $Q(a_i, w_i) = 0$的约束数量；并且 Q 的$(1, k, \ldots, k)$加权次数小于一致参数 t。第一条性质保证存在一个非零的 Q；第二条性质则保证，对于任意次数小于 k的一元多项式 $f(X) \in \mathbb{F}_q[X]$，若对至少 t个指标 $i \in [n]$，有 $f^{(<s)}(a_i) = w_i$，则

$Q(X,\ f(X)\ f^{(1)}(X)\ \cdots,\ f_{(s-1)}(X))$是一个次数小于 t的一元多项式，它至少有 t个根，因此它是零多项式。

为了将重数码列表译码至容量，我们希望将一致参数 t 设得比算法 4 中更小。与之前一样，这意味着$Q(X,\ f(X)\ f^{(1)}(X)\ \cdots,\ f_{(s-1)}(X))$的根数会更少，因此，为了证明它是零多项式，就必须降低 Q的次数。因此， Q 可能少于 n个单项式，所以我们可能无法证明存在非零多项式 Q。

为了解决这个问题，我们将 Q 定义为一个$(r+1)$元多项式 $Q(X,Y_0,\ldots,Y_{r-1})$，其中 $r<s$为某个值，并要求对于任意满足 $f^{(<s)}(a_i)=w_i$的点 $i\in[n]$， $Q(X,f(X)\ f(1)(X)\ldots,f_{(r-1)}(X))$在 a_i 上以重数 $s-r+1$ 消失。因此， $Q(X,f(X)\ f(1)(X)\ \cdots,f_{(s-1)}(X))$的根更多（按重数计），从而可以具有更高的次数和更多的系数，这可能有助于证明非零多项式 Q的存在。然而，这也要付出代价，因为我们还将 Q 上的约束数量增加了 $s-r+1$倍，因此现在要求 Q 比之前有更多系数。不过事实证明，这种权衡是有利的；通过适当设置 r 和 s，可以将一致参数 t 降至可能的最小值。

接下来，我们将分别描述插值步骤和求根步骤中的变化，并分析它们的正确性和效率。

步骤 1：插值。在插值步骤中，我们现在希望求出一个非零的低次数 $r+1$ 元多项式 $Q(X,Y_0,\ldots,Y_{r-1})$，使得对于任意满足 $f^{(<s)}(a_i)=w_i$ 的点 $i\in[n]$， $P_f(X):=Q(X,f(X)\ f(1)(X)\ldots,f^{(r-1)}(X))$ 在 a_i 上以重数 $s-r+1$ 消失。在 Reed-Solomon 码列表译码至 Johnson界的算法中（参见图3），这是通过要求 Q 在任意点 (a_i,w_i) 上以较高的多变量重数消失来保证的（参见断言 3.9）。然而，在当前的设定中，要求 Q 在所有这些点上以较高的多变量重数消失，代价过高；因此，我们直接强制要求，对于每个满足 $f^{(<s)}(a_i)=w_i$ 的 a_i， $P_f(X)$ 都以较高的单变量重数消失。[3]

为了理解这对 Q 提出了什么要求，回想一下，根据 (4)，对于任意 $j\in\mathbb{N}$，我们有

$$P_f^{(j)}(X)=A^{(j)}(X)+\sum_{\ell=0}^{r-1}\sum_{h=0}^{j}\binom{h+\ell}{\ell}B_\ell^{(j-h)}(X)\cdot f^{(h+\ell)}(X).$$

还要注意，在 $f^{(<s)}(a_i)=w_i$ 的情况下，对于任意 $j\in\{0,1,\ldots,s-r\}$，我们都可以得到形如 $f^{(h+\ell)}(a_i)$ 的所有导数，其中 $\ell\in\{0,1,\ldots,r-1\}$ 和 $h\in\{0,1,\ldots,j\}$ 可供我们使用。

引理 4.5。 令 $t=\frac{(s-r+1)n+r(k-1)+1}{(s-r+1)(r+1)}$，那么存在一个非零的 $(r+1)$ 元多项式 $Q(X,Y_0,\ldots,Y_{r-1})$，其系数属于 $\mathbb{F}_q$，且具有如下形式

$$Q(X,Y_0,\ldots,Y_{r-1})=A(X)+B_0(X)\cdot Y_0+\cdots+B_{r-1}(X)\cdot Y_{r-1},$$

其中 $A(X)$ 的次数小于 $(s-r+1)\cdot t$，且每个 $B_\ell(X)$ 的次数小于$(s-r+1)\cdot t-k+1$，并满足

$$A^{(j)}(a_i)+\sum_{\ell=0}^{r-1}\sum_{h=0}^{j}\binom{h+\ell}{\ell}B_\ell^{(j-h)}(a_i)\cdot w_{i,h+\ell}=0 \tag{5}$$

[3]具体而言，正如下文所示，要求 P_f 在 a_i 上的单变量重数至少为 $s-r+1$，会对 Q 的系数施加 $s-r+1$ 个线性约束；而要求 Q 在 a_i 上的多元重数至少为 $s-r+1$，会对 Q 的系数施加 $\binom{(r+1)+(s-r+1)-1}{r+1}=\binom{s+1}{r+1}\approx s^r$ 个线性约束。

对于任意 $i \in [n]$ 和 $j = 0, 1, \ldots, s-r$。

此外，这样一个多项式 $Q(X, Y_0, \ldots, Y_{r-1})$ 可以通过求解一个线性方程组来找到。该方程组是将 $A(X)$ $B_0(X) \ldots, B_{r-1}(X)$ 中的单项式系数视为未知数，并将每个形如 *(5)* 的要求视为关于这些未知数的齐次线性约束后得到的。

证明。 如果将 $A(X)$ $B_0(X) \ldots, B_{r-1}(X)$ 中的单项式系数视为未知数，那么每个形如 (5) 的要求都会对这些未知数施加一个齐次线性约束。

进一步注意，未知数的个数为

$$(s-r+1) \cdot t + r \cdot ((s-r+1) \cdot t - k + 1) = (r+1) \cdot (s-r+1) \cdot t - r \cdot (k-1) = (s-r+1) \cdot n + 1$$

而线性约束的个数为 $(s-r+1) \cdot n$，因此这个线性系统有非零解。

□

步骤 2：求根。在这一步中，我们寻找所有次数小于 k 的单变量多项式 $f(X) \in \mathbb{F}_q[X]$，使得 $Q(X, f(X), f^{(1)}(X), \ldots, f^{(r-1)}(X)) = 0$；我们希望证明，任何次数小于 k 的单变量多项式 $f(X) \in \mathbb{F}_q[X]$，只要对至少 t 个指标 $i \in [n]$ 满足 $f^{(<s)}(a_i) = w_i$，就会满足 $Q(X, f(X), f^{(1)}(X), \ldots, f^{(r-1)}(X)) = 0$。我们已经在引理 4.3 中说明了如何完成前者，下面的引理将说明后者。

引理 4.6。 设 Q（X、Y_0、...、Y_{r-1}）是定义在 $\mathbb{F}_q$ 上的一个非零（$r+1$）元多项式，其形式为

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1},$$

其中，A（X）的次数小于（$s-r+1$）$\cdot t$，且每个 B_ℓ（X）的次数都小于（$s-r+1$）$\cdot t-k+1$，并且对任意 $i \in [n]$ 和 $j = 0$、1、...、$s-r$，均满足 *(5)*。设 f（X）$\in \mathbb{F}_q[X]$ 是一个次数小于 k 的一元多项式，使得对于至少 t 个指标 $i \in [n]$，有 $f^{(<s)}(a_i) = w_i$。则

$$Q(X, f(X), f^{(1)}(X), \ldots, f^{(r-1)}(X)) = 0.$$

证明。 多项式 $P_f(X) := Q(X, f(X), f^{(1)}(X), \ldots, f^{(r-1)}(X))$ 是一个次数小于 $(s-r+1) \cdot t$ 的一元多项式。此外，根据 (4)，对于任意满足 $f^{(<s)}(a_i) = w_i$ 的 $i \in [n]$，有：

$$\begin{aligned} P_f^{(j)}(a_i) &= A^{(j)}(a_i) + \sum_{\ell=0}^{r-1} \sum_{h=0}^{j} \binom{h+\ell}{\ell} B_\ell^{(j-h)}(a_i) \cdot f^{(h+\ell)}(a_i) \\ &= A^{(j)}(a_i) + \sum_{\ell=0}^{r-1} \sum_{h=0}^{j} \binom{h+\ell}{\ell} B_\ell^{(j-h)}(a_i) \cdot w_{i,h+\ell} \end{aligned}$$

对任意 $j = 0, 1, \ldots\ldots, s-r$。因此，对任意满足 $f^{(<s)}(a_i) = w_i$ 的 $i \in [n]$，$P_f(X)$ 在 a_i 上以重数 $s-r+1$ 为零。从而 $P_f(X)$ 是次数小于 $(s-r+1) \cdot t$ 的一元多项式，且至少有 t 个重数为 $s-r+1$ 的根，故由事实 2.3，它必为零多项式。 □

算法的完整描述见下方图 5，随后给出正确性和效率分析。

达到 $\mathsf{MULT}_q^{(s)}(a_1, \ldots, a_n; k)$ 容量的列表译码：

- **输入：** $w \in (\mathbb{F}_q^s)^n$，其中 $w_i = (w_{i,\,0},\ \ldots\ldots,\ w_{i,\,s-1}) \in \mathbb{F}_q^s$ 对每个 $i \in [n]$。
- **输出：** **</style}所有满足以下条件的多项式列表：这些多项式() 的次数小于，且对于至少($s-r+1)n+r$ $(k-1)+1$ $(s-r+1)(r+1)$ ~~个指标 $i \in [n]$~~，有 $f^{(<s)}(a_i) = w_i$。

1. 求一个非零的（$r+1$）元多项式 $Q(X, Y_0, \ldots, Y_{r-1})$，其系数属于 $\mathbb{F}_q$，形式如下

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1},$$

其中 $A(X)$的次数小于$(s-r+1)\cdot t$，且每个 $B_\ell(X)$的次数都小于$(s-r+1)\cdot(t-k+1)$，并且满足

$$A^{(j)}(a_i) + \sum_{\ell=0}^{r-1} \sum_{h=0}^{j} \binom{h+\ell}{\ell} B_\ell^{(j-h)}(a_i) \cdot w_{i,h+\ell} = 0$$

对于任意 $i \in [n]$ 和 $j = 0,\ 1, \ldots, s-r$。
这样的多项式 $Q(X, Y_0, \ldots, Y_{r-1})$可以通过求解一个线性方程组找到：将 Q 中单项式的系数视为未知数，并将上述每项要求视为关于这些未知数的齐次线性约束。

2. 求列表 $\mathcal{L}'$ 的一个基，该列表由所有次数小于 k 的单变量多项式 $f(X)$组成，使得

$$Q(X, f(X), \ldots, f^{(r-1)}(X)) = 0.$$

这个基可以通过求解一个线性方程组得到；该方程组是将 $f(X)$的k 个系数视为未知数，并将$Q(X, f(X)\ f^{(1)}(X) \ldots, f^{(r-1)}(X))$的 t 个系数均为零这一要求视为对这些未知数的 t 个（非齐次）线性约束而得到的。

3. 输出列表 $\mathcal{L}$，其中包含所有码字$(f(a_1)\ f(a_2) \ldots, f(a_n))$，这些码字对应于次数小于 k 的单变量多项式 $f(X)$ $\in \mathcal{L}'$，且满足对至少 t 个指标 $i \in [n]$有 $f^{(<s)}(a_i) = w_i$。

图 5：重数码直至容量的列表译码

正确性。假设 $f(X) \in \mathbb{F}_q[X]$ 是一个次数小于 k 的一元多项式，使得对至少 t个指标 $i \in [n]$有$f^{(<s)}(a_i) = w_i$，我们将证明 $f(X) \in \mathcal{L}$。由引理 4.5，存在一个满足步骤 1 中要求的非零$(r+1)$元多项式 $Q(X, Y_0, \ldots, Y_{r-1})$。由引理 4.6，我们有 $Q(X, f(X)\ f^{(1)}(X) \ldots, f^{(r-1)}(X)) = 0$，因此 $f(X)$将在步骤 2 中被包含于 $\mathcal{L}'$。显然，$f(X)$也将通过步骤 3 中的检验，从而 $f(X)$也将被包含于 $\mathcal{L}$。

效率。步骤 1 可以通过使用高斯消元求解一个包含 $(s-r+1)$ 个 $\cdot n$ 线性方程和 $(s-r+1)$ 个 $\cdot n+1$ 变量的方程组，在 poly$(n,\ s,\ \log(q))$ 时间内完成。步骤 2 可以通过求解一个包含 t 个线性方程和 k 个变量的方程组，在 poly$(n,\ s,\ \log(q))$ 时间内完成。根据引理 4.3，步骤 3 可以在 $|\mathcal{L}| \cdot \text{poly}(n,\ s,\ \log(q)) \le q^r \cdot \text{poly}(n,\ s,\ \log(q))$ 时间内完成，其中后一个上界对于一个常数 r 和 $q = \text{poly}(n)$而言，是关于码长的多项式。

4.3 列表译码 子域求值点上的 Reed-Solomon 码，直至容量 y

现在我们回到 Reed-Solomon 码这一基本族，并考察这类码的一个特殊子类：它们定义在扩域上，且在子域上取值。我们将证明，可以使用一种类似于第 4.1 节中介绍的算法，对这些码进行列表译码，达到容量，尽管其运行时间仅为略具非平凡性的亚指数运行时间。特别地，这意味着这些码的列表大小具有亚指数上界；稍后在第5.3节中我们将证明，通过转而使用一个（经过谨慎选择的）子码，可以将列表大小降至一个与码长无关的常数（并将运行时间降至关于码长的多项式）。

更具体地说，在下文中固定一个素数幂 q、互异点 $a_1, \ldots, a_n \in \mathbb{F}_q$、满足 $k < n$ 的正整数k 以及正整数 s，并考虑定义在扩域 $\mathbb{F}_{q^s}$上的 Reed-Solomon 码 RS$_{q^s}$($a_1, \ldots, a_n$; k)。我们将证明，RS$_{q^s}$($a_1, \ldots, a_n$; k) 可以进行列表译码，并且在唯一译码半径之外具有与重数码的列表译码算法（算法 4）类似的保证。设 $w \in (\mathbb{F}_{q^s})^n$ 是一个接收字。令 $r \in \{1, \ldots, s\}$ 为稍后确定的参数。我们将说明如何计算所有次数小于 k的多项式 $f(X) \in \mathbb{F}_{q^s}[X]$ 组成的列表，使得对于至多 $e = {}^{r}(_{n-k+1})_{r+1}{}^{-1}$ 个指标 $i \in [n]$，有 $f(a_i) \neq w_i$。~~也就是说，~~ 对于至少 $t := n - e = \binom{n+r}{r+1}(k-1+1)$ 个指标 $i \in [n]$，有 ~~$f(a_i) = w_i$~~。

然而，Reed-Solomon 码 RS$_{q^s}$(a_1、……、 a_n; k) 相比相应的重数码 MULT$_q^{(s)}$(a_1、……、 a_n; k) 的主要优势在于，RS$_{q^s}$(a_1、……、 a_n; k) 的码率高出一个乘法因子 s。更具体地说，若令 $R := \frac{k}{n}$ 表示 RS$_{q^s}$(a_1、……、 a_n; k) 码的码率，那么该算法能够在大约 q^{rk} 的时间内，对错误比例最高约为 $\frac{r}{r+1}(1-R)$ 的字进行列表解码。特别地，对于任意常数 $\epsilon > 0$，我们可以选择 $r = \Theta(1/\epsilon)$ 和 $s = \Theta(1/\epsilon^2)$，使得错误比例至少为 $1 - R - \epsilon$，而运行时间（以及列表大小）约为 $q^{rk} = q^{\epsilon s k}$；相对于不同码字的数量 q^{sk}，这属于次多项式时间。稍后在第5.3节中，我们将说明，通过转而使用一个合适的子码，可以将列表大小降至与码长无关的常数（并将运行时间降至关于码长的多项式时间）。

概述。 该列表译码算法与超出唯一译码半径的重数码列表译码算法（算法 4）非常相似。回想一下，在算法 4 中，在插值步骤中，我们寻找了一个形如 $Q(X, Y_0, \ldots, Y_{s-1})$ 的非零低次数 $s+1$ 元多项式

$$Q(X, Y_0, \ldots, Y_{s-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{s-1}(X) \cdot Y_{s-1},$$

使得对于任意 $i \in [n]$，$Q(a_i, w_i) = 0$，并且在求根步骤中，我们寻找了所有满足以下条件的一元多项式$f(X) \in \mathbb{F}_q[X]$

$$Q(X, f(X), f^{(1)}(X), \ldots, f^{(s-1)}(X)) = 0.$$

我们将用于在子域求值点上对 Reed-Solomon 码进行列表译码的主要观察是：对于扩域 $\mathbb{F}_{q^s}$ 上的任意多项式 $f(X) = \sum_{i=0}^{k-1} f_i X^i$，以及基域 $\mathbb{F}_q$ 中的任意点 a，

$$(f(a))^q = \left(\sum_{i=0}^{k-1} f_i a^i\right)^q = \sum_{i=0}^{k-1} (f_i)^q (a^q)^i = \sum_{i=0}^{k-1} (f_i)^q a^i,$$

其中第二个等式利用了如下事实：取 q 次幂是一个 $\mathbb{F}_q$-线性变换，而第三个等式利用了如下事实：对任意 $a \in \mathbb{F}_q$，$a^q = a$。受此启发，对于一个多项式

$f(X) = \sum_{i=0}^{k-1} f_i X^i \in \mathbb{F}_{q^s}[X]$，我们令 $\sigma(f) = \sum_{i=0}^{k-1} (f_i)^q X^i \in \mathbb{F}_{q^s}[X]$。在此记号下，对任意多项式 $f(X) \in \mathbb{F}_{q^s}[X]$ 以及点 $a \in \mathbb{F}_q$，我们有$(f(a))^q = \sigma(f)(a)$。

利用上述结果，在 RS$_{q^s}(a_1, \ldots, a_n; k)$ 的列表译码算法中，我们再次在插值步骤中寻找一个非零的低次数（$r+1$）元多项式，形式为 $Q(X) = A(X) + \sum_{\ell=0}^{r-1} B_\ell(X) \cdot Y^\ell$（其系数取自扩域 $\mathbb{F}_{q^s}$）。不过，现在在插值步骤中，我们要求

$$Q\left(a_i, w_i, (w_i)^q, \ldots, (w_i)^{q^{r-1}}\right) = 0$$

对任意 $i \in [n]$ 均成立。接着在求根步骤中，我们寻找所有满足以下条件的一元多项式 $f(X) \in \mathbb{F}_{q^s}[X]$

$$Q\left(X, f(X), \sigma(f)(X), \ldots, \sigma^{r-1}(f)(X)\right) = 0.$$

接下来，我们分别描述插值步骤和求根步骤，并分析它们的正确性和效率。

步骤 1：插值。在此步骤中，我们希望求出一个非零的低次数（$r+1$）元多项式$Q(X, Y_0, \ldots, Y_{r-1})$，使得 $Q\left(a_i, w_i, (w_i)^q, \ldots, (w_i)^{q^{r-1}}\right) = 0$。以下引理的证明与引理 4.1 的证明完全相同。

引理4.7。设 $t = \frac{n+r}{r+1}$。则存在一个非零的$(r+1)$元多项式$Q(X, Y_0, \ldots, Y_{r-1})$，其定义域为 $\mathbb{F}_{q^s}$，形式为

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1},$$

其中，$A(X)$ 的次数小于 t，且每个 $B_\ell(X)$ 的次数小于 $t - k + 1$，并且满足

$$Q\left(a_i, w_i, (w_i)^q, \ldots, (w_i)^{q^{r-1}}\right) = 0$$

对任意 $i \in [n]$均成立。

此外，这样的多项式$Q(X, Y_0, \ldots, Y_{r-1})$ 可以通过求解一个线性方程组得到：将 $A(X)$ $B_0(X)$ $\ldots$, $B_{r-1}(X)$ 中的单项式的系数视为未知数，并将每个形式为 $Q\left(a_i, w_i, (w_i)^q, \ldots, (w_i)^{q^{r-1}}\right) = 0$ 的要求视为关于这些未知数的齐次线性约束。

步骤 2：求根。在这一步中，我们寻找所有满足$Q\left(X, f(X)\ \sigma(f)(X) \ldots, \sigma^{r-1}(f)(X)\right) = 0$，的单变量多项式 $f(X) \in \mathbb{F}_{q^s}[X]$，并希望证明：任何次数小于 k 的单变量多项式$f(X) \in \mathbb{F}_{q^s}[X]$，只要 $f(a_i) = w_i$ 对至少 t 个指标 $i \in [n]$ 成立，就满足$Q\left(X, f(X)\ \sigma(f)(X) \ldots, \sigma^{r-1}(f)(X)\right) = 0$。我们先证明后者。

引理 4.8。假设 满足 $Q(X, Y_0, \ldots, Y_{r-1})$ 是一个非零的$(r+1)$元多项式，定义在 $\mathbb{F}_{q^s}$ 上，其形式为

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1},$$

其中 $A(X)$ 的次数小于 t，且每个 $B_\ell(X)$ 的次数小于 $t - k + 1$，并且满足

$$Q\left(X, f(X), \sigma(f)(X), \ldots, \sigma^{r-1}(f)(X)\right) = 0$$

对任意 $i \in [n]$。设 $f(X) \in \mathbb{F}_{q^s}[X]$ 是一个次数小于 k 的一元多项式，使得 $f(a_i) = w_i$ 对至少 t 个指标 $i \in [n]$ 成立。那么

$$Q\left(X, f(X), \sigma(f)(X), \ldots, \sigma^{r-1}(f)(X)\right) = 0.$$

证明。 多项式 $P_f(X) := Q\left(X, f(X)\ \sigma(f)(X) \ldots, \sigma^{r-1}(f)(X)\right)$ 是定义在 $\mathbb{F}_{q^s}$ 上的次数小于 t 的一元多项式，它满足

$$\begin{aligned} P_f(a_i) &= Q\left(a_i, f(a_i), \sigma(f)(a_i), \ldots, \sigma^{r-1}(f)(a_i)\right) \\ &= Q\left(a_i, f(a_i), (f(a_i))^q, \ldots, (f(a_i))^{q^{r-1}}\right) \\ &= Q\left(a_i, w_i, (w_i)^q, \ldots, (w_i)^{q^{r-1}}\right) = 0 \end{aligned}$$

对于任意满足 $f(a_i) = w_i$ 的 $i \in [n]$。因此， $P_f(X)$ 是一个次数小于 t 且至少有 t 个根的一元多项式，所以它必定是零多项式。 □

下一个引理给出了满足方程$Q\left(X, f(X)\ \sigma(f)(X) \ldots, \sigma^{r-1}(f)(X)\right) = 0$.的单变量多项式 $f(X) \in \mathbb{F}_{q^s}[X]$ 的数量上界

引理 4.9。 设 $Q(X, Y_0, \ldots, Y_{r-1})$ 是一个非零的 $r+1$ 元多项式，系数取自 $\mathbb{F}_{q^s}$，其形式为

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1},$$

并令 $\mathcal{L}$ 为包含所有次数小于 k 的多项式 $f(X) \in \mathbb{F}_{q^s}[X]$ 的列表，使得

$$Q\left(X, f(X), \sigma(f)(X), \ldots, \sigma^{r-1}(f)(X)\right) = 0.$$

那么 $|\mathcal{L}| \le q^{(r-1)\cdot k}$。

此外， $\mathcal{L}$构成 $\mathbb{F}_q$ 上一个维数至多为 $(r-1)k$ 的仿射子空间。通过求解 $\mathbb{F}_q$ 上的一个线性方程组，可以找到该子空间的一组基。这个方程组是这样得到的：将 $f(X)$ 的系数（表示为 $\mathbb{F}_q^s$ 中的字符串）视为未知数，并将要求 $Q\left(X, f(X)\ \sigma(f)(X) \ldots, \sigma^{r-1}(f)(X)\right)$ 的每个系数都为零，视为关于这些未知数的一个（非齐次） $\mathbb{F}_q$-线性约束。

证明。 与引理 4.3 的证明一样，我们可以假设存在一个元素 $a \in \mathbb{F}_q^s$，使得 $B_{r-1}(a) \neq 0$。不失一般性，我们还可以进一步假设 $a = 0$；否则，我们可以将所有多项式$A(X)\ B_0(X) \ldots, B_{r-1}(X)$ 平移 a，这相当于将 $\mathcal{L}$ 中的所有多项式平移 a，而这不会改变 $\mathcal{L}$ 的大小。

设 $f(X) = \sum_{j=0}^{k-1} f_j X^j$ 是一个次数小于 k 的 $\mathbb{F}_{q^s}$ 上的多项式，满足

$$\begin{aligned} P_f(X) &:= Q\left(X, f(X), \sigma(f)(X), \ldots, \sigma^{r-1}(f)(X)\right) \\ &= A(X) + \sum_{\ell=0}^{r-1} B_\ell(X) \cdot \sigma^\ell(f)(X) \\ &= A(X) + \sum_{\ell=0}^{r-1} B_\ell(X) \sum_{j=0}^{k-1} (f_j)^{q^\ell} X^j \\ &= 0. \end{aligned}$$

我们将证明，对于任意 $j \in \{0, 1, \ldots, k-1\}$，给定前 $j-1$ 个系数 f_0， $f_1, \ldots, f_{j-1}$， f_j至多有 q^{r-1} 种取值，因此 $|\mathcal{L}| \le q^{(r-1)k}$。

为证明上述结论，固定 $j \in \{0, 1, \ldots, k-1\}$。由于 $P_f(X)$ 是零多项式， $P_f(X)$ 中 X^j 的系数必为零。另一方面，检查上面关于 $P_f(X)$ 的表达式，我们看到

$P_f(X)$ 中 X^j 的系数可写为 $y_j + \sum_{\ell=0}^{r-1} B_\ell(0) \cdot (f_j)^{q^\ell}$，其中 $y_j \in \mathbb{F}_{q^s}$ 由f_0，f_1，……，f_{j-1}确定。

Let

$$B(X) := B_0(0) \cdot X + B_1(0) \cdot X^q + \cdots + B_{r-1}(0) \cdot X^{q^{r-1}}.$$

于是由上文可知，$f_j \in \mathbb{F}_{q^s}$ 必须满足 $B(f_j) = -y_j$。另一方面，由假设$B_{r-1}(0) \neq 0$，$B(X)$是一个次数为 q^{r-1}的非零多项式，因此它在 $\mathbb{F}_{q^s}$中对任意值至多取到 q^{r-1}个赋值。因此，对任意 $j \in \{0, 1, \ldots, k-1\}$，在给定先前系数 $f_0, \ldots, f_{j-1}$的情况下，系数 f_j至多有 q^{r-1} 种选择，这进而意味着 $|\mathcal{L}| \leq q^{(r-1)k}$。

此外部分由 Q的线性结构，以及取 q 次幂是一个$\mathbb{F}_q$-线性变换这一事实得出。

□

该算法的完整描述见下方图 6，随后是正确性与效率分析。

对 $a_1, \ldots, a_n \in \mathbb{F}_q$的$\mathrm{RS}_{q^s}(a_1, \ldots, a_n; k)$ 进行列表译码：

- **输入：** $w \in (\mathbb{F}_{q^s})^n$。
- **输出：</style}所有次数小于 的多项式 () 的列表，其中 () 至少对 ($\binom{k-1+1}{r+1}$) 个指标 $i \in [n]$成立。**

1. 求一个非零的 $(r+1)$ 元多项式 $Q(X, Y_0, \ldots, Y_{r-1})$，其系数属于 $\mathbb{F}_q$，形式如下

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1},$$

其中 $A(X)$ 的次数小于 t，且每个 $B_\ell(X)$ 的次数小于 $t - k + 1$，并且满足：对于任意 $i \in [n]$，$Q(a_i, (w_i)^q, \ldots, (w_i)^{q^{r-1}}) = 0$。
可以通过求解一个线性方程组来找到这样的多项式 $Q(X, Y_0, \ldots, Y_{r-1})$。该方程组的构造方法是：将 Q 中单项式的系数视为未知数，并将每个形如 $Q(a_i, (w_i)^q, \ldots, (w_i)^{q^{s-1}}) = 0$ 的条件视为关于这些未知数的齐次线性约束。

2. 求出列表 $\mathcal{L}'$ 的一个基，其中包含所有次数小于 k 的 $f(X)$ 一元多项式，这些多项式定义在 $\mathbb{F}_{q^s}$ 上，使得

$$Q\left(X, f(X), \sigma(f)(X), \ldots, \sigma^{r-1}(f)(X)\right) = 0.$$

这个基可以通过求解 $\mathbb{F}_q$ 上的一个线性方程组得到。该方程组的构造方式是：将 $f(X)$ 的 k 个系数（表示为 $\mathbb{F}_q^s$ 上的字符串）视为未知数，并将要求 $Q\left(X, f(X)\ \sigma(f)(X) \ldots, \sigma^{r-1}(f)(X)\right)$ 的每个 t 系数均为零，视为关于这些未知数的 t（非齐次）$\mathbb{F}_q$-线性约束。

3. 输出列表 $\mathcal{L}$，其中包含与满足以下条件的一元多项式 $f(X) \in \mathcal{L}'$ 相对应的所有码字 $(f(a_1)\ f(a_2) \ldots, f(a_n))$：其次数小于 k，且对于至少 t 个指标 $i \in [n]$，有 $f(a_i) = w_i$。

图 6：基于子域求值点的里德-所罗门码列表译码

正确性。假设 $f(X) \in \mathbb{F}_{q^s}[X]$ 是一个次数小于 k 的单变量多项式，使得$f(a_i) = w_i$ 对至少 t 个指标 $i \in [n]$成立，我们将证明 $f(X) \in \mathcal{L}$。根据引理 4.7，存在一个

非零的 $(r+1)$ 元多项式 $Q(X,\ Y_0,\ \ldots\ldots,\ Y_{r-1})$，满足步骤 1 的要求。根据引理 4.8，我们有 $Q\left(X,\ f(X)\ \sigma(f)(X)\ \ldots\ldots,\ \sigma^{r-1}(f)(X)\right)=0$，因此 $f(X)$ 将被纳入步骤 2。显然，$f(X)$ 也会通过步骤 3 的检查，因此 $f(X)$ 也将被纳入 $\mathcal{L}$。

效率。步骤 1 可以通过使用高斯消元法求解一个含有 $n+1$ 个变量的 n 个线性方程组，在 poly$(n, s,$log$(q))$ 时间内完成。步骤 2 可以通过求解一个含有 ks 个变量的 t 个线性方程组，在 poly$(n, s,$log$(q))$ 时间内完成。根据引理 4.9，步骤 3 可以在时间 $|\mathcal{L}|\cdot$poly$(n, s,$ log$(q)) \le q^{(r-1)k}\cdot$ poly$(n, s,$ log$(q))$ 内完成，其中后一个界关于 $r \le \epsilon s$ 的不同码字数量 q^{sk} 是次多项式的。

4.4 文献注记

在 [GR08], Guruswami 和 Rudra 提出了折叠 Reed-Solomon（FRS）码这一类码，并给出了一个高效算法，可将这些码列表译码至容量，从而首次构造出一类能够高效列表译码至容量的显式码。折叠 Reed-Solomon 码的定义与 Reed-Solomon 码类似，只是将每个码字条目 $f(a_i)$ 替换为由求值组成的元组 $(f(a_i)\ f(\gamma\cdot a_i)\ldots, f(\gamma^{s-1}\cdot a_i)) \in \mathbb{F}_q^s$，其中 γ 是乘法群 $\mathbb{F}_q^*$ 的生成元，$s\ge 1$ 是折叠参数，并且对于 $i\in[n]$，所有集合 $\{a_i, \gamma a_i, \ldots, \gamma^{s-1}a_i\}$ 两两不相交。Guruswami 和 Rudra 证明，当 s 足够大时（取决于与容量的间隙 ϵ），这些码可以列表译码至容量，其所用算法与第 3.3 节中将 Reed-Solomon 码列表译码至 Johnson 界的算法类似。后来，Kopparty [Kop15] 证明，类似的算法也可用于将重数码列表译码至容量。

第 4.2 节介绍了利用具有线性结构的插值多项式 Q将重数码（以及 FRS 码）列表译码至容量的算法。该算法由 Vadhan [Vad12, 第 5.2 节.4] 以及 Guruswami 和 Wang [GW13]发现。第 4.1 节将重数码超出唯一译码半径的列表译码算法作为预备内容介绍，其内容遵循 [GRS, 第 17 节. 2] 中关于折叠 Reed-Solomon 码列表译码的讲解。

Bhandari、Harsha、Kumar 和 Sudan [BHKS24b]证明，折叠 Reed-Solomon 码和重数码的列表译码算法可以推广到更一般的多项式理想码这一类码；折叠 Reed-Solomon 码和重数码都是该类码的特例。第 4.3 节介绍了在子域求值点上将 Reed-Solomon 码列表译码至容量的算法，该算法由 Guruswami 和 Xing [GX22]发现。

上述所有列表译码算法也可以扩展到列表恢复的情形：对于每个码字条目，给定一个由少量 ℓ 可能值组成的列表，目标是返回与这些列表中的大多数相一致的所有码字所构成的列表（列表译码对应于$\ell = 1$这一特殊情形）。关于列表恢复模型的动机，以及上述算法向列表恢复情形的扩展，读者可参阅综述 [RV25]，了解更多信息。

5 列表大小的组合上界

在上一节中，我们介绍了可将重数码列表译码至容量的高效（多项式时间）算法，并且还证明，一种类似算法可用于对采用子域求值点的 Reed-Solomon 码进行列表译码，所需时间略高于平凡的次指数时间。这些算法尤其意味着对这些码的列表大小存在组合上界，不过所得上界相当大。具体而言，重数码的列表大小是一个较大的多项式 $n^{\Theta(1/\epsilon)}$，而且仅

采用子域求值点的 Reed-Solomon 码的列表大小略呈次指数级 N^{ϵ}，其中 n, N分别表示码长和码大小，而 ϵ表示与容量的间隙。

在本节中，我们将给出关于这些码的列表大小的更紧组合上界。具体而言，我们首先将在下文第 5.1 节证明，在随机求值点上取值的 Reed-Solomon 码（组合意义上）可列表译码直至广义辛格尔顿界，因此尤其可列表译码至容量，列表大小为 $O(1/\epsilon)$。接着，在第 5.2 节中，我们证明重数码在任意 求值点集合上都能达到广义辛格尔顿界。最后，在第 5.3 节中，我们证明，在子域求值点上取值的 Reed-Solomon 码的某个子码（即仅选取部分码字构成的码）可高效列表译码至容量，且列表大小为常数 （取决于 ϵ）。

5.1 随机求值点上的 Reed-Solomon 码

在本节中，我们证明：从一个足够大的（指数规模）域中选取随机 点作为求值点时，Reed-Solomon 码以高概率可列表译码至广义辛格尔顿界 （参见定理 2.2）。证明依赖于两个主要要素：高阶 MDS 码和超图连通性。我们将在下文第 5.1.1 节和第 5.1.2 节分别回顾这两个要素，然后在第 5.1.3 节利用它们证明关于随机 Reed-Solomon 码的结果。

5.1.1 高阶 MDS 码

*Singleton*界指出，对于任意距离为 Δ、大小为 $|C| = \Sigma^k$ 的码 $C \subseteq \Sigma^n$，必有$\Delta \leq n - k + 1$（这尤其意味着 $\delta \leq 1 - R$）。若码 C 达到 Singleton 界，即满足 $\Delta = n - k + 1$，则称其为最大距离可分（MDS）码。众所周知，线性码线性码 C 是 MDS 码，当且仅当其对偶码 $C^{\perp}$ 也是 MDS 码。在第 2.1 节中，我们介绍了广义辛格尔顿界（参见定理 2.2），它将 MDS 码的概念推广到了列表译码的情形。本节将介绍线性线性MDS 码概念的另一种推广，并称之为高阶 *MDS* 码。稍后，在第 5.1.3 节中，我们将通过证明：如果 C 是高阶 MDS 码，那么其对偶码 $C^{\perp}$ 达到广义辛格尔顿界，从而建立这两个概念之间的联系。

设 $C \subseteq \mathbb{F}^n$ 是一个维数为 k 的线性码，且 $G \in \mathbb{F}^{n \times k}$ 是 C 的生成矩阵，其中 $G_1, \ldots, G_k \in \mathbb{F}^n$ 表示 G 的列。对于字符串 $w \in \mathbb{F}^n$，令 $\mathcal{Z}(w) := \{i \in [n] \mid w_i = 0\}$ 表示 w 的零分量集合。注意， G 的任意一列 G_j 都是 C 的非零码字，因此，若 C 是最大距离可分码，则 G_j 的权重至少为 $n - k + 1$，或者等价地， $|\mathcal{Z}(G_j)| \leq k - 1$。以下事实通过指出，对于线性 MDS 码， G 的任意 t 列至多有 $k - t$ 个公共零点，推广了这一观察。

事实 5.1. 设 $C \subseteq \mathbb{F}^n$ 是一个线性 *MDS* 码，其生成矩阵为 $G \in \mathbb{F}^{n \times k}$，列为 $G_1, \ldots, G_k$。则对于任意非空子集 $J \subseteq [k]$， $\left|\bigcap_{j \in J} \mathcal{Z}(G_j)\right| \leq k - |J|$。

证明。 反设存在一个大小为 t 的非空子集 $J \subseteq [k]$，使得$\left|\bigcap_{j \in J} \mathcal{Z}(G_j)\right| \geq k - t + 1$。不失一般性，我们可以假设 $J = \{1, 2, \ldots, t\}$ 且$\bigcap_{j \in J} \mathcal{Z}(G_j) \supseteq \{1, 2, \ldots, k - t + 1\}$。令 A 表示 G的左上角 $k \times k$ 阶子式。于是， A 的左上角有一个 $(k - t + 1) \times t$ 零块，因此其前 t 列的秩至多为 $t - 1$，所以这些列线性相关。由此， A 不是满秩的，因此存在 $0 \neq m \in \mathbb{F}^k$，使得 $A \cdot m = 0$。但这又意味着， $G \cdot m$ 是 C 中的一个非零码字，其权重至多为 $n - k$，这与假设 C 是最大距离可分码相矛盾。 □

高阶 MDS 码是满足上述事实逆命题的码，即对于满足上述事实所给交条件的任意零模式，都存在一个该码的生成矩阵，使其具有

这个零模式。更正式地说，如果对于任意 $\emptyset \neq J \subseteq [k]$ 都有 $\left|\bigcap_{j\in J} Z_j\right| \leq k - |J|$，则称一系列（不一定互不相同）的子集 Z_1、Z_2..... $Z_k \subseteq [n]$ 是一般零模式 （GZP）。此外，如果一个矩阵$G \in \mathbb{F}^{n\times k}$的列为 G_1..... $G_k \in \mathbb{F}^n$，且对于所有 $j \in [k]$ 都有 $Z_j \subseteq \mathcal{Z}$（$G_j$），则称该矩阵$G \in \mathbb{F}^{n\times k}$实现 Z_1..... Z_k。

定义 5.2 （高阶 MDS 码）。设 $C \subseteq \mathbb{F}^n$ 是一个维数为 k 的线性最大距离可分码 。我们称C为高阶 *MDS* 码，如果对于任意GZP $Z_1, \ldots, Z_k \subseteq [n]$，都存在 C的生成矩阵 G，使其达到 $Z_1, \ldots, Z_k$。

5.1.2 超图连通性

为了将高阶 MDS 码的概念与列表译码联系起来，我们将使用一种特定的超图连通性概念。为描述这一概念，我们首先需要引入一些记号与定义。一个超图 $H = (V, E)$由一个顶点全集 $V = \{v_1, \ldots, v_n\}$和一个（可能为空的）超边集合（也可能是多重集） $E = \{e_1, \ldots, e_m\}$构成，其中的超边是顶点V的（可能为空的）子集。我们将边 $e \in E$ 的权重 wt(e)定义为 wt(e) := max $\{|e| - 1, 0\}$，并将超图H 的权重 wt(H)定义为边权重之和 wt(H) := $\sum_{i=1}^{m}$wt(e_i)。对于 $U \subseteq V$，令 $H|_U$ 表示子超图$H|_U = (U, E|_U)$，其中 $E|_U := \{e_1 \cap U, \ldots, e_m \cap U\}$。

若超图 $H = (V, E)$ 对任意非空真子集 $U \subseteq V$，集合 U 与 $V \setminus U$ 之间的跨割边数量（即至少有一个顶点属于 U 且至少有一个顶点属于 $V \setminus U$的边 $e \in E$ 的数量）都不少于 k，则称其为 k-边连通。 $k = 1$ 情形对应于超图连通性的标准概念，要求 V中的任意一对顶点之间都存在一条路径。[4] 根据超图门格尔定理 [Kir03，定理 1，11]，$k \geq 2$情形等价于以下性质： V中每一对顶点之间都存在 k 条边不相交路径。

k-划分连通性是上述 k-边连通概念的强化。它要求对于任意整数 $t \geq 2$，以及将 V划分为 t 个部分的任意划分 $\mathcal{P}$，跨割边的数量（即不完全包含在划分的某一个部分中的边的数量）至少为 $k(t-1)$。注意， k-边连通对应于 $t = 2$这一特殊情形。我们将使用以下较弱的划分连通性概念。

定义 5.3 （弱划分连通性）。超图 $H = (V, E)$ 是 k-弱划分连通的，当且仅当对于将 V划分为 t个部分的每个划分 $\mathcal{P}$，均满足：

$$\sum_{e\in E} \max\{|\mathcal{P}(e)| - 1, 0\} \geq k(t-1),$$

其中， $|\mathcal{P}(e)|$ 表示与 e相交的划分部分数。

注意，对于任意划分 $\mathcal{P}$，每条跨割边 $e \in E$ 对上述不等式左侧的贡献至少为 1，因此 k-划分连通性蕴含 k-弱划分连通性。此外，对于分成两部分的划分 $\mathcal{P}$，上述不等式左侧等于跨割边的数量，因此 k-弱划分连通性也蕴含 k-边连通度。

接下来我们证明,任何权重足够大的超图都包含一个弱划分连通的子超图 .

引理 5.4。设 $H = (V, E)$ 是一个至少有两个顶点且权重至少为 $k(|V| - 1)$ 的超图。那么存在一个包含至少两个顶点的子集 $U \subseteq V$，使得 $H|_U$ 是 k-弱划分连通的。

[4]超图中的一条路径 $H = (V, E)$ 是一个序列 $v_1, e'_1, v_2, e'_2, \ldots\ldots, v_{\ell-1}, e'_{\ell-1}, v_\ell$，其中 $v_1, \ldots\ldots, v_\ell \in V$、$e'_1, \ldots\ldots, e'_{\ell-1} \in E$，且对于所有 $i = 1, \ldots\ldots, \ell - 1$，$v_i, v_{i+1} \in e'_i$。

证明。 设 $U \subseteq V$是一个包含极小子集，满足 $|U| \geq 2$，使得

$$\mathsf{wt}(H|_U) \geq k(|U| - 1). \tag{6}$$

注意到，对于任意大小为一的子集 $U' \subseteq V$，$\mathsf{wt}(H|_{U'})$与 $k(|U'| - 1)$均为零点，因此由 U的极小性，对任意非空的 $U' \subsetneq U$，我们有

$$\mathsf{wt}(H|_{U'}) \leq k(|U'| - 1). \tag{7}$$

设 $\mathcal{P}$是将 U分成 t 个部分 P_1，P_2，……，P_t的一个划分，我们将证明

$$\sum_{e \in E|_U} \max\{|\mathcal{P}(e)| - 1, 0\} \geq k(t-1),$$

从而 $H|_U$ 是 k-弱分割连通的。若 $t = 1$，则显然上述不等式的两边均为零点，因此不等式成立。故我们可以假设 $t \geq 2$。

于是我们有：

$$\begin{aligned}
\sum_{e \in E|_U} \max\{|\mathcal{P}(e)| - 1, 0\} &= \sum_{e \in E|_U} \Big(\mathsf{wt}(e) - \sum_{i=1}^{t} \mathsf{wt}(e \cap P_i)\Big) \\
&= \sum_{e \in E|_U} \mathsf{wt}(e) - \sum_{i=1}^{t} \sum_{e \in E|_U} \mathsf{wt}(e \cap P_i) \\
&= \mathsf{wt}(H|_U) - \sum_{i=1}^{t} \mathsf{wt}(H|_{P_i}) \\
&\geq k(|U| - 1) - \sum_{i=1}^{t} k(|P_i| - 1) \\
&= k\Big((|U| - 1) - \sum_{i=1}^{t} (|P_i| - 1)\Big) \\
&= k(t-1),
\end{aligned}$$

其中该不等式由(6)和(7)得到（注意到，根据假设 $t \geq 2$，对任意 $i \in [t]$，P_i 是 U 的一个非空真子集）。 □

我们将使用的弱划分连通超图的主要性质是，它们可以被定向。有向超图 $H = (V, E)$是一个超图，其中在每条超边 $e \in E$中，有一个顶点被指定为头部，其余顶点被指定为尾部。顶点 $v \in V$ 的入度$\deg_{\text{in}}(v)$是以 v 为头部的边的数目。 H中的一条路径是序列 $v_1, e'_1, v_2, e'_2, \ldots, v_{\ell-1}, e'_{\ell-1}, v_\ell$，其中$v_1, \ldots, v_\ell \in V$, $e'_1, \ldots, e'_{\ell-1} \in E$，并且对所有 $i = 1, \ldots, \ell - 1$，顶点 v_i是超边 e'_i的一个尾部，而顶点v_{i+1} 是 e'_i的头部。（无向）超图的一个定向是通过为每条超边指定头部而得到的。

定理 5.5。 超图 $H = (V, E)$ 是 k-弱划分连通的，当且仅当它存在一种定向，使得对于某个顶点 v （即“根”），每个其他顶点 u都存在 k 条到达 v的边不相交路径。

上述定理的证明超出了本综述的范围。有兴趣的读者可参阅 [Fra11, 定理9.4.13和15.4.4]。

最后，以下引理将弱分割连通超图的概念与上一节讨论的 GZP 概念联系起来。

引理 5.6. 设 $H=(V,E)$ 是一个 k-弱分割连通超图，满足 $V=\{v_1,\dots,v_n\}$ 和 $E=\{e_1,\dots,e_m\}$，其中 $n\geq 2$。对于 $i\in[n]$，令 $Z_i=\{j\in[m]\mid v_i\notin e_j\}\subseteq[m]$。那么存在非负整数 $\delta_1,\dots,\delta_n$，其和为 $m-k$，使得取每个 Z_i 的 δ_i 个副本后，可得到一个 *GZP*。

证明。 考虑定理 5.5 给出的 H 的定向。不失一般性，我们可以假设 v_1 是此定向中的根。令 $\delta_1:=\deg_{\text{in}}(v_1)-k$，并令 $\delta_i:=\deg_{\text{in}}(v_i)$，其中 $i>1$ 任意。显然，对于 $i>1$，有 $\delta_i\geq 0$；此外，由于从 v_2 到 v_1 存在 k 条边不相交路径，因此还有 $\delta_1\geq 0$，故 $\deg_{\text{in}}(v_1)\geq k$。此外，由于有 m 条边，δ_i 的和必为 $m-k$。

还需要证明 GZP 性质。考虑任意一个非空多重集 $U\subseteq V$，其中每个顶点 v_i 在 U 中至多出现 δ_i 次。我们将证明 $\left|\bigcap_{i:\ v_i\in U} Z_i\right|\leq\sum_{i:\ v_i\notin U}\delta_i$，因此

$$\Big|\bigcap_{i:v_i\in U} Z_i\Big|\leq\sum_{i:v_i\notin U}\delta_i=m-k-\sum_{i:v_i\in U}\delta_i\leq m-k-|U|,$$

这就得到了 GZP 性质。

为证明 $\left|\bigcap_{i:\ v_i\in U} Z_i\right|\leq\sum_{i:\ v_i\notin U}\delta_i$，首先注意到，该不等式左边等于 E 中不包含 U 中任何顶点的边数。显然，这个数至多等于不在 U 中的顶点的入度之和；当 $v_1\in U$ 时，该和恰好等于右边。接下来假设 $v_1\notin U$，并任取一个顶点 $v_i\in U$。此时，从 v_o 到 v_1 有 k 条边不相交路径。每条路径都必须包含一条头部不在 U 中、但包含 U 中某个顶点的边。因此，左边至多为 $\left(\sum_{i:\ v_i\notin U}\deg_{\text{in}}(v_i)\right)-k$，当 $v_1\notin U$ 时，该值也等于右边。 □

5.1.3 随机求值点上的里德-所罗门码可列表译码至广义辛格尔顿界

接下来，我们将运用前几节引入的高阶 MDS 码和超图连通性概念，证明在从指数级大的域中选取随机求值点时，里德-所罗门码可列表译码至广义辛格尔顿界。为此，我们将使用以下一致性超图的概念。

定义 5.7 (一致性超图**)。** 对于字符串 $c_0,c_1,\dots,c_\ell,w\in\Sigma^n$，我们将 $c_0,c_1,\dots,c_\ell$ 和 w 的一致性超图定义为顶点集为 $\{0,1,\dots,\ell\}$、边为 $e_i:=\{j\in\{0,1,\dots,\ell\}\mid(c_j)_i=w_i\}\subseteq\{0,1,\dots,\ell\}$（其中 $i\in[n]$）的超图（即，每条边 e_i 对应于所有在第 i 个位置上与 w 一致的字符串 c_j）。

命题 5.8. 假设 $c_0,c_1,\dots,c_\ell,w\in\Sigma^n$ 是字符串，且对于任意 $j\in\{0,1,\dots,\ell\}$，都有 $\Delta(c_j,w)\leq\frac{\ell}{\ell+1}\cdot(n-k)$。那么 $c_0,c_1,\dots,c_\ell$ 和 w 的一致性超图 H 的权重至少为 $\ell\cdot k$。

证明。 我们有:

$$\begin{aligned}
\mathsf{wt}(H) &= \sum_{i=1}^{n} \mathsf{wt}(e_i) \\
&\geq \sum_{i=1}^{n} (|e_i| - 1) \\
&= \sum_{i=1}^{n} \left(\left(\sum_{j=0}^{\ell} \mathbf{1}_{(c_j)_i = w_i} \right) - 1 \right) \\
&= -n + \sum_{j=0}^{\ell} (n - \Delta(w, c_j)) \\
&\geq -n + (\ell+1)n - \ell(n-k) = \ell \cdot k.
\end{aligned}$$

□

以下定理说明，高阶 MDS 码的对偶码 达到广义辛格尔顿界。

定理 5.9。 设 $C \subseteq \mathbb{F}^n$ 是码率为 R的线性 最大距离可分码，并假设 $C^\perp$ 是一个高阶 *MDS* 码。那么，对于任意正整数 L， C都是 $(\ {}_{L+1}^{L}(1-R)\ L)$-列表可译码的。

证明。根据假设， C 是最大距离可分码，因此该定理对 $L = 1$ 显然成立。接下来，假设对于某个整数 $L \geq 2$， C 不是 $(\ {}_{L+1}^{L}(1-R)\ L)$- 列表可译码的。那么，存在一个字符串 $w \in \mathbb{F}^n$ 和互不相同的码字 c_0、 c_1、 $\ldots c_L \in C$，使得对于任意 $j \in \{0, 1, \ldots, L\}$，都有 $\Delta(w, c_j) \leq {}_{L+1}^{L}(1-R)n = {}_{L+1}^{L}(n-k)$，其中 $k = \dim(C) = Rn$。令 $H = (\{0, 1, \ldots, L\}, E)$ 为 c_0、 c_1、 ……、 c_L 和w的一致性超图。由命题 5.8 可得 $\mathsf{wt}(H) \geq L \cdot k$。根据引理 5.4，存在一个至少包含两个顶点的子集 $J \subseteq \{0, 1, \ldots, L\}$，使得 $H|_J$ 是 k-弱分割连通的。不失一般性，设对于某个 $\ell \in [L]$，有 $J = \{0, 1, \ldots, \ell\}$。对于 $j \in \{0, 1, \ldots, \ell\}$，令 $Z_j = \{i \in [n] \mid (c_j)_i \neq w_i\} \subseteq [n]$。根据引理 5.6，存在非负整数 δ_0、 δ_1、 ……、 δ_ℓ，其和为 $n - k$，使得对每个 Z_j 取 δ_j 个副本即可得到一个 GZP。

根据假设， $C^\perp$ 是一个高阶 MDS 码，因此存在一个生成矩阵 $G \in \mathbb{F}^{n \times (n-k)}$，对应于$C^\perp$，使得 G 达到上述 GZP。于是， $H := G^T \in \mathbb{F}^{(n-k) \times n}$ 是 C的一个校验矩阵。由于对于任意 $c \in C$, $Hc = 0$，我们有 $Hw = H(w - c_j)$，对于任意 $j \in \{0, 1, \ldots, \ell\}$均成立。此外，根据 Z_j的定义，对于任意 $j \in \{0, 1, \ldots, \ell\}$， $Hw = H(w - c_j)$中对应于 Z_j 的元素均为零。由此可得 $Hw = 0$，因此 $w \in C$。最后，由于 $\ell \geq 1$，必然存在某个 $j \in \{0, 1, \ldots, \ell\}$，使得 $w \neq c_j$。因此， w和c_j是两个不同的码字，且 $\Delta(w, c_j) \leq {}_{L+1}^{L}(n-k) < n - k + 1$，这与 C 是 MDS 码的假设矛盾。 □

接下来，我们希望将上述定理应用于里德-所罗门码。为此，我们需要证明 Reed-Solomon 码的对偶码 是高阶 MDS。众所周知，在整个域上求值的 Reed-Solomon 码 $\mathsf{RS}_q(k)$ 的对偶码也是 Reed-Solomon 码 $\mathsf{RS}_q(n-k)$。对于在域元素子集上求值的 Reed-Solomon 码 $\mathsf{RS}_q(a_1, \ldots, a_n;\ k)$，已知存在非零标量 $b_1, \ldots, b_n \in \mathbb{F}_q$，使得对偶码包含所有形如 $(b_1 \cdot c_1, \ldots, b_n \cdot c_n)$ 的码字，其中 $(c_1, \ldots, c_n) \in \mathsf{RS}_q(a_1, \ldots, a_n;\ n-k)$。注意，若 G 是 $\mathsf{RS}_q(a_1, \ldots, a_n;\ n-k)$ 的生成矩阵，那么 $B \cdot G$ 是 $\mathsf{RS}_q(a_1, \ldots, a_n;\ k)^\perp$ 的生成矩阵，其中 B 是一个对角元素为

$b_1, \ldots, b_n$。由于 G 和 $B \cdot G$ 具有相同的零分量，要证明 $\mathrm{RS}_q(a_1, \ldots, a_n; k)^{\perp}$ 是高阶 MDS，只需证明 $\mathrm{RS}_q(a_1, \ldots, a_n; n-k)$ 是高阶 MDS。

我们将证明，具有随机求值点的 Reed-Solomon 码以高概率是高阶 MDS。证明依赖于以下定理，即所谓的"生成矩阵 MDS（GM-MDS）"定理（该定理的证明超出了本综述的范围，详情请参阅[Lov21, YH19]）。下文中，对于 $Z \subseteq [n]$，令 f_Z 表示由 $f_Z(X, Y_1, \ldots, Y_n) = \prod_{i \in Z}(X - Y_i)$ 给出的 $(n+1)$ 元多项式。此外，对于域 $\mathbb{F}$，令 $\mathbb{F}(Y_1, \ldots, Y_n)$ 表示以不定元 $Y_1, \ldots, Y_n$ 为变量、定义在 $\mathbb{F}$ 上的有理函数域。

定理 5.10（GM-MDS 定理，[Lov21, YH19]）。设 $\mathbb{F}$ 为一个域，且令 $Z_1, \ldots, Z_k \subseteq [n]$ 为一个 *GZP*。则多项式 $f_{Z_1}, f_{Z_2}, \ldots, f_{Z_k}$ 视为以 X 为变量、系数属于 $\mathbb{F}(Y_1, \ldots, Y_n)$ 的一元多项式时，在 $\mathbb{F}(Y_1, \ldots, Y_n)$ 上线性无关。

推论 5.11. 设 q 为一个素数幂，且 k、n 为正整数，使得 $k < n$ 且 $2^{kn} \cdot (kn) < q$。那么，在独立且均匀地选取 a_1、……、$a_n \in \mathbb{F}_q$ 的情况下，至少以 $1 - \frac{2^{kn} \cdot (kn)}{q}$ 的概率，有 $\mathrm{RS}_q(a_1$、……、$a_n; k)$ 是一个高阶 *MDS* 码。

证明. 固定一个 GZP $Z_1, \ldots, Z_k \subseteq [n]$，注意到根据 GZP 性质，对于任意 $j \in [k]$，都有 $|Z_j| \leq k-1$。对于 $j \in [k]$，令 $f'_{Z_j}(X) = f_{Z_j}(X, a_1, \ldots, a_n) = \prod_{i \in Z_j}(X - a_i)$，，并注意到 f'_{Z_j} 是一个系数属于 $\mathbb{F}_q$ 且次数小于 k 的一元多项式。我们将证明，在选择 $a_1, \ldots, a_n \in \mathbb{F}_q$ 的情况下，至少以 $1 - \frac{k \cdot n}{q}$ 的概率，$f'_{Z_1}(X) \ldots, f'_{Z_k}(X)$ 在 $\mathbb{F}_q$ 上线性无关。

为说明上述结论，考虑矩阵 M，其第 j 列是多项式 f_{Z_j} 的系数向量，其中将该多项式视为以 X 为不定元、系数属于 $\mathbb{F}_q(Y_1, \ldots, Y_n)$ 的一元多项式。根据定理 5.10，$f_{Z_1}, \ldots, f_{Z_k}$ 视为以 X 为不定元、系数属于 $\mathbb{F}_q(Y_1, \ldots, Y_n)$ 的一元多项式时，在 $\mathbb{F}_q(Y_1, \ldots, Y_n)$ 上线性无关，因此 M 是 $\mathbb{F}_q(Y_1, \ldots, Y_n)$ 上的满秩矩阵。还要注意，M 中的每个元素都是关于 $\mathbb{F}_q[Y_1, \ldots, Y_n]$ 的多线性多项式，因此，$\det(M)$ 是 $\mathbb{F}_q(Y_1, \ldots, Y_n)$ 上关于 $\mathbb{F}_q[Y_1, \ldots, Y_n]$ 的非零多项式，其总次数至多为 $k \cdot n$。根据 Schwartz-Zippel 引理（引理 2.5），在选择 $a_1, \ldots, a_n \in \mathbb{F}_q$ 时，以至少 $1 - \frac{k \cdot n}{q}$ 的概率，由 M 将 $a_1, \ldots, a_n$ 赋给不定元 $Y_1, \ldots, Y_n$ 得到的矩阵 $M' \in \mathbb{F}_q^{k \times k}$ 在 $\mathbb{F}_q$ 上的行列式非零，因此是满秩的。但请注意，M' 的各列恰好是 $f'_{Z_1}(X) \ldots, f'_{Z_k}(X)$ 的系数向量，因此若 M' 满秩，这些多项式就在 $\mathbb{F}_q$ 上线性无关。

接下来假设 $f'_{Z_1}(X) \ldots, f'_{Z_k}(X)$ 线性无关，并令 $G \in \mathbb{F}_q^{n \times k}$ 为以这些多项式所对应的 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 的码字为列的矩阵。则 G 的列是 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 中的 k 个线性无关码字，因此我们显然有 $\mathrm{Image}(G) = \mathrm{RS}_q(a_1, \ldots, a_n; k)$，从而 G 是该码的生成矩阵。此外，由 $f'_{Z_1}(X) \ldots, f'_{Z_k}(X)$ 的定义，我们也显然有 G 达到 $Z_1, \ldots, Z_k$。

因此我们得出：对任意 GZP $Z_1, \ldots, Z_k \subseteq [n]$，在选取 $a_1, \ldots, a_n \in \mathbb{F}_q$ 时，以至少 $1 - \frac{k \cdot n}{q}$ 的概率，存在 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 的一个生成矩阵，它达到 $Z_1, \ldots, Z_k$。由于 GZP $Z_1, \ldots, Z_k \subseteq [n]$ 的个数至多为 2^{kn}，由并集界，我们得出：在选取 $a_1, \ldots, a_n \in \mathbb{F}_q$ 时，以至少 $1 - 2^{kn} \cdot \frac{k \cdot n}{q}$ 的概率，对任意 GZP $Z_1, \ldots, Z_k \subseteq [n]$，存在 $\mathrm{RS}_q(a_1, \ldots, a_n; k)$ 的一个生成矩阵，它达到 $Z_1, \ldots, Z_k$。 □

结合上述推论与定理 5.9，我们得出结论：在指数级大小的域中随机选取求值点时，Reed-Solomon 码以高概率达到广义辛格尔顿界（特别地，以高概率可列表译码至容量）。经过更多努力，可以证明域大小可在 n 中降至多项式级，甚至线性级，但代价是

只能近似达到广义辛格尔顿界，即对于任意正整数 L 和常数 $\epsilon > 0$（可以证明这是必要的），达到 $\frac{L}{L+1}(1 = \frac{k}{n} - \epsilon)$ 的列表译码半径；更多细节请参阅 [AGG+25]。有趣的开放问题包括：求出显式的求值点，使得在这些点上求值的 Reed-Solomon 码达到列表译码容量；以及设计针对 Reed-Solomon 码、可译码至容量的高效列表译码算法。

5.2 重数码

本节将证明，对于任意求值点集合，重数码都能达到广义辛格尔顿界。具体而言，我们先在下文第 5.2.1 节给出一个简单的概率论证，证明重数码在容量范围内列表可译码，且列表大小为常数，并且该常数以指数级增长地依赖于 $1/\epsilon$。这一论证相当普遍，适用于任何在容量范围内列表可译码、且列表包含于低维子空间的线性码。随后，在第 5.2.2 节，我们将利用重数码更具体的性质，证明重数码甚至能达到广义辛格尔顿界（特别是，列表大小仅线性地依赖于 $1/\epsilon$）。

5.2.1 常数列表大小

本节将基于一个简单的概率论证，证明重数码在容量范围内列表可译码，且列表大小为常数（取决于与容量的间隙 ϵ）。该论证表明，对于距离较大的线性码，列表中来自低维子空间的码字数量不会很多。

更具体地说，我们将证明下面这个相当一般的引理。该引理适用于任意线性码，并指出：如果 C 是一个相对距离为 δ 的线性码，能够从错误比例为（$\delta - \epsilon$）的错误中列表译码，且其列表包含于一个维数至多为 r 的线性子空间中，那么列表大小实际上可以由一个只依赖于 δ、ϵ 和 r 的量上界。在特别情况下，如果 δ、ϵ、r 都是与码长无关的常数，那么列表大小也同样是常数。

引理 5.12。设 $\mathbb{F}$ 为一个有限域，且 $C \subseteq \Sigma^n$ 为一个相对距离为 δ的 $\mathbb{F}$-线性码。进一步设，C 能够从错误比例为（$\delta - \epsilon$）的错误中列表译码，其列表 $\mathcal{L}$ 包含于一个$\mathbb{F}$-线性子空间 $V \subseteq C$ 中，且该子空间的维数为 r。则

$$|\mathcal{L}| \leq \left(\frac{r}{\epsilon(1-\delta)}\right)^{O\left(\frac{r}{\epsilon(1-\delta)} \cdot \log\left(\frac{1}{1-\delta}\right)\right)}.$$

回顾一下，码率为 R 的重数码的相对距离至少为 $\delta = 1 - R$；根据引理 4.3，这些码能够从错误比例为（$\delta - \epsilon$）的错误中列表译码，且其列表包含于一个 $\mathbb{F}$-线性子空间中，该子空间的维数为 $r = O(1/\epsilon)$。由上述引理可知，这些码能够从错误比例为（$1 - R - \epsilon$）的错误中列表译码，且列表大小为数量级（$1/\epsilon$）$^{O(1/\epsilon^2)}$ 的常数。稍后在第 5.2.2 节中，我们将利用重数码更为特有的一些附加性质，进一步将列表大小降至 $O(1/\epsilon)$（甚至一直达到广义辛格尔顿界！）。现在我们转向上述引理 5.12 的证明。

引理 5.12 的证明。 该证明是算法性的：我们将给出一个简单的随机化算法 Prune，给定接收字 $w \in \Sigma^n$ 后，它要么输出一个向量 $v \in V$，要么输出 $\perp$。我们保证，对于任意 $v \in \mathcal{L}$，算法 Prune 以至少 $\underline{p_0} = p_0(\delta, \epsilon, r)$ 的概率输出 v，进而可得 $|\mathcal{L}| \leq \frac{1}{p_0}$。

Prune 算法的工作方式如下。对于某个稍后确定的参数 t，它均匀且独立地随机选取条目$i_1, i_2, \ldots, i_t \in [n]$，并令 $I := \{i_1, \ldots, i_t\}$。接着，算法检查是否存在唯一一个在 I 上与 w 一致的 $v \in V$（也就是说，对于所有 $i \in I$，都有 $v_i = w_i$）。如果存在，则输出该唯一元素 v；否则（即这样的 v 要么不存在，要么多于一个），则输出 $\perp$。

我们希望证明，对于任意 $v \in \mathcal{L}$，算法以常数概率 p_0（该概率仅取决于 δ，ϵ 和 r）输出 v。固定这样一个 $v \in \mathcal{L}$。令 E_1 表示事件：v 在 I上与 w 一致；令 E_2 表示事件：V中的两个不同码字在 I上相同。注意，当且仅当事件E_1 发生且事件 E_2 不发生时，算法才会输出 v，因此输出 v 的概率至少为 $\Pr[E_1] - \Pr[E_2]$。下面两个命题分别给出事件 E_1 和 E_2的概率的下界和上界。

命题 5.13。$\Pr[E_1] \geq (1 - \delta + \epsilon)^t$.

证明。 这是因为 $v \in \mathcal{L}$，因此对于至少 $(1 - \delta + \epsilon)$ 比例的条目 $i \in [n]$，$v_i = w_i$成立；并且$i_1, \ldots, i_t \in [n]$ 是均匀且相互独立地随机选取的。 □

命题 5.14. $\Pr[E_2] \leq (1 - \delta)^t \cdot \left(\frac{t}{1-\delta}\right)^r$.

证明. 对于 $i \in [n]$，令 $A_i := \{v \in C \mid v_i = 0\}$，令 $V_0 := V$，并且对于 $j = 1, \ldots\ldots, t$，令

$$V_j := V \cap A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j},$$

以及 $r_j := \dim_{\mathbb{F}}(V_j)$。注意到 $r = r_0 \geq r_1 \geq \ldots \geq r_t$，且事件 E_2成立当且仅当 $r_t > 0$。另请注意，对于任意非零 $v \in V$，都有 $|v| \geq \delta n$，因为 $V \subseteq C$ 且 C 的相对距离为 δ。

接下来我们声称，对于任意 $j = 0, 1, \ldots\ldots, t-1$，以至少 δ 的概率（对 i_{j+1}的选择而言），有 $r_{j+1} \leq \max\{0, r_j - 1\}$。为此，首先注意，如果 $r_j = 0$，那么 $r_{j+1} \leq r_j \leq 0$，因此结论成立。否则，如果 $r_j \neq 0$，则存在一个非零向量 $v \in V_j$。回想 $V_j \subseteq V$，可得 $|v| \geq \delta n$，因此以至少 δ 的概率（对 i_{j+1}的选择而言），有 $v_{i_{j+1}} \neq 0$。但回想$V_{j+1} \subseteq A_{i_{j+1}}$，这又意味着 $v \notin V_{j+1}$。因此在这种情况下，存在一个非零 $v \in V_j$，使得$v \notin V_{j+1}$，于是 V_{j+1} 的维数严格小于 V_j的维数。

最后，注意如果 $r_t > 0$，那么对于至少 $t - r + 1$ 个 j，必有 $r_{j+1} > \max\{0, r_j - 1\}$，其中这些 j取自 $0, 1, \ldots\ldots, t-1$。根据上述结果及并集界，该事件发生的概率至多为

$$\binom{t}{t-r+1} \cdot (1-\delta)^{t-r+1} \leq (1-\delta)^t \cdot \left(\frac{t}{1-\delta}\right)^r.$$

□

根据上述断言5.13和5.14，我们得出，任意 $v \in \mathcal{L}$ 由算法 Prune 以至少……的概率输出

$$p_0 \geq \Pr[E_1] - \Pr[E_2] \geq (1 - \delta + \epsilon)^t - (1-\delta)^t \cdot \left(\frac{t}{1-\delta}\right)^r.$$

最后，在上述表达式中令 $t := 3 \cdot \epsilon^{r}(1-\delta)$ 对数 $\left(\epsilon^{r}(1-\delta)\right)$，我们得到

$$
\begin{aligned}
p_0 : &= (1-\delta+\epsilon)^t - (1-\delta)^t \cdot \left(\frac{t}{1-\delta}\right)^r \\
&\geq (1-\delta)^t \cdot \left[(1+\epsilon)^t - \left(\frac{t}{1-\delta}\right)^r\right] \\
&\geq (1-\delta)^t \cdot \left[\left(\frac{r}{\epsilon(1-\delta)}\right)^{3\cdot r} - \left(3 \cdot \frac{r}{\epsilon(1-\delta)^2} \cdot \log\left(\frac{r}{\epsilon(1-\delta)}\right)\right)^r\right] \\
&\geq (1-\delta)^t \\
&\geq (1-\delta)^{O\left(\frac{r}{\epsilon(1-\delta)} \cdot \log\left(\frac{r}{\epsilon(1-\delta)}\right)\right)},
\end{aligned}
$$

其中，倒数第二个不等式在比值 $\epsilon^{r}(1-\delta)$ 足够大时成立。由此可得

$$
|\mathcal{L}| \leq \frac{1}{p_0} \leq \left(\frac{1}{1-\delta}\right)^{O\left(\frac{r}{\epsilon(1-\delta)} \cdot \log\left(\frac{r}{\epsilon(1-\delta)}\right)\right)} = \left(\frac{r}{\epsilon(1-\delta)}\right)^{O\left(\frac{r}{\epsilon(1-\delta)} \cdot \log\left(\frac{1}{1-\delta}\right)\right)},
$$

至此，引理得证。 □

5.2.2 广义 Singleton界

本节将证明，重数码（近似地）达到了定理 2.2 的广义辛格尔顿界，这尤其意味着重数码的列表大小仅线性地依赖于 $1/\epsilon$。

更具体地说，下面固定一个素数幂 q、互异的求值点 a_1、…、$a_n \in \mathbb{F}_q$，以及正整数 s、k，使得 $k < sn$ 且 $\max\{k, s\} \leq \mathrm{char}(\mathbb{F}_q)$，并令 $\mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$ 为相应的重数码。我们将证明，对于任意正整数 $L < s$，$\mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$ 对 $\alpha < \frac{L}{L+1}(1 - \frac{k}{n}(s-L+1))$ 是 (α, L)-列表可译码的。特别地，若令 $R := \frac{k}{s \cdot n}$ 表示该码的码率，则它可从 $\frac{L}{L+1}(1 - \frac{s}{s-L+1} \cdot R)$ 的错误比例进行列表可译码，列表大小为 L。因此，对于任意 $\epsilon > 0$，我们可以选择 $s = \Theta(L/\epsilon)$，使错误比例至少为 $\frac{L}{L+1}(1 - R - \epsilon)$。特别地，我们可以选择 $s = \Theta(1/\epsilon^2)$，使重数码 $\mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$ 能够从 $(1 - R - \epsilon)$ 的错误比例进行列表可译码，列表大小为 $O(1/\epsilon)$。

根据命题 5.8，这将是下述引理的推论。

引理 5.15. 设 q 为素数幂，设 $a_1, \ldots, a_n$ 为 $\mathbb{F}_q$ 中的互异点，并设 s, k, ℓ 为正整数，使得 $\ell < s, k < sn$，且 $\max\{k, s\} \leq \mathrm{char}(\mathbb{F}_q)$。设 $w \in (\mathbb{F}_q^s)^n$ 为字符串，设 $c_0, c_1, \ldots, c_\ell$ 为 $\mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$ 中的互异码字，并设 H 为 $c_0, c_1, \ldots, c_\ell$ 与 w 的一致性超图（参见定义 5.7）。则 $\mathrm{wt}(H) < \frac{\ell}{s-\ell+1} \cdot k$。

在证明上述引理之前，我们说明该引理意味着 $\mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$ 对于 $\alpha < \frac{L}{L+1}(1 - \frac{k}{n}(s-L+1))$ 是 (α, L)- 列表可译码的。为此，反设 $\mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$ 不是 (α, L)- 列表可译码的。那么存在一个字符串 $w \in (\mathbb{F}_q^s)^n$ 以及码字 $c_0, c_1 \ldots, c_L \in \mathrm{mult}_q^{(s)}(a_1, \ldots, a_n;\ k)$，使得对于任意 $j \in \{0, 1, \ldots, L\}$，$\Delta(w, c_j) \leq \frac{L}{L+1}(n - \frac{k}{s-L+1})$。令 H 为 $c_0, c_1, \ldots, c_L$ 和 w 的一致性超图。那么根据命题 5.8，H 的权重至少为 $L \cdot \frac{k}{s-L+1}$，这与上述引理 5.15 矛盾。

在引理 5.15 的证明中，我们首先回顾第 5.2.1 节中的结论：对于任意 $\mathbb{F}$-线性码$C \subseteq \Sigma^n$以及任意 $\mathbb{F}$-线性子空间 $V \subseteq C$，对于随机的$i \in [n]$，交 $V \cap A_i$ 的维数通常很小，其中 $A_i := \{v \in C \mid v_i = 0\}$。在引理 5.15 的证明中，我们首先针对重数码这一特殊情形，证明随机 $i \in [n]$ 下 $V \cap A_i$ 期望维数的一个更紧的上界。

引理 5.16。令 q 为素数幂，令 a_1、...、a_n 为 $\mathbb{F}_q$中的互异点，并令 s、k 为满足 $k < sn$ 且 $\max\{k, s\} \leq$ *char*$(\mathbb{F}_q)$的正整数。令 $V \subseteq \mathsf{mult}_q^{(s)}(a_1、...、a_n;\ k)$ 为维数为 $r \leq s$的 $\mathbb{F}_q$-线性子空间，并且对于 $i \in [n]$，令 $A_i := \{v \in \mathsf{mult}_q^{(s)}(a_1、...、a_n;\ k) \mid v_i = 0\}$。则有：

$$\sum_{i=1}^{n} \dim(A_i \cap V) \leq \frac{r}{s-r+1} \cdot k.$$

证明。令 c_1、...、c_r 为 V的一组基，并令 $f_1(X)$ ...、$f_r(X) \in (\mathbb{F}_q)_{<k}[X]$ 为与这些码字对应的多项式。令 $W(X)$为多项式环 $\mathbb{F}_q[X]$上的 $r \times r$ 朗斯基矩阵，其定义为

$$W(X) = \begin{pmatrix} f_1(X) & f_2(X) & \cdots & f_r(X) \\ f_1^{(1)}(X) & f_2^{(1)}(X) & \cdots & f_r^{(1)}(X) \\ \vdots & \vdots & \vdots & \vdots \\ f_1^{(r-1)}(X) & f_2^{(r-1)}(X) & \cdots & f_r^{(r-1)}(X) \end{pmatrix},$$

并令 $D(X) := \det(W(X)) \in \mathbb{F}_q[X]$。

那么，$D(X)$ 是一个次数至多为 $(k-1) \cdot r$ 的多项式。接下来，我们断言 $D(X) \neq 0$。有趣的是，一种证明方法是利用引理 4.3；该引理表明，重数码的列表包含在一个低维子空间中。具体来说，反设 $D(X) \neq 0$。那么，$W(X)$ 在有理函数域 $\mathbb{F}_q(X)$ 上是奇异的，因此存在一个非平凡的行线性组合，其和为零。也就是说，存在 $B_0(X)$ $B_1(X) \ldots, B_{r-1}(X) \in \mathbb{F}_q[X]$，它们不全为零，使得对任意$t = 1, \ldots, r$，

$$B_0(X) \cdot f_t(X) + B_1(X) \cdot f_t^{(1)}(X) + \cdots + B_{r-1}(X) \cdot f_t^{(r-1)}(X) = 0.$$

因此，引理 4.3 推出 $f_1(X) \ldots, f_r(X)$ 位于一个 $(r-1)$ 维子空间中，这与我们的假设矛盾：它们张成一个 r 维子空间。

接下来我们证明，对于任意 $i \in [n]$，$D(X)$，其在每个元素 a_i 处的重数至少为 $(s-r+1) \cdot \dim(A_i \cap V)$。为此，固定 $i \in [n]$，并令 $r_i := \dim(A_i \cap V)$。我们要证明 $D(X)$ 在 a_i 处的重数至少为 $(s-r+1) \cdot r_i$；根据 Hasse 导数的定义，这等价于 $(X-a_i)^{(s-r+1)\cdot r_i}$ 整除 $D(X)$。

为证明上述结论，首先注意到，对 $W(X)$ 的列进行初等变换只会将 $D(X)$ 改变一个常数乘性因子，因此我们不妨假设 $f_1(X) \ldots, f_{r_i}(X)$ 构成 $A_i \cap V$ 的一组基，从而对任意 $t = 1, 2, \ldots, r_i$ 以及 $j = 0, 1, \ldots, s-1$，有 $f_t^{(j)}(a_i) = 0$。因此 $f_1(X) \ldots, f_{r_i}(X)$ 在 a_i 上均以至少 s 的重数取零，从而 $(X-a_i)^s$ 整除所有这些多项式。此外，对任意 $t = 1, 2, \ldots, r_i$ 以及 $j = 0, 1, \ldots, r-1$，$(X-a_i)^{s-r+1}$ 整除 $f_t^{(j)}(X)$，因为求导至多使每个单项式的次数降低 1。因此我们得出 $(X-a_i)^{s-r+1}$ 整除前 r_i 列中的每一项，进而 $(X-a_i)^{(s-r+1)\cdot r_i}$ 整除 $W(X)$ 的行列式 $D(X)$。

因此我们得出， $D(X)$ 是一个次数至多为 $(k-1)\cdot r$ 的非零多项式，它在每个 a_i 上以至少 $(s-r+1)\cdot \dim(A_i \cap V)$ 的重数取零。因此，我们有

$$\sum_{i=1}^{n}(s-r+1)\cdot \dim(A_i \cap V) \le (k-1)\cdot r.$$

将上述不等式两边除以 $s-r+1$，即可得出所需结论。 □

现在我们转而证明引理 5.15，该证明基于上述引理 5.16。

引理 *5.15* 的证明。 我们对 ℓ 使用归纳法。对于基例 $\ell = 1$，考虑一个字符串 $w \in (\mathbb{F}_q^s)^n$ 以及一对不同的码字 $c_0, c_1 \in \mathsf{mult}_q^{(s)}(a_1, \ldots, a_n; k)$，并令 $H = (\{0,1\}, E)$ 为相应的一致性超图。那么我们有

$$\mathsf{wt}(H) = \sum_{e\in E}\max\{|e|-1, 0\} = |\{i \in [n] \mid (c_0)_i = (c_1)_i = w_i\}| \le n - \Delta(c_0, c_1) < \frac{k}{s},$$

这就证明了 $\ell = 1$ 情形。

对于归纳步骤，固定 $1 < \ell < s$。我们假设引理 5.15 对任意 $1 \le \ell' < \ell$ 均成立，并证明它对 ℓ 也成立。令 $w \in (\mathbb{F}_q^s)^n$ 为一个字符串，并令 $c_0, c_1, \ldots, c_\ell$ 为 $\mathsf{mult}_q^{(s)}(a_1, \ldots, a_n; k)$ 中互不相同的码字。不失一般性，我们可以假设 $c_0 = 0$，否则可以将 w 和 $c_0, c_1, \ldots, c_\ell$ 平移 c_0。令 $H = (\{0,1,\ldots,\ell\}, E = \{e_1, \ldots, e_n\})$ 为相应的一致性超图，并反设 $\mathsf{wt}(H) \ge \frac{\ell}{s-\ell+1}\cdot k$。

令 $V :=$ 张成空间$\{c_0, c_1, \ldots, c_\ell\}$，令 $r := \dim(V)$，并注意到根据假设，$1 \le r \le \ell$ $c_0 = 0$。不失一般性，我们还可以进一步假设 $c_1, \ldots, c_r$ 是 V 的一组基。令 $\mathcal{P}$ 为将$\{0,1,\ldots,\ell\}$ 划分为 $r+1$ 个部分 $P_0, P_1, \ldots, P_r$ 的一个划分，其中对于 $t \in \{0,1,\ldots,r\}$，

$$P_t := \{j \in [\ell] \mid c_j \in \mathrm{span}\{c_0, c_1, \ldots, c_t\} \setminus \mathrm{span}\{c_0, c_1, \ldots, c_{t-1}\}\}.$$

对于 $i \in [n]$，令 $A_i := \{v \in \mathsf{mult}_q^{(s)}(a_1, \ldots, a_n; k) \mid v_i = 0\}$。那么，主要观察结果如下。

断言 5.17。 *对于任意 $i \in [n]$，都有 $\dim(A_i \cap V) \ge \max\{|\mathcal{P}(e_i)| - 1, 0\}$，其中 $|\mathcal{P}(e_i)|$ 表示与 e_i 相交的划分部分的数量。*

证明。 固定 $i \in [n]$。当 $e_i = \emptyset$ 时，结论显然成立，因此接下来假设 $e_i \ne \emptyset$，并令 $V_i =$ 表示$\{c_j | j \in e_i\}$ 中所有码字张成的空间，其中 e_i。

首先假设 $w_i = 0$。此时，V_i 中所有码字的第 i 个分量都是零，因此 $V_i \subseteq A_i \cap V$。此外，我们有 $c_0 = 0 \in e_i$，所以 e_i 与 P_0相交。假设 e_i 还与划分 $\mathcal{P}$ 中其他的 t 部分相交。那么 e_i 包含 t 个线性无关的向量，因此 $t \le \dim(V_i) \le \dim(A_i \cap V)$。所以在这种情况下，我们有 $\dim(A_i \cap V) \ge t = |\mathcal{P}(e_i)| - 1$。

接下来假设 $w_i \ne 0$，并令 c_j 为 e_i 中任意一个码字。由于 e_i 中的所有码字在第 i 个位置上都相同，因此 e_i 中的所有码字都包含在 $c_j + A_i \cap V$ 中，于是 $\dim(V_i) \le \dim(A_i \cap V) + 1$。此外，$0 \notin e_i$，因此 e_i 与 P_0 不相交。假设 e_i 与划分 $\mathcal{P}$ 中的 t 个部分相交。那么 e_i 包含 t 个线性无关向量，因此 $t \le \dim(V_i) \le \dim(A_i \cap V) + 1$。所以在这种情况下，我们也有 $\dim(A_i \cap V) \ge t - 1 = |\mathcal{P}(e_i)| - 1$。 □

根据 a 上述断言，并使用与引理 5.4 的证明中相同的计算，我们得到 at

$$\begin{aligned}\sum_{i\in[n]}\dim(A_i\cap V) &\geq \sum_{e\in E}\max\{|\mathcal{P}(e)|-1,0\}\\ &= \mathsf{wt}(H)-\sum_{t=0}^{r}\mathsf{wt}(H|_{P_t})\\ &> \frac{\ell}{s-\ell+1}\cdot k-\sum_{t=0}^{r}\frac{|P_t|-1}{s-|P_t|+2}\cdot k\\ &> \frac{\ell}{s-\ell+1}\cdot k-\frac{\sum_{t=0}^{r}(|P_t|-1)}{s-\ell+2}\cdot k\\ &= \frac{\ell}{s-\ell+1}\cdot k-\frac{\ell-r}{s-\ell+1}\cdot k\\ &= \frac{r}{s-\ell+1}\cdot k,\end{aligned}$$

其中，在第二个不等式中，我们用到了假设 $\mathsf{wt}(H)\geq\frac{\ell}{s-\ell+1}\cdot k$，以及根据归纳假设，对任意 $t\in\{0,1,\ldots,r\}$，都有 $\underline{\mathsf{wt}(H|_{P_t})}<\frac{|P_t|-1}{s-|P_t|+2}\cdot k$（因为 $\mathcal{P}$是真划分）。最后，回想起 $r\leq\ell$，上述不等式与引理 5.16 矛盾，由此完成本引理的证明。 □

5.3 子域求值点上的里德-所罗门码

在本节中，我们证明，子域求值点上的里德-所罗门码的某个子码可（高效地）列表译码至容量，且列表大小为常数（取决于与容量的间隙 ϵ）。对于子域求值点上的里德-所罗门码，引理 4.9 仅给出了列表维数的线性上界，因此，第 5.2.1 节中用于减小列表大小的方法不适用于这种情形。

在这种情形下，能够缩小列表大小的关键观察是，引理 4.9 的证明实际上表明，该列表具有一种更精细的低维周期性 结构。具体而言，存在一个维数为常数 $r=O(1/\epsilon)$的 $\mathbb{F}_q$线性子空间$\hat{}$ $V\subseteq\mathbb{F}_{q^s}$，使得以下结论成立：对于任意$i\in\{0,1,\ldots,k-1\}$，若多项式 $f(X)$所对应的码字属于该列表，那么给定前 i 个系数 f_0，f_1，…，$f_{i-1}\in\mathbb{F}_{q^s}$后，下一个系数 f_i 属于$\hat{}V$的一个仿射平移（该仿射平移仅依赖于 f_0，f_1，…，f_{i-1}）。[5]这启发了下面的定义。下文中，对于一个向量 $v\in\mathbb{F}^{sk}$，记 $v=(v_{s,\,1},\ldots,v_{s,\,k})$，其中$v_{s,\,i}$表示 v 中长度为 s的第 i个块。

定义 5.18（周期子空间）。设 $\mathbb{F}$ 是一个有限域，且 k、s、r 是正整数。若存在一个维数为 r 的线性子空间 $\hat{}\,V\subseteq\mathbb{F}^s$，使得下述条件成立，则线性子空间 $V\subseteq\mathbb{F}^{sk}$ 称为（k、s、r）-周期子空间：对于任意 $v\in V$ 和 $i\in\{1,2,\ldots,k\}$，都存在一个仅取决于$\hat{}v_{s,\,1}$、……、$v_{s,\,i-1}$ 的 $z_i\in\mathbb{F}^s$，使得 $v_{s,\,i}\in z_i+V$。

[5]回顾引理 4.9 的证明可知，对于任意 $i\in\{0,1,\ldots,k-1\}$，f_i必须满足 $B(f_i)=-y_i$，其中 y_i仅取决于 f_0，f_1，……，f_{i-1}，且 $B(X)=\sum_{\ell=0}^{r-1}B_\ell(0)X^{q^\ell}$。因此，我们有 $f_i\in z_i+\hat{}V$，其中 $\hat{}V\subseteq\mathbb{F}_{q^s}$表示 $B(X)$ 的根集合，而 $z_i\in\mathbb{F}_{q^s}$满足 $B(z_i)=-y_i$。最后，注意到根据 $B(X)$ 的线性结构，$\hat{}V$是一个维数至多为 $r-1$ 的 $\mathbb{F}_q$-线性子空间。

根据上述结果，对于 a_1、……、 $a_n \in \mathbb{F}_q$，以子域元素为求值点的 Reed-Solomon 码 $\mathrm{RS}_{q^s}(a_1, \ldots\ldots, a_n; k)$ 可纠正 $(1-R-\epsilon)$ 比例的错误；其码字属于列表的多项式都包含在一个 $(k、 s、 r)$-周期子空间中，其中 $r = O(1/\epsilon)$（将每个多项式 $f(X) \in \mathbb{F}_{q^s}[X]$ 视为次数小于 k 的多项式，并将其表示为 $\mathbb{F}_{q^s}$ 中 k 个系数的级联；通过某个 $\mathbb{F}_q$-线性双射将 $\mathbb{F}_{q^s}$ 与 $\mathbb{F}_q^s$ 等同，并以自然方式将 $(\mathbb{F}_q^s)^k$ 与 $\mathbb{F}_q^{sk}$ 等同）。这种周期结构能够产生一个具有列表且列表维数为常数维数的 $\mathbb{F}_q$- 线性子码（根据引理 5.12，其列表大小也为常数大小）：只保留码中对应多项式属于周期规避子空间的码字即可。该子空间规模较大，且与任意周期子空间的交维数都很低。

定义 5.19（周期规避子空间）。设 $\mathbb{F}$ 是一个有限域，且 k、 s、 r、 t 是正整数。若对于任意$(k、 s、 r)$周期子空间 $V \subseteq \mathbb{F}^{sk}$，线性子空间 $W \subseteq \mathbb{F}^{sk}$ 满足（k、 s、 r、 t）-周期规避子空间 的条件维数$(W \cap V) \leq t$，则称 $W \subseteq \mathbb{F}^{sk}$ 是（k、 s、 r、 t）-周期规避子空间。

获得周期规避子空间的一种方法是利用子空间设计这一概念。子空间设计是 $\mathbb{F}^s$ 的一族大子空间，其与任意低维子空间的交在平均意义上具有较低维数。

定义 5.20（子空间设计）。设 $\mathbb{F}$ 是一个有限域，且 k、 s、 r、 t 是正整数。若对于任意维数为 r 的线性ˆ子空间 $V \subseteq \mathbb{F}^s$， H_1、……、 $H_k \subseteq \mathbb{F}^s$ 这组 k 个子空间满足维数$(\hat{}V \cap H_i) \leq t$，则称其为（$r$、 t）-子空间设计。

下一个断言表明，如果 $H_1, \ldots, H_k$是子空间设计，那么 $H_1 \times H_2 \times \cdots \times H_k$就是具有相同参数的周期规避子空间。

断言 5.21. 设 $\mathbb{F}$ 是一个有限域，并设 k、 s、 r、 t 为正整数。假设一族 k子空间 H_1、...、 $H_k \subseteq \mathbb{F}^s$ 构成一个(r, t)-子空间设计。那么 $W := H_1 \times H_2 \times \cdots \times H_k \subseteq \mathbb{F}^{sk}$ 是一个(k, s, r, t)-周期规避子空间。

证明。设 $V \subseteq \mathbb{F}^{sk}$是一个 (k, s, r)-周期子空间，且 $V' := V \cap W$。由于 V和 W都是 $\mathbb{F}$上的线性子空间，因此 V'也是如此。因此，要证明 V' 的维数至多为 t，只需证明 V'的大小至多为 q^t。

ˆ 要理解上述内容，请回顾：由于 V 是一个 (k, s, r)-周期子空间，因此存在一个维数至多为 r 的子空间 $V \subseteq \mathbb{F}^s$，使得对于任意 $v \in V$ 和 $i \in \{1, \ldots, k\}$，都存在一个仅取决于 $v_{s,}1, \ldots, v_{s,i-1}$ 的 $z_i \in \mathbb{F}^s$，从而 $v_{s,i} \in z_i + \hat{}V$。根据 W 的定义，这又意味着对于任意 $v \in V' = V \cap W\hat{}$ 和 $i \in \{1, \ldots, k\}$，都存在一个仅取决于 $v_{s,}1, \ldots, v_{s,i-1}$ 的 $z_i \in \mathbb{F}^s$，从而 $v_{s,i} \in (z_i + V) \cap H_i$。因此，给定 $v_{s,}1, \ldots, v_{s,i-1}$ 的取值，$v_{s,i}$ 至多有 $q^{\dim(\hat{V} \cap H_i)}$ 种可能取值。因此，V' 的总大小至多为

$$\prod_{i=1}^{k} q^{\dim(\hat{V} \cap H_i)} = q^{\sum_{i=1}^{k} \dim(\hat{V} \cap H_i)} \leq q^t,$$

其中，上界成立是因为 $H_1, \ldots, H_k$是一个（k, s, r, t）-子空间设计。 □

下一个定理给出了一个子空间设计的显式构造，其中包含较大的子空间 $H_1, \ldots, H_k$，且它们与任意低维子空间的交总维数都很小。有趣的是，该构造依赖于重数码的列表译码性质！

定理 5.22. 对于任意素数幂 q、素数 d 以及满足 $s < 2rk$、$\max\{2r, s\} < \mathit{char}(\mathbb{F}_q)$ 和 $k \leq \frac{q^d - q}{d}$ 的正整数 k, s, r，存在一个 $(r, \frac{s}{d})$-子空间设计$H_1, \ldots, H_k \subseteq \mathbb{F}_q^s$ 的显式构造，其中每个子空间 H_i 的余维数为 $2rd$。

证明. 我们首先注意到，引理 5.16 蕴含了该定理关于 $d=1$ 和 $k \le q$ 的一个版本。为此，取 $\mathbb{F}_q$ 中互不相同的元素 $a_1, a_2, \ldots, a_k$，并令 $i \in [k]$,

$$H_i := \left\{ f(X) \in (\mathbb{F}_q)_{<s}[X] \mid f(a_i) = f^{(1)}(a_i) = \cdots = f^{(2r-1)}(a_i) = 0 \right\},$$

其中，我们将多项式 $f(X) \in (\mathbb{F}_q)_{<s}[X]$ 视为 $\mathbb{F}_q^s$ 中系数构成的向量。于是，每个 H_i 的余维至多为 $2r$，因为形如 $f^{(j)}(a_i) = 0$ 的任一条件都会对 H_i 中多项式的系数施加一个线性约束。令 $\hat{}$ $V \subseteq (\mathbb{F}_q)_{<s}[X]$ 为一个 r 维子空间。对于 $i \in [n]$，令A_i为 $\mathrm{mult}_q^{(2r)}(a_1, \ldots\ldots, a_k; s)$ 中与 H_i 中多项式对应的码字集合，并令 V为该码中与 V 中多项式对应的码字集合。于是，使用 k 个互不相同的求值点、重数参数 $2r$和次数参数 s 应用引理 5.16，可得

$$\sum_{i=1}^{n} \dim(H_i \cap \hat{V}) = \sum_{i=1}^{n} \dim(A_i \cap V) \le \frac{r}{r+1} \cdot s \le s.$$

要将证明推广到 $d>1$，并得到更大的子空间族 H_i，可以从扩域 $\mathbb{F}_{q^d}$ 中选取 a_i。具体而言，取 a_1、a_2、……、a_k为 $\mathbb{F}_{q^d}$ 中的元素，使得对于 $i \in [k]$ 和 $\ell \in \{0,1,\ldots,d-1\}$，所有形如$a_i^{q^\ell}$ 的元素都互不相同。注意，若 d 是素数，则任意元素 $a \in \mathbb{F}_{q^d} \setminus \mathbb{F}_q$ 的幂 a、a^q、……、$a^{q^{d-1}}$均互不相同。因此，在这种情况下，可以在 $\mathbb{F}_{q^d}$ 中找到至少 $k = \frac{q^d-q}{d}$ 个满足上述要求的元素 a_1、……、a_k。

与 $d=1$ 情形类似，对于 $i \in [k]$，令

$$H_i := \left\{ f(X) \in (\mathbb{F}_q)_{<s}[X] \mid f(a_i^{q^\ell}) = f^{(1)}(a_i^{q^\ell}) = \cdots = f^{(2r-1)}\left(a_i^{q^\ell}\right) = 0 \text{ for any } \ell = 0,1,\ldots,d-1 \right\},$$

其中，我们将多项式 $f(X) \in (\mathbb{F}_q)_{<s}[X]$ 视为 $\mathbb{F}_q^s$ 中的系数向量。可以验证，每个 H_i 的余维数至多为 $2rd$。此外，引理 5.16 的证明表明，

$$\sum_{i \in [k]} \dim(H_i \cap \hat{V}) \le \frac{r}{d \cdot (r+1)} \cdot s \le \frac{s}{d}$$

$\hat{}$ 对于任意 r 维子空间 $V \subseteq (\mathbb{F}_q)< s[X]$。 □

在上述定理 5.22 中令 $d = \frac{\epsilon s}{2r}$（假设 $r \le \frac{\epsilon s}{2}$），可得以下推论。

推论 5.23 (显式子空间设计)。 对于任意素数幂 q、 $\epsilon > 0$，以及满足 $s < 2rk$、 $s <$ 特征$(\mathbb{F}_q)$、 $q^s \ge (k \cdot \frac{\epsilon s}{2r})^{2r/\epsilon}$ 和 $r < \frac{\epsilon s}{2}$ 的正整数 k、s、r，存在一个显式构造的 $(r, \frac{2r}{\epsilon})$-子空间设计 $H_1, \ldots, H_k \subseteq \mathbb{F}_q^s$，其中每个子空间 H_i 的余维数为 ϵs。

回忆一下，根据引理 4.9，在子域求值点上定义的 Reed-Solomon 码 $\mathrm{RS}_{q^s}(a_1, \ldots, a_n; k)$，对于 $a_1, \ldots, a_n \in \mathbb{F}_q$ 和 $s = \Theta(1/\epsilon^2)$，可从 $(1-R-\epsilon)$ 的错误比例下进行列表译码；列表中对应码字的多项式包含在一个 (k, s, r)-周期子空间中，该子空间用于 $r = O(1/\epsilon)$。令 $H_1, \ldots, H_k$ 为上述推论针对这些参数给出的子空间设计，并回忆一下，根据断言 5.21， $W := H_1 \times H_2 \times \cdots \times H_k$ 是一个 $(k, s, r, \frac{2r}{\epsilon})$-周期规避子空间。令 $C \subseteq \mathrm{RS}_{q^s}(a_1, \ldots, a_n; k)$ 为子码，它由与满足以下条件的多项式 $f(X) = \sum_{i=0}^{k-1} f_i X^i \in \mathbb{F}_{q^s}[X]$ 相关联的所有码字组成：对于任意 $i \in \{0,1,\ldots,k-1\}$，均有 $f_i \in H_{i+1}$。那么， C 的码率为 $R-\epsilon$，且可从 $(1-R-\epsilon)$ 的错误比例下进行列表可译码，列表维数为 $O(1/\epsilon^2)$（根据引理 5.12，这也意味着该子码的列表大小至多为 $\exp(\mathrm{poly}(1/\epsilon))$）。

最后，注意到 C 可按如下方式在多项式时间内达到容量进行列表译码。首先注意，根据引理 4.9，通过求解一个线性方程组，可以在多项式时间内求出包含 $\mathrm{RS}_{q^s}(a_1, \ldots, a_n;\ k)$ 列表的 (k, s, r)-周期子空间 V 的一个基。然后，通过求解另一个线性方程组，求出 V 与包含所有系数属于 $W = H_1 \times \cdots \times H_k$ 的次数为 k 的多项式编码的子空间的交，即可在多项式时间内求出包含 C 列表的 $O(1/\epsilon^2)$ 维子空间 V' 的一个基。最后，由于 V' 的大小为 $q^{O(1/\epsilon^2)}$，因此可以在 $q^{O(1/\epsilon^2)}$ 时间内找到列表中的所有元素；当 ϵ 为常数且 $q = \mathrm{poly}(n)$ 时，该时间关于码长为多项式。

5.4 文献注记

高阶 MDS 码。 高阶 MDS 码的概念由 Brakensiek、Gopi 和 Makam [BGM22] 以及 Roth [Rot22]分别独立提出。在 [Rot22], 中，高阶 MDS 码被定义为达到广义辛格尔顿界的码；而在 [BGM22], 中，则根据其生成矩阵的列子集所张成的子空间的交的维数来定义。第 5.1.1 节中给出的高阶 MDS 码定义，是基于生成矩阵各列零点模式的交的大小；这一后来的定义见 Brakensiek、Gopi 和 Makam 的另一篇论文 [BGM25]。该论文还证明了上述三种定义彼此等价（在对偶意义下）。事实 5.1 在 [DSY14], 中被称为 MDS 条件，其证明似乎早已广为人知。

超图连通性。 Király [Kir03] 引入了超图的边连通度 这一概念，并证明了适用于超图的 Menger 定理 。该定理指出，边连通度等价于任意一对顶点之间存在多条边不相交路径（此定理推广了图论中广为人知的 Menger 定理 [Men27]）。超图的（弱）划分连通性 概念在组合学 [FKK03a, FKK03b, Kir03] 和优化 [JMS03, FK08, Fra11, CX18], 中得到了深入研究，并推广了广为人知的图划分连通性概念（特别是，著名的Nash-Williams-Tutte 树打包定理 表明，在图中，划分连通性等价于存在边不相交的打包树）。我们对引理 5.4 的证明遵循 [AGG$^+$25 引理 2.4] 的证明。关于超图定向 的定理 5.5 在 [Fra11], 中表述得最为明确，但在 [Kir03, FKK03b] 中也有隐含表述。

随机求值点上的 Reed-Solomon 码。 Shangguan 和 Tamo [ST20] 猜想随机 Reed-Solomon 码是高阶 MDS 码，并证明了该猜想的若干特殊情形；这一猜想最终由 [BGM25]完整证明。我们介绍他们证明的另一种视角，该证明由 Alrabiah、Guo、Guruswami、Li 和 Zihan [AGG$^+$25]提出，基于超图连通性；而这一思路又建立在超图视角之上，这种视角最初由 Guo、Li、Shangguan、Tamo 和 Wootters [GLS$^+$24]针对列表译码提出。将弱划分连通性与广义零模式 联系起来的引理 5.6 沿用了 [AGG$^+$25 的推论 A.4]。定理 5.9 指出，高阶 MDS 码（按照基于 GZP 的定义）的对偶码满足广义辛格尔顿界；其证明沿用了 [AGG$^+$25 的定理 2.11]。GM-MDS 定理（定理 5.10）由 Lovett [Lov21] 以及 Yildiz 和 Hassibi [YH19], 独立证明，此前 Dau、Song 和 Yuen[DSY14]曾提出这一猜想。推论 5.11 沿用了 [BGM25 命题 4.5] 的证明。

高阶 MDS 码的域大小存在指数级下界，这一点已在 [BGM22, 推论 4.2], 中证明；而 [AGG$^+$25] 则证明，基于线性大小字母表的随机 Reed-Solomon 码近似达到广义辛格尔顿界 [GZ23, AGG$^+$25]。Levi 提出了一种替代方法，用于证明随机 Reed-Solomon 码达到广义辛格尔顿界，

Mosheiff 和 Shagrithaya [LMS25]。这种方法基于证明：就列表可译码性质（更一般地说，任何局部性质，见下文）而言，随机 Reed-Solomon 码的表现与随机线性码相似。

重数码与具有子域求值点的里德-所罗门码。 第 5.2.1 节给出的概率论证表明，任何以常维列表直至容量列表可译码的线性码，也以常数列表大小 直至容量列表可译码；该论证由 Kopparty、Ron-Zewi、Saraf 和 Wootters 发现 [KRSW23，引理 3。1]（Tamo 后来给出了若干改进与推广 [Tam24]）。第 5.2.2 节给出的、重数码（以及折叠里德–所罗门码）达到广义辛格尔顿界的证明由 Chen 和 Zhang 发现 [CZ25], , 其算法版本见 [AHS26]。该证明所用的引理 5.16 由 Guruswami 和 Kopparty 证明 [GK16b]。Brakensiek、Chen、Dhar 和 Zhang [BCDZ25]推广了 [CZ25]的证明，表明重数码（以及折叠 Reed-Solomon 码）满足随机线性码所满足的任何局部性质 （非正式地说，局部性质 [MRR$^+$24、LMS25] 是指可用少量码字证明其不成立的性质，列表译码和列表恢复是其特例）。

第 5.3 节中介绍的利用子空间设计来缩减子域求值点上的里德-所罗门码子码列表大小的方法，是由 Guruswami 和 Xing [GX22] 提出的。

代数几何码。 迄今为止我们讨论过的所有显式达到容量的列表可译码的一个缺点是，它们的字母表大小是码长的一个较大多项式（至少为 n^{1/ϵ^2}，其中 n 是码长，ϵ 是与容量的间隙）。若要将字母表大小降至常数，可以采用代数几何码。粗略地说，代数几何码是 Reed-Solomon 码向函数域情形的推广，其中码字对应于某个代数曲线 在某个有限域 $\mathbb{F}$上的有理点处对某些函数求值。Reed-Solomon 码则对应于这样一种特殊情形：代数曲线是 $\mathbb{F}$ 上的仿射直线，而函数是直线上的低次多项式。由于仿射直线上只有 $|\mathbb{F}|$ 个有理点，这就迫使 Reed-Solomon 码的字母表大小至少与其码长相同。代数几何码的优势在于，代数曲线通常可以有更多有理点，因此字母表大小有可能远小于码长。特别是，通过对参数作某种选择，随着码长增加，字母表大小可以保持为常数。

代数几何码最早由 Goppa [Gop83] 引入。Guruswami 和 Sudan [GS99] 表明，他们在第 3.3 节介绍的、可将 Reed-Solomon 码列表译码至*Johnson*界的算法，可以推广到代数几何码。后来，Guruswami 和 Xing [GX22]引入了折叠代数几何码的若干版本，以及采用子域求值点的代数几何码，并利用这些码将第 4.2 节（针对相关的重数码族）和第 4.3 节中介绍的结果——折叠 Reed-Solomon 码和采用子域求值点的 Reed-Solomon 码均可达到列表译码容量——推广到代数几何码。最近，Brakensiek、Dhar、Gopi 和 Zhang [BDGZ25] 将第 5.1 节介绍的结果——随机 Reed-Solomon 码可达到广义辛格尔顿界——推广到了代数几何码。第 5.3 节介绍了利用子空间设计缩小 Reed-Solomon 码子码列表大小的方法，Guruswami 和 Xing [GX22] 也采用了该方法，将代数几何码子码的列表大小缩小至近似常数（约为 $\log^*(n)$ 量级），随后 Guo 和 Ron-Zewi [GR22] 又将其缩小到了常数。

6 近线性时间列表译码

本节将讨论 Reed-Solomon 码和重数码的更快速列表译码算法。回顾一下，我们已经在第 3 节和第 4 节看到过这类算法的若干版本：它们的运行时间关于输入规模为多项式时间，能够将 Reed-Solomon 码译码至 Johnson界，并将重数码译码至列表译码容量。现在的目标是了解针对这些问题的其他算法；在某些参数范围内，这些算法的时间复杂度快得多，达到关于输入规模的近线性时间。我们先在下面的第 6.1 节介绍一种用于 Reed-Solomon 码的此类算法，随后在第 6.2 节介绍一种用于重数码的快速列表译码算法。

6.1 达到 Johnson界的 Reed-Solomon码快速列表译码

本节将介绍一种针对 Reed-Solomon 码的近线性时间列表译码算法，其译码半径可逼近 Johnson界。具体而言，在下文中，固定一个素数幂 q、互不相同的求值点 $a_1, \ldots, a_n \in \mathbb{F}_q$ 以及一个正整数 $k < n$，并令 $\mathrm{RS}_q(a_1, \ldots, a_n;\ k)$ 表示相应的 Reed-Solomon 码。我们将展示一种算法：对于任意 $\epsilon > 0$，该算法都能在 $n \cdot \mathrm{poly}(\binom{n}{k}, \log(q), \log(n)\ \frac{1}{\epsilon})$ 时间内，对该码中占 $(1 - \sqrt{\frac{k}{n}} - \epsilon)$ 比例的错误进行列表译码。因此，当 ϵ 和该码的码率 $R := \frac{k}{n}$ 均为常数时，该算法的运行时间为 $n \cdot \mathrm{poly}(\log(n), \log(q))$。注意，与第 3.3 节中介绍的 Reed-Solomon 码多项式时间列表译码算法不同，本节介绍的算法无法达到 Johnson界，而只能逼近该界。

概述。 回顾一下，第 3.3 节介绍的、可将 Reed-Solomon 码列表译码至 Johnson界的多项式时间算法（参见图3）包含两个主要步骤：构造一个非零二元多项式，使所有足够接近的码字都被编码在其内部；以及求出二元多项式的根。此外，第一步通过建立并求解线性系统来完成，第二步则依赖现成的二元多项式根计算算法。尽管这两个步骤的时间复杂度都被证明是多项式有界的，但能否将时间复杂度进一步改进到关于输入规模的近线性时间，目前尚不清楚。事实上，即使对于 Reed-Solomon 码唯一解码算法插值步骤中出现的、看似更简单的线性系统（该算法见第 3.1 节），能否在近线性时间内求解该系统也尚不明确。实际上，自20世纪60年代以来已知的 Reed-Solomon 码快速唯一解码算法，也依赖于一些非平凡的洞见。

本节介绍的快速列表译码算法有两个主要的技术组成部分。第一个部分表明，图3中的算法可以利用一元多项式环上的适当格，在近线性时间内完成插值步骤。第二个部分则主要使用Roth和Ruckenstein的一种现成算法，来计算二元多项式的低次根。 [RR00] 我们现在更详细地讨论这些思路。

6.1.1 插值步骤的快速实现

设 $w \in \mathbb{F}_q^n$ 为接收字。本步骤的目标是在近线性时间内求出一个非零二元多项式 $Q(X,\ Y)$，其(1，k)-加权次数较小，并且对每个 i，Q 在(a_i，w_i)处都有一个高重数零点。为此，我们先给出一些定义；这些定义乍看之下可能有些难以理解。

令 $R(X)$ 为次数至多为 $n-1$ 的唯一多项式，使得对每个 i，$R(a_i) = w_i$。借助基于快速傅里叶变换的标准单变量多项式快速插值算法，可以在近线性时间内求得 R

（例如 [vzGG13] 中的算法10.22）。 R 的用途源于以下简单观察：若 $f(X)$ 满足 $f(a_i) = w_i$，则 $X - a_i$ 整除 $f(X) - R(X)$，或者等价地， $f(X) \equiv R(X) \bmod (X - a_i)$。令 ℓ， $m \in \mathbb{N}$ 为满足 $\ell \leq m$（稍后设定）的参数，并且对每个 $j \in \{0, 1, \ldots, m-1\}$，令 $P_j(X, Y)$ 为如下定义的二元多项式。

$$\begin{aligned} &\forall j \in \{0, 1, \ldots, \ell - 1\}, \qquad P_j(X, Y) := (Y - R(X))^j \cdot \prod_{i=1}^{n} (X - a_i)^{\ell - j} \\ &\forall j \in \{\ell, \ell + 1, \ldots, m - 1\}, \quad P_j(X, Y) := (Y - R(X))^j \end{aligned}$$

现在考虑由 $P_0, P_1, \ldots, P_{m-1}$ 张成的 $\mathbb{F}_q[X]$-线性空间中的二元多项式集合，也就是说，

$$\mathcal{L}^{(\ell, m)} := \left\{ \sum_{j=0}^{m-1} g_j(X) \cdot P_j(X, Y) : g_j \in \mathbb{F}_q[X] \right\}.$$

集合 $\mathcal{L}^{(\ell,m)}$ 也可以从以下角度理解。我们将每个 P_j 视为一个以 Y 为变量、系数取自环 $\mathbb{F}_q[X]$ 的一元多项式；因此， P_j 可以视为一个维数为 m 的向量（即将其视为以 Y 为变量的一元多项式时的系数向量），其中每个元素都属于 $\mathbb{F}_q[X]$。于是，集合 $\mathcal{L}^{(\ell,m)}$ 就是这些向量的 $\mathbb{F}_q[X]$ 线性张成空间。此外，我们注意到，由于 P_j 的 Y-次数等于 j （因此彼此不同），所以 P_j （将其视为以 Y 为变量的一元多项式时）的系数向量在域 $\mathbb{F}_q(X)$ 上线性无关。

回顾一下，在整数环上，格的概念定义如下：对于任意正整数 n，以及实数上的线性无关 n 维向量 $v_0, \ldots, v_m$，由 $v_0, v_1, \ldots, v_m$ 生成的格定义为 $\{\sum_i a_i v_i : a_i \in \mathbb{Z}\}$。上文对整数格的定义与集合 $\mathcal{L}^{(\ell,m)}$ 的定义在句法上有一些明显的相似之处：两种情况下，我们都有整环（整数和 $\mathbb{F}_q[X]$），并取一组在包含这些整环的底层域（分别为实数域和分式域 $\mathbb{F}_q(X)$）上线性无关的向量，再考虑它们的加权线性组合，其中权重取自相应的整环。此外，这两个整环实际上都是欧几里得整环。鉴于这些句法上的相似之处，在本综述中，我们遵循惯例，将 $\mathcal{L}^{(\ell,m)}$ 称为由 $P_0, P_1, \ldots, P_{m-1}$ 生成的格。

下面的引理说明了格 $\mathcal{L}^{(\ell,m)}$ 与 Reed-Solomon 码列表译码算法的插值步骤之间的相关性。

引理6.1。 令 $Q(X, Y)$ 为格 $\mathcal{L}^{(\ell,m)}$中的任意非零多项式。那么，对于每个 $i \in [n]$, $Q(X, Y)$，在 (a_i, w_i)处的零点重数至少为 ℓ。

证明。 令 u, v 为满足 $u + v < \ell$的非负整数。于是，为证明该引理，只需证明 Q 的 Hasse 导数 $Q^{(u,v)}$ 在 (a_i, w_i)处为零。回顾可知， Q 具有如下形式：$\sum_{j=0}^{m-1} g_j(X) P_j(X, Y)$。因此，根据 Hasse 导数的线性性，只需证明每个求和项 $g_j(X)P_j(X, Y)$ 的 (u, v) 阶 Hasse 导数在 (a_i, w_i)处为零。根据 Hasse 导数的乘积法则（参见引理 2.7），我们有

$$(g_j(X) P_j(X, Y))^{(u,v)} = \sum_{0 \leq u' \leq u, 0 \leq v' \leq v} P_j(X, Y)^{(u', v')} \cdot g_j(X)^{(u-u', v-v')},$$

因此，只需证明对于任意 $u' + v' < \ell$， j 在 (a_i, w_i) 处为零，其中 $P^{(u',v')}$.

为理解上述内容，由于 P_j 在 $j \geq \ell$ 时会改变结构，因此我们根据 j 考虑两种情况。

- $j \geq \ell$：根据其定义，我们有 $P_j = (Y - R(X))^j$。现在我们说明，对于任意非负的 u'，v'，只要满足 $u' + v' < \ell$，$P^{(u', v')}_j$ 就可被 $(Y - R(X))$ 整除。由于 $(Y - R(X))$（因此 $P^{(u', v')}_j$）在 (a_i, w_i) 处取值为零，这就完成了论证。

  为了证明可整除这一结论，我们考虑 $P_j(X + Z_1, Y + Z_2) = (Y + Z_2 - R(X + Z_1))^j$。将$R(X + Z_1)$视为关于 Z_1 的多项式，可得 $R(X + Z_1)$ 等于 $R(X) + Z_1 \cdot \Gamma(X, Z_1)$，其中 Γ为某个二元多项式。因此，$P_j(X + Z_1, Y + Z_2) = ((Y - R(X)) - (Z_1\Gamma(X, Z_1) - Z_2))^j$。由二项式定理，还可得

$$P_j(X + Z_1, Y + Z_2) = \sum_{t=0}^{j} \binom{j}{t} (Y - R)^{j-t} (Z_1\Gamma - Z_2)^t.$$

  根据 Hasse 导数的定义，$P^{(u', v')}_j$ 等于上述展开式中 $Z_1^{u'} Z_2^{v'}$ 的系数。注意，多项式 $(Z_1\Gamma - Z_2)^t$ 中的每个单项式在Z 变量中的总次数至少为 t。因此，$Z_1^{u'} Z_2^{v'}$ 在 $P_j(X + Z_1, Y + Z_2)$ 中的系数等于截断和 $\sum_{t=0}^{u'+v'} \binom{j}{t} (Y - R)^{j-t} (Z_1\Gamma - Z_2)^t$ 中 $Z_1^{u'} Z_2^{v'}$ 的系数。此外，由 $t \leq u' + v' < \ell$ 和 $\ell \leq j$ 可知，上述和中的每一项都可被 $(Y - R)$ 整除（其 Z 次数为零）。因此，$P^{(u', v')}_j$ 必定可被 $(Y - R)$ 整除。

- $j < \ell$：这一情形也沿上述情形的思路进行，只是需要稍加小心。对于 $j < \ell$，由 P_j 的定义，我们有 $P_j(X, Y) = (Y - R(X))^j \prod_{t=1}^{n} (X - a_t)^{\ell - j}$。为记号方便，我们可以将 P_j 改写为 $P_j(X, Y) = (Y - R(X))^j \cdot (X - a_i)^{\ell - j} \cdot \prod_{t \neq i} (X - a_t)^{\ell - j}$。这一重排的好处在于，$(Y - R)$ 与 $(X - a_i)$ 在 (a_i, w_i) 处均为零点。因此，按重数计，P_j 至少有 ℓ 个在 (a_i, w_i) 处为零的因子。直观上，这表明 P_j 在 (a_i, w_i) 处的重数至少为 ℓ，从而对所有 $u' + v' < \ell$，其 (u', v')-Hasse 导数应在 (a_i, w_i) 处为零。利用 Hasse 导数的定义，可将这一直观严格化，从而得出 $P^{(u', v')}_j$ 可写成若干项之和，其中每一项都可被 $(Y - R(X))$ 或 $(X - a_i)$（或两者）整除。我们在此略去该断言的形式证明。

至此，引理的证明完成。 □

引理6.1表明，格 $\mathcal{L}^{(\ell, m)}$ 中的每个非零多项式在 (a_i, w_i) 处都具有高重数零点，因此满足图3中的算法所要求的插值条件（只要谨慎选择 ℓ）。因此，如果我们能以近线性时间在此格中找到一个非零且 $(1, k)$-加权次数较低的多项式，就能朝着构造快速 Reed-Solomon 码列表译码器迈出重要一步。

核心思路是为格 $\mathcal{L}^{(\ell, m)}$ 中的向量引入一种范数或长度的概念，使得在此范数下，寻找该格中一个非零的、$(1, k)$-加权次数较低的多项式 $Q(X, Y)$，恰好等同于寻找该格中一个在此范数下较短的非零向量。因此，证明这个短向量的范数上界，并以近线性时间找到这样的向量，便能共同完成插值步骤的快速实现。下面我们将讨论细节，首先介绍一元多项式环上的格的定义，以及格中向量长度的概念。

一元多项式环上的格。我们先介绍几个定义。设 $\mathbb{F}$ 是一个有限域，设 $\mathcal{P} = \{P_0, P_1, \ldots, P_{m-1}\} \subseteq \mathbb{F}[X]^r$ 是由 m 个向量组成的集合，且这些向量属于 $\mathbb{F}[X]^r$。由格 $\mathcal{L}$ 生成的

$\mathcal{P}$ 定义在环 $\mathbb{F}[X]$ 上的格为

$$\mathcal{L} := \left\{ \sum_{i=0}^{m-1} g_i(X) \cdot P_i : g_i(X) \in \mathbb{F}[X] \right\}.$$

如果集合 $\mathcal{P} \subseteq \mathbb{F}[X]^r$ 在上述意义下生成格 $\mathcal{L}$，且 $\mathcal{P}$ 中的向量在域 $\mathbb{F}(X)$（即 X 上关于 $\mathbb{F}$ 的有理函数域）上线性无关，则称 $\mathcal{P} \subseteq \mathbb{F}[X]^r$ 是格 $\mathcal{L}$ 的一个 基。格的基的大小是格的一项基本性质；特别是，同一格的所有基大小都相同。注意，$\mathcal{P}$ 中的向量也可以看作 $\mathbb{F}[X, Y]$ 中二元多项式的系数向量，其中这些多项式被视为关于 Y 的一元多项式。在本综述的讨论过程中，我们会根据需要在这两种视角之间切换。

在本综述的应用中，我们仅考虑按如下意义具有满秩的格：它们由某个基 $\mathcal{P} \subseteq \mathbb{F}[X]^m$ 生成，且 $|\mathcal{P}| = m$，也就是说，基的大小等于环境空间的维数。例如，我们注意到，本节前面定义的格 $\mathcal{L}^{(\ell,m)}$ 是满秩的。为此，只需观察该格的生成元，也就是二元多项式 P_0、P_1、.....、P_{m-1}，具有互不相同的 Y 次数，因此它们在 $\mathbb{F}_q(X)$ 上线性无关。

对于 $\mathbb{F}[X]$上的满秩格 $\mathcal{L}$ 的一组基 $\mathcal{P}$，我们将 $\mathcal{P}$的行列式记作 $\det(\mathcal{P})$，定义为其列为 $\mathcal{P}$中向量的方阵的行列式。回忆一下，$\det(\mathcal{P})$是变量 X的多项式。与整数环上的满秩格的情形一样，格 $\mathcal{L}$ 所有基的行列式都彼此相等，这是格 $\mathcal{L}$的一项基本性质，我们将其记作 $\det(\mathcal{L})$。

接下来，我们定义这些格中向量的范数概念。

定义 6.2 (次数范数)。对于任意向量 $P = (p_0, p_1, \ldots, p_{r-1}) \in \mathbb{F}[X]^r$，我们将 P的次数范数记作 $\mu(P)$，定义为

$$\mu(P) := \max_{j \in \{0,1,\ldots,r-1\}} \deg(p_j),$$

其中，$\deg(p_j)$ 是 P中任意条目 $p_j \in \mathbb{F}[X]$ 关于 X的次数的最大值。

换句话说，$\mu(P)$ 是二元多项式 $\sum_{j=0}^{r-1} p_j(X)Y^j$关于变量 X 的次数。

以下定理结合了 Alekhnovich 在 [Ale05] 中的关键技术结果，以及闵可夫斯基关于格的经典定理。该定理隐含于 [Ale05] 中；关于这一点的更详细讨论，请参见 [GHKS24] 中的第 3.3 节。

定理 6.3 ([Ale05]). 设 $\mathcal{L} \subseteq \mathbb{F}[X]^m$ 是由基 $\mathcal{P}$生成的满秩格。那么，存在一个非零向量 v 属于 $\mathcal{L}$，使得

$$\mu(v) \leq \frac{1}{m} \deg(\det(\mathcal{L})).$$

此外，存在一种算法，以基 $\mathcal{P}$ 为输入，求出一个满足上述不等式的非零向量 $v \in \mathcal{L}$，运行时间为 $O(\mu(\mathcal{P})) \cdot \mathrm{poly}(m)$，其中 $\mu(\mathcal{P})$ 等于 $\max_{P \in \mathcal{P}} \mu(P)$。

简要讨论了格的性质之后，我们现在回到任务本身：为图3所示算法的插值步骤获得一种快速实现，并证明以下引理。

引理 6.4. 设 $P_0(X, Y)$..., $P_{m-1}(X, Y)$ 为多项式，并设 $\mathcal{L}^{(\ell,m)}$ 为本节前文针对接收字 $w \in \mathbb{F}_q^n$和求值点 a_1, ..., $a_n \in \mathbb{F}_q$定义的格，且

设 $k < n$ 为正整数。那么，存在一个 $\mathcal{L}^{(\ell,m)}$ 中的非零多项式 $Q(X,Y)$，其 $(1,k)$-加权次数至多

$$\left(\frac{n(\ell+1)\ell}{2m} + \frac{(m-1)k}{2}\right).$$

此外，存在一种算法：当给定 P_0、P_1、……、P_{m-1} 的系数向量作为输入时，在时间 $O(n)\cdot\mathrm{poly}(m)$ 内输出 $\tilde{Q}$ 的系数向量。

证明。为了讨论 $\mathcal{L}^{(\ell,m)}$ 中多项式的 $(1,k)$-加权次数，转而使用由二元多项式 $P'_0, P'_1, \ldots, P'_{m-1}$ 的 $\mathbb{F}_q[X]$ 张成空间所生成的如下相关格 $(\mathcal{L}')^{(\ell,m)}$ 会更有帮助，其定义为

$$\begin{aligned}
&\forall j \in \{0,1,\ldots,\ell-1\}, && P'_j(X,Y) := (X^kY - R(X))^j \cdot \prod_{i=1}^{n}(X-a_i)^{\ell-j} \\
&\forall j \in \{\ell,\ell+1,\ldots,m-1\}, && P'_j(X,Y) := (X^kY - R(X))^j .
\end{aligned}$$

我们再次将这些多项式视为变量为 Y、系数属于 $\mathbb{F}_q[X]$ 的一元多项式。因此，P'_j 是一个 Y 次数等于 j 的多项式；对于 $j<\ell$，其首项系数等于 $X^{kj}\cdot\prod_{i=1}^{n}(X-a_i)^{\ell-j}$，而对于 $j\geq\ell$，其首项系数等于 X^{kj}。因此，若考察由 P'_j 的系数向量所构成的 $m\times m$ 矩阵（我们将其中每一个都视为 Y 上次数至多为 $m-1$ 的多项式），便得到一个三角矩阵，其对角元素恰好对应于 $P'_0, P'_1, \ldots, P'_{m-1}$ 的首项系数。因此，由它们生成的格是满秩的，且其行列式为该矩阵对角元素之积，等于

$$\left(\prod_{j=0}^{\ell-1} X^{kj}\cdot\prod_{i=1}^{n}(X-a_i)^{\ell-j}\right)\cdot\left(\prod_{j=\ell}^{m-1} X^{kj}\right).$$

因此，$\mathcal{L}^{(\ell,m)}$ 的行列式的次数等于 $\left(\binom{n(\ell+1)\ell}{2} + \binom{m}{2}k\right)$。现在我们调用定理 6.3 来 $(\mathcal{L}')^{(\ell,m)}$，从而得到一个非零多项式 $\tilde{Q}(X,Y)$，它属于 $(\mathcal{L}')^{(\ell,m)}$，且其 $\overline{\mu(\tilde{Q})}$（即其 X 次数）至多为

$$\frac{1}{m}\cdot\left(\frac{n(\ell+1)\ell}{2} + \frac{m(m-1)k}{2}\right) = \left(\frac{n(\ell+1)\ell}{2m} + \frac{(m-1)k}{2}\right).$$

此外，由于任意 P'_j 的 X 次数至多为 $(mk+n\ell)$，因此存在一个算法，当以 P'_0、……、P'_{m-1} 为输入时，可在 $O(mk+n\ell)\cdot\mathrm{poly}(m) \leq O(n)\cdot\mathrm{poly}(m)$ 时间内输出 Q。由于 Q 属于 $(\mathcal{L}')^{(\ell,m)}$，且 P'_0、P'_1、……、P'_{m-1} 在域 $\mathbb{F}_q(X)$ 上线性无关，因此存在唯一的一元多项式 g_0、g_1、……、$g_{m-1}\in\mathbb{F}_q[X]$，使得 $\tilde{Q}=\sum_{j=0}^{m-1} g_j(X)P'_j(X,Y)$。令 $Q(X,Y)$ 为如下定义的多项式

$$Q(X,Y) := \sum_{j=0}^{m-1} g_j(X)P_j(X,Y).$$

根据 $Q, P_0, P_1, \ldots, P_{m-1}, P'_0, P'_1, \ldots, P'_{m-1}$ 的定义，可以立即得出，Q 的 $(1,k)$-加权次数至多为 $\tilde{Q}$ 的 X-次数，而后者至多为 $\left(\binom{n(\ell+1)\ell}{2m} + \binom{m-1}{2}k\right)$。此外，存在一种算法：给定 Q 的系数向量后，该算法能在关于输入规模的近线性时间内输出 Q 的系数向量。

为说明“此外”这一部分，我们只需注意到，在每个 P'_j 中， Y^i 的系数都具有可被 X^{ik} 整除的性质。由于 $\tilde{Q}$ 是通过对这类多项式取 $\mathbb{F}_q[X]$-线性组合得到的，因此这一性质对 $\tilde{Q}$ 仍然成立。最后，要从 $\tilde{Q}$ 得到 Q，我们只需对每个 i，将 $\tilde{Q}$ 中 Y^i 的系数除以 X^{ik}；该操作可以在关于 $\tilde{Q}$ 描述长度的近线性时间内完成，因此其时间复杂度至多为 $O(n)\cdot\mathrm{poly}(m)$。

因此，在给定 $P_0, P_1, \ldots, P_{m-1}$ 的情况下，求得 Q 的总体时间复杂度包括：从 $P_0, P_1, \ldots, P_{m-1}$ 求得 $P'_0, P'_1, \ldots, P'_{m-1}$ 的时间复杂度 $\tilde{}$，调用定理 6.3 求得 Q，然后对 Q 执行上述变换 $\tilde{}$ 以求得 Q。除构造 $P'_0, \ldots, P'_{m-1}$ 的复杂度外，我们已经将这些步骤中每一步的时间复杂度 $\tilde{}$ 限定为 $O(n)\cdot\mathrm{poly}(m)$。最后，由于 $P'_j(X,Y)$ 等于 $P_j(X, X^kY)$，我们可以将 $P_j(X,Y)$ 中 Y^i 的系数乘以 X^{ki}（对每个 $i<m$），从而得到 P'_j 的系数向量。这还需要额外的 $\tilde{O}(n)\cdot\mathrm{poly}(m)$ 时间，因此总复杂度的最终上界为 $\tilde{}$所需的 $O(n)\cdot\mathrm{poly}(m)$。 □

为了完成图3中算法的插值步骤，我们现在调用上述引理 6.4，并正确设置参数，同时计算求得 P_j 的时间复杂度。

引理6.5。设 q 为素数幂， $a_1, \ldots, a_n$ 为 $\mathbb{F}_q$ 中互不相同的元素，且 $k<n$ 和 $\ell\in\mathbb{N}$ 为参数。那么，存在一个算法，其运行时间为 $n\cdot\mathrm{poly}(\log(n), \log(q)\ \ell, \binom{n}{k})$；对于任意输入 $w\in\mathbb{F}_q^n$，该算法输出一个非零二元多项式 $Q(X,Y)$，其 $(1,k)$-加权次数至多为 $\sqrt{nk(\ell+1)\ell}$，并且对于每个 $i\in[n]$， Q 在 (a_i, w_i) 处的重数至少为 ℓ。

证明。该算法首先设置参数 m，使得 m 满足 $n(\ell+1)\ell = m(m-1)k$。为简单起见，我们假设在满足该方程的同时，可以将 m 选为正整数。因此，$m = O(\ell\sqrt{\frac{n}{k}})$。

接下来，我们通过快速一元多项式插值，构造次数至多为$n-1$ 的多项式 $R(X)$，使得对每个 $i\in[n]$，都有 $R(a_i) = w_i$。这可以在 $n\cdot\mathrm{poly}(\log(q), \log(n))$时间内完成。现在我们按如下方式构造格 $\mathcal{L}^{(\ell,m)}$ 的基 P_0， P_1，…， P_{m-1}。我们重点讨论 $j<\ell$，因为更大的 j 的论证类似（而且更简单）。对于 $j<\ell$， P_j 定义为$(Y-R(X))^j\cdot\prod_{i=1}^n(X-a_i)^{\ell-j}$。展开$(Y-R(X))^j$ 并重新排列各项，可得

$$P_j = \sum_{t=0}^{j} Y^t\left(\binom{j}{t}R^{j-t}\prod_{i=1}^{n}(X-a_i)^{\ell-j}\right).$$

因此，对于每个 t， P_j 中 Y^t 的系数是一个关于 X、次数至多为 $O(nm)$的多项式。此外，给定 R 的系数向量（我们已在上文计算得到）以及 a_1， a_2，…， a_n，我们可以使用用于快速多项式乘法的标准基于快速傅里叶变换的算法，通过底层域上的 $\tilde{O}(nm)$次算术运算计算多项式 $R^{j-t}\prod_{i=1}^n($ $X-a_i)^{\ell-j}$。因此，每个 P_j（进而整个基）都可以在 $n\cdot\mathrm{poly}(m,\ \log(n),\ \log(q))$时间内计算出来。对于我们所选的 $m = O(\ell\sqrt{\frac{n}{k}})$，该时间至多为 $n\cdot\mathrm{poly}(\log(n),\ \log(q)\ \ell,\ \binom{n}{k})$。

现在，由引理 6.4，我们知道存在一个算法，它以格 $\mathcal{L}^{(\ell,m)}$ 的基作为输入，并在时间 $n\cdot\mathrm{poly}(m)$ $\le n\cdot\mathrm{poly}(\ell, \binom{n}{k})$内输出该格中一个非零 $Q(X,Y)$的系数向量，使得 Q 的$(1,k)$-加权次数至多为 $\binom{n(\ell+1)\ell}{2m} + \binom{(m-1)_2}{k}$。对于我们所选取的 m，该加权次数界中的两项彼此相等，因此 Q 的$(1,k)$-次数至多为

$$\sqrt{\tfrac{nk(\ell+1)\ell(m-1)}{m}} \le \sqrt{nk(\ell+1)\ell}.$$

最后，由引理6.1，我们得到该多项式 Q 对每个 $i \in [n]$都在(a_i, w_i)上以至少 ℓ 的重数消失。这一观察连同该算法的总运行时间至多为 $n \cdot \text{poly}(\log(n), \log(q)\ \ell, \frac{n}{k})$这一事实，完成了该引理的证明。

□

6.1.2 求根步骤的快速实现

首先注意，由引理 6.5 中构造的多项式Q的性质，可以得出以下结论。

引理 6.6。设 $Q(X, Y)$ 是引理 *6.5* 中构造的多项式，并设 $f(X) \in \mathbb{F}_q[X]$ 是一个次数小于 k 的一元多项式，使得对于至少 $\sqrt{nk(\ell+1)\ell}$ 个指标 $i \in [n]$，有 $f(a_i) = w_i$。那么，$Q(X, f(X)) = 0$。

证明。该引理可由断言 3.9 立即得出，论证方式与引理 3.10 的证明类似。我们仅简述细节，同时跟踪参数的变化。按照引理 3.10 证明中的相同论证可知，$Q(X, f(X))$是一个次数至多为 $\sqrt{nk(\ell+1)\ell}$的一元多项式；对于每个满足 $f(a_i) = w_i$的 a_i，它的零点重数至少为 ℓ。因此，如果 f与 w的一致数至少为$\sqrt{nk(\ell+1)\ell}$，那么 $Q(X, f(X))$ 必定恒等于零。

□

Reed-Solomon 码列表译码算法快速变体所需的最后一个技术工具，是 Roth 与 Ruckenstein [RR00] 的以下定理。该定理在某些参数设置下，给出了比定理 3.7 中所述方法更快的二元多项式求根算法。证明可参见 [Ale05] 中的定理 1.2。

定理 6.7 ([RR00], [Ale05]). 设 $\mathbb{F}$ 为任意有限域。那么，存在一个随机算法，以二元多项式 $Q(X, Y) \in \mathbb{F}[X, Y]$ 的系数向量作为输入，并输出其所有形如 $Y - f(X)$ 的因子，其中 $f \in \mathbb{F}[X]$，运行时间为 $O(\deg_X(Q)) \cdot \text{poly}(\deg_Y(Q), \log(|\mathbb{F}|))$。

6.1.3 Johnson界以内的 Reed-Solomon 码快速列表译码

通过适当地设置参数，我们现在可以证明如下定理，该定理给出了一种逼近 Johnson 界的里德-所罗门码快速列表解码算法。

定理6.8. 设 q 为素数幂，设 a_1、a_2、.....、a_n 为 $\mathbb{F}_q$ 中互不相同的点，设 $k < n$ 为正整数，并设 $\epsilon > 0$ 为参数。则 ***Reed-Solomon*** 码 $\text{RS}_q(a_1, \ldots, a_n; k)$ 可从 $(1 - \sqrt{\frac{k}{n}} - \epsilon)$ 错误比例的错误中进行列表译码，时间为 $n \cdot \text{poly}(\frac{n}{k}, \log(q), \log(n)\ \frac{1}{\epsilon})$。

证明。给定定理中的参数 $\epsilon > 0$，我们将参数 ℓ 设为大于 $\frac{1}{\epsilon}$ 的最小自然数。注意，对于 ℓ 的这一选取，我们有 $\sqrt{nk(\ell+1)\ell} < (1+\epsilon)\sqrt{nk}$。

现在，我们将给定的接收字作为输入，应用引理6.5。由此得到一个非零二元多项式 $Q(X,\ Y)$。正如引理 6.6 所示，该多项式具有如下性质：任何次数小于 k、与接收字的一致度至少为 $(1+\epsilon)\sqrt{nk}$ 的多项式 $f(X) \in \mathbb{F}_q[X]$，都满足 $Q(X,\ f(X)) = 0$。现在，我们应用定理 6.7，计算 $Q(X,\ Y)$ 的所有此类根 $f(X)$，并输出其中次数小于 k 且与接收字有足够高一致度的根。

该算法的时间复杂度取决于插值步骤（引理6.5）的时间复杂度，即

$$n \cdot \text{poly}\left(\log(n), \log(q), \ell, \frac{n}{k}\right) \leq n \cdot \text{poly}\left(\log(n), \log(q), \frac{n}{k}, \frac{1}{\epsilon}\right)$$

以及求根步骤（定理 6.7）的时间复杂度，即

$$\tilde{O}(\deg_X(Q)) \cdot \mathrm{poly}(\deg_Y(Q), \log(q)) \leq \sqrt{nk} \cdot \mathrm{poly}\left(\frac{n}{k}, \log(nk), \log(q), \frac{1}{\epsilon}\right),$$

其中我们用到了这样一个事实：$\deg_X(Q)$ 至多为 Q 的 $(1,k)$-加权次数，因此至多为$O(\sqrt{nk/\epsilon})$；而 $\deg_Y(Q)$ 至多为 Q 的 $(1,k)$- 加权次数的 $\frac{1}{k}$，因此至多为 $O(\sqrt{\frac{n}{k}} \cdot \frac{1}{\epsilon})$。最后，回想一下，$k < n$ 给出了算法 $n \cdot \mathrm{poly}(\frac{n}{k}, \log(q), \log(n)\ \frac{1}{\epsilon})$ 时间复杂度的上界，从而完成了定理的证明。

□

6.2 直至容量的重数码快速列表译码

本节将在上一节所讨论思想的基础上，构造一种算法，在适当的参数范围内，以近线性时间将重数码列表译码至容量。在下文中，固定一个素数幂 q、互异的求值点 a_1、……、$a_n \in \mathbb{F}_q$，以及正整数 k，s，使得 $k < sn$ 且 $\max\{k, s\} \leq \mathrm{char}(\mathbb{F}_q)$，并令 $\mathrm{MULT}_q^{(s)}(a_1$，……、$a_n; k)$ 表示相应的重数码。我们将证明，对于任意常数 $\delta := 1 - \frac{k}{sn}$ 和常数 $\epsilon > 0$，以及充分大的 s（取决于 ϵ），重数码 $\mathrm{MULT}_q^{(s)}(a_1$，……、$a_n; k)$ 可以在时间 $\tilde{O}(n) \cdot \mathrm{polylog}(q)$ 内从 $(1 - R - \epsilon)$-比例的错误中进行列表译码，其中 $R := \frac{k}{sn}$ 是该码的码率。

概述。 达到容量的重数码列表译码快速算法，本质上是对第 4.2 节所介绍的、达到容量的重数码列表译码多项式时间算法进行快速实现。我们将先介绍一种更快的插值步骤算法，以便构造一个高阶常微分方程，使所有距离足够近的码字都满足该方程。这基于我们已经见过的一元多项式环上的格理论。证明的第二部分是一个快速算法，用于求解这些微分方程；其解是低维子空间，并可据此求出解子空间的一组基。最后，我们将看到，利用第 5.2.1 节的结果，可以在近线性时间内恢复一个常数大小（取决于 ϵ）的距离足够近的码字列表。

6.2.1 插值步骤的快速实现

设 $w \in (\mathbb{F}_q^s)^n$ 为接收字，其中对任意 $i \in [n]$，$w_i = (w_{i,0}$，……，$w_{i,s-1})$，并设 $r \leq s$ 为一个参数。这一步的目标是以近线性时间求出一个非零的低次数（$r+1$）.元多项式 $Q(X$，Y_0，$= Q\ X\ f\ X\ \ f^{1}\ X\ \ldots\ f^{(r-1)}\ X\ \ a_i\ \ i \in [n]$，$Y_{r-1})$，它关于 Y_0，，Y_{r-1} 是线性的，并满足：对于任何使 $f^{(<s)}(a_i) = w_i$ 的点，$P_f(X)$: (，( )()( )，( )) 都以高重数消失。下面的定义有助于简洁地陈述一些技术性结论。

定义 6.9 （导数算子）。 导数算子 τ 是一个 $\mathbb{F}_q$-线性映射，它将关于 $\mathbb{F}_q[X, Y_0, \ldots, Y_{r-1}]$ 且对 $Y_0, \ldots, Y_{r-1}$ 呈线性的多项式映射为关于 $\mathbb{F}_q[X, Y_0, \ldots, Y_r]$ 且对 $Y_0, \ldots, Y_r$ 呈线性的多项式，如下所示：

$$\tau\left(A(X) + \sum_{\ell=0}^{r-1} B_\ell(X) Y_\ell\right) := A^{(1)}(X) + \sum_{\ell=0}^{r-1}\left(B_\ell^{(1)}(X) \cdot Y_\ell + (\ell+1) B_\ell(X) \cdot Y_{\ell+1}\right).$$

更一般地，对于一个非负整数 j，令 $\tau^{(j)}$ 表示以下线性算子：

$$\tau^{(j)}\left(A(X)+\sum_{\ell=0}^{r-1}B_\ell(X)Y_\ell\right):=A^{(j)}(X)+\sum_{\ell=0}^{r-1}\sum_{h=0}^{j}\binom{h+\ell}{\ell}B_\ell^{(j-h)}(X)\cdot Y_{\ell+h}.$$

因此，$\tau^{(j)}$ 的像包含于 $\mathbb{F}_q[X,Y_0,\ldots,Y_{r-1+j}]$中。

注意，根据式 (4)，对于任意多项式 $Q(X)=A(X)+\sum_{\ell=0}^{r-1}B_\ell(X)Y_\ell$和 $f(X)\in\mathbb{F}_q[X]$，若令 $P_f(X):=Q(X,\ f(X)\ f^{(1)}(X)\ldots,\ f^{(r-1)}(X))$，则有

$$\tau^{(j)}(Q)(X,f(X),f^{(1)}(X),\ldots,f^{(r-1+j)}(X))=P_f^{(j)}(X),$$

对于任意非负整数 j。

下面的引理是引理 4.5 的一个更快版本。

引理 6.10。存在一种算法，以接收字 $w\in(\mathbb{F}_q^s)^n$作为输入，运行时间为 $O(n)\cdot$多项式(s)，并输出一个定义在 $\mathbb{F}_q$ 上的非零$(r+1)$元多项式 $Q(X,Y_0,\ldots,Y_{r-1})$，其形式为

$$Q(X,Y_0,\ldots,Y_{r-1})=A(X)+B_0(X)\cdot Y_0+\cdots+B_{r-1}(X)\cdot Y_{r-1}$$

使得：

1. Q的 X-次数至多为 $n_{(s-r+1)\ r+1}$。

2. 对于任意 $i\in[n]$ 和 $j\in\{0,1,\ldots,s-r\}$，我们有

$$\tau^{(j)}(Q)(a_i,w_{i,0},w_{i,1},\ldots,w_{i,s-1})=0\,.$$

证明。我们将首先在环 $\mathbb{F}_q[X]$ 上定义一个适当的格，使得该格中的所有多项式关于 $Y_0,Y_1,\ldots,Y_{r-1}$的次数至多为1，并满足上述引理第二项中的约束。然后我们证明，该格中存在一个 X-次数至多为 $n_{(s-r+1)\ r+1}$ 的多项式，因此以 X-次数为度量的最短向量满足这一性质。基于这些观察，该算法相当自然——它将构造该格的一个基，然后运行定理 6.3 中给出的算法，以求出该格中的一个最短向量。

更具体地说，设 $R_0,R_1,\ldots,R_{r-1}\in\mathbb{F}_q[X]$ 是次数分别至多为 $sn-1,(s-1)n-1,\ldots,(s-r+1)n-1$ 的多项式，使得对于每个 $\ell\in\{0,1\ldots,r-1\}$、$j\in\{0,1,\ldots,s-\ell-1\}$ 和$i\in[n]$，我们有

$$R_\ell^{(j)}(a_i)=\binom{\ell+j}{j}w_{i,\ell+j}.$$

显然，由次数方面的考量可知，这样的多项式确实存在；事实上，它们是唯一的，并且可以使用基于快速傅里叶变换的算法在时间 $O(ns)$内求得（[vzGG13]中的算法10.22）。给定这些 R_ℓ，我们来考虑如下定义的格 $\mathcal{L}$。

$$\mathcal{L}:=\left\{\tilde{g}(X)\cdot\prod_{i=1}^{n}(X-a_i)^{s-r+1}+\sum_{\ell=0}^{r-1}g_\ell(X)\cdot(Y_\ell-R_\ell(X)):\tilde{g},g_0,\ldots,g_{r-1}\in\mathbb{F}_q[X]\right\}$$

我们首先证明，对于任意多项式 $Q\in\mathcal{L}$、$i\in\{1,2,\ldots,n\}$ 和 $j\in\{0,1,\ldots,s-r\}$，都有$\tau^{(j)}(Q)(a_i,\ w_{i,\ 0},\ w_{i,\ 1},\ \ldots,\ w_{i,\ s-1})=0$。为了证明这一结论，只需证明所需性质成立于

以下两种形式的多项式：$\tilde{g}(X)\cdot\prod_{t=1}^{n}(X-a_t)^{s-r+1}$ 和 $g_\ell(X)\cdot(Y_\ell-R_\ell(X))$，其中 $\ell\in\{0,1,\ldots,r-1\}$。由于格中的每个多项式都是这两种形式的多项式的一个 $\mathbb{F}_q$-线性组合，利用 τ 的 $\mathbb{F}_q$- 线性性即可得出结论。此外，对于形式为 $\tilde{g}(X)\cdot\prod_{t=1}^{n}(X-a_t)^{s-r+1}$ 的多项式，该性质显然成立，因为对于不含 Y 变量的多项式，算子 τ 就是关于 X 的导数算子。因此，我们只需关注形式为 $g_\ell(X)\cdot(Y_\ell-R_\ell(X))$ 的多项式。根据 R_ℓ 的定义，该性质对 $j=0$ 显然成立。接下来我们讨论 $j=1$ 的情形，因为推广到更大的 j 的证明非常相似。

根据 $\tau,\tau^{(1)}$ 的定义，$(g_\ell(Y_\ell-R_\ell))$ 等于

$$\tau^{(1)}(g_\ell(Y_\ell-R_\ell))=g_\ell^{(1)}(X)(Y_\ell-R_\ell(X))+g_\ell(X)((\ell+1)Y_{\ell+1}-R_\ell^{(1)}(X))\,.$$

令 X 为 a_i，Y_ℓ 为 $w_{i,\ \ell}$，并令 $Y_{\ell+1}$ 为 $w_{i,\ \ell+1}$。根据 R_ℓ 的定义，我们注意到 $(w_{i,\ \ell}-R_\ell(a_i))$ 和 $((\ell+1)w_{i,\ \ell+1}-R_\ell^{(1)}(a_i))$ 均为零。因此，$\tau^{(1)}(g_\ell(Y_\ell-R_\ell))$ 在输入 $(a_i,\ w_{i,\ 0},\ w_{i,\ 1},\ \ldots,\ w_{i,\ s-1})$ 上为零。仔细遵循算子 $\tau^{(j)}$ 的定义以及关于 R_ℓ 的插值约束，这一论证自然可推广至 j 取较大值时的 $\tau^{(j)}$。

接下来，我们证明存在一个 X-次数至多为 $n(s-r+1)/(r+1)$ 的 ~~Q~~ $\in\mathcal{L}$。格 $\mathcal{L}$ 的生成元若视为一个维数为 $(r+1)$、元素取自 $\mathbb{F}_q[X]$ 的向量空间（其中，条目 0、1、2..... $r-1$ 分别对应 Y_0、Y_1、..... Y_{r-1} 的系数，而第 r 个条目是 Y 自由项），则构成一个三角系统。因此，我们得到一个满秩格。于是，以这些生成元为列的 $(r+1)\times(r+1)$ 维矩阵的行列式非零。此外，该行列式是 $\mathbb{F}_q[X]$ 中的一个多项式，其次数至多为 $\prod_{i=1}^{n}(X-a_i)^{s-r+1}$ 的次数，因此至多为 $n(s-r+1)$。因此，根据定理 6.3，我们可得存在一个 $\mathcal{L}$ 中的多项式，它非零且 X-次数至多为 $n(s-r+1)/(r+1)$。此外，还有一种算法，以该格的~~生成元~~˜作为输入，并在 $O(n)\cdot\mathrm{poly}(s)$ 时间内输出这个非零向量。

□

6.2.2 求根步骤的快速实现

接下来注意，根据引理 4.6 的证明，对于引理 6.10 中构造的任意多项式 Q，以及次数小于 k 的任意单变量 f，只要 f 在至少

$$t:=\frac{(s-r+1)n+(r+1)(k-1)}{(s-r+1)(r+1)}=\frac{n}{r+1}+\frac{k-1}{s-r+1}$$

个求值点上与 {v5} 一致，就有

$$Q(X,f(X),f^{(1)}(X),\ldots,f^{(r-1)}(X))=0\,.$$

此外，与第 4.2 节开头的讨论类似，可以根据 ϵ 设置参数 s，r，使得这种容错能力能够让我们达到距列表译码容量所需的 ϵ。

因此，要完成列表译码任务，只需解出上述方程。为了以近线性时间完成这一操作，我们首先回顾引理 4.3：次数小于 k 且满足 $Q(X,\ f(X)\ f_{(1)}(X)\ldots,f^{(r-1)}(X))=0$ 的多项式构成的解空间，是域 $\mathbb{F}_q$ 上维数至多为 r 的仿射空间。因此，只需指定一组基（其总描述长度至多为 $O(kr\cdot\log(q))$），即可描述该子空间。

此外，根据引理 5.12，该仿射空间中与 w 足够接近的码字数量为常数（仅取决于 ϵ、该码的相对距离 δ 以及维数 r）。为了完成该算法，我们将描述一种随机化近线性时间算法，用于输出这些码字。

这基本上可直接由引理 5.12 的证明得出：回想一下，在该引理中，我们描述了一种随机算法 Prune；给定 $w \in \Sigma^n$后，该算法以常数概率（取决于 ϵ、 δ和 r）输出列表中的任意一个码字，并据此得出列表大小为常数。因此，我们只需运行 Prune 常数次，并返回各次输出列表的并集。根据并集界，所有邻近的码字以较高的（常数）概率出现在这些输出列表的并集中。最后，注意 Prune 算法通过从 $[n]$ 中随机抽取常数多个元素，并对这些元素求解一个线性方程组来完成，因此使用标准线性方程组求解器，这一步可在 n 的近线性时间内实现。

因此，只需说明如何求出该微分方程的解子空间

$$Q(X, f(X), \ldots, f^{(r-1)}(X)) = 0$$

且时间复杂度接近线性。

以下引理给出了这样一种算法。

引理 6.11. 假设 $Q(X, Y_0, \ldots, Y_{r-1})$ 是一个定义在 $\mathbb{F}_q$ 上的非零$(r+1)$元多项式，其形式为

$$Q(X, Y_0, \ldots, Y_{r-1}) = A(X) + B_0(X) \cdot Y_0 + \cdots + B_{r-1}(X) \cdot Y_{r-1}$$

且次数至多为 D。令 $\mathcal{L}$ 为由所有次数小于k 的多项式 $f(X) \in \mathbb{F}_q[X]$ 组成的列表，使得

$$Q(X, f(X), f^{(1)}(X), \ldots, f^{(r-1)}(X)) = 0.$$

那么，如果 最大值$\{k, s\} \leq$ 特征$(\mathbb{F}_q)$，则 $\mathcal{L}$ 构成 $\mathbb{F}_q$ 上一个维数至多为 $r-1$ 的仿射子空间，并且存在一种算法，以 Q和 k 的系数向量为输入，输出该解仿射子˜空间的一组基，运行时间为 $O(D+k)$ ·多项式$(r,$对数$(q))$。

注意，对于我们所选的 $D = {}^{n}{}_{(s-r+1)\ r+1}$ 和 $r < s$，算法的运行时间为 $\tilde{O}(D+k) \cdot \text{poly}(r, \log(q)) = n \cdot \text{poly}(s, \log(q), \log(n))$。在本节余下部分，我们将概述上述引理证明中的一些主要思路；感兴趣的读者可参阅 [GHKS24, Theorem 5.1] ，了解完整证明。特别地，为了简化记号，我们只关注较小 r 的情形，即 $r = 0$ 和 $r = 1$；这些情形已经包含了大部分技术要点。

求解 $r = 0$ 情形。 对于 $r = 0$，我们只需寻找次数小于 k 的 f，使得 $A(X) + f(X) \cdot B(X) = 0$。因此，在这种情况下，如果方程有解，则解 $f(X)$ 唯一，且等于用 $B(X)$ 除 $A(X)$ 所得的商。因此，一种自然的求解方法是计算用 $B(X)$ 除 $A(X)$ 所得的商和余式；若余式为零且商的次数小于 k，则输出该商。利用基于快速傅里叶变换的经典计算代数算法，可以在关于输入规模的近线性时间内完成这项任务。下面我们将概述一种基于分治的此类算法。正如我们稍后将看到的，该算法背后的一些思路将自然地引导我们处理更大的 r 情形。

在下面的讨论中，假设 k 是 2 的幂。首先注意，任何次数小于 k 的多项式 f都可以唯一地写成 $f = f_0(X) + X^{k/2} f_1(X)$的形式，其中 f_0， f_1 是次数小于$\frac{k}{2}$ 的（可能为零）多项式。我们的思路是尝试通过求解规模较小的方程来恢复 f_0 和 f_1 ，然后将它们组合起来计算 f。首先要注意，如果 f 满足$A(X) + f(X) \cdot B(X) = 0$，那么它满足

$$A + f \cdot B \equiv 0 \mod X^k. \tag{8}$$

此外，由于 f 的次数小于 k，只需模 X^k恢复 f 即可。因此，要解原方程，我们将改为求解上述模方程，然后检查所得解是否满足原方程。为了解上述模方程，我们尝试理解 f_0，f_1 必须满足的性质。

将 $f = f_0 + X^{k/2} f_1$ 代入（$A + fB \equiv 0$ 模 X^k）后，我们得到

$$A + f_0 \cdot B + X^{k/2} f_1 \cdot B \equiv 0 \mod X^k.$$

现在，项 $X^{k/2} f_1 \cdot B$ 中的每个单项式的次数都至少为 $\frac{k}{2}$。因此，上述方程成立当且仅当

$$A + f_0 B \equiv 0 \mod X^{k/2} \tag{9}$$

and

$$(A + f_0 B) + X^{k/2} f_1 B \equiv 0 \mod X^k$$

此外，对于任意满足（$A + f_0 B \equiv 0$ 模 $X^{k/2}$）的 f_0，都有 $A + f_0 B$ 等于某个~多项式$A(X)$。因此，f_1 必须满足

$$X^{k/2} \tilde{A} + X^{k/2} f_1 B \equiv 0 \mod X^k,$$

这等价于

$$\tilde{A} + f_1 B \equiv 0 \mod X^{k/2}. \tag{10}$$

~因此，要在方程（8）中求解 f，只需先求解方程（9），再构造 A 并求解方程~（10）。此外，在方程（9）和方程（10）中，多项式 A, B, A 可以替换为它们模 $X^{k/2}$ 的余式。因此，我们已将求解方程（8）这一原问题化简为求解两个规模恰好减半的问题。如果在递归的任何阶段得到一个无解的方程，就可以得出原方程无解。此外，如果这些方程中的任何一个有解，则其解是唯一的（模 X^k）。

最后，为了分析运行时间，我们注意到，要解决模 X^k 的实例，需要依次进行两次递归调用，每次都涉及模 $X^{k/2}$ 运算。由于我们只关心这些模方程中模 X^k（或更低次的 X 的幂）下的解，因此不失一般性（只需忽略次数大于 k 的所有单项式，因为它们不会参与模 X^k 下的任何计算），我们可以假设 A 和 B 的次数也至多为 k。构造第一次递归调用 (9) 的问题实例需要 $O(k)$ 时间；得到该实例的一个解 f_0 后，我们需要构造多项式~A，以进行第二次递归调用 (10)。给定 f_0，通过在 X^k 下计算多项式 $(A + f_0 B) \bmod X^k$，即可在 $\tilde{O}(k)$ 时间内得到 A（使用快速傅里叶变换进行多项式乘法）。给定两个子问题的解 f_0 和 f_1，解 $f := f_0 + X^{k/2} f_1$ 也可在 $O(k)$ 时间内构造。因此，总时间复杂度 $T(k)$ 可由以下递推式给出

$$T(k) \leq 2T(\frac{k}{2}) + k \log^c(k),$$

其中 c 是某个固定常数，而 c 仅取决于底层域 $\mathbb{F}$ 上快速傅里叶变换的复杂度。

这就得到了所需的运行时间近线性上界。

求解 $r = 1$ 情形。现在我们考虑 $r = 1$ 的情形。对于较大的 r，这一情形基本涵盖了上述引理 6.11 证明中的所有主要思想，同时在符号表示上使叙述更为简洁。回顾一下，对于 $r = 1$，我们要寻找以下微分方程的解：

$$A + fB_0 + f^{(1)}B_1 = 0.$$

不失一般性，我们假设 $B_1(X)$ 是一个非零多项式（否则我们就处于 $r = 0$ 情形），并且 $B_1(0)$ 非零；否则，我们将 X 平移到 $X + a$，其中 a 不是 B_1 的根。这样的平移~可以通过确定性算法在时间 $O(D)$ 内找到（使用单变量多点求值的快速算法，例如 [vzGG13] 中的第 10 章），也可以直接从底层域中随机选取一个 a。

再一次，改为处理模方程会很有帮助。

$$A + fB_0 + f^{(1)}B_1 \equiv 0 \mod X^k. \tag{11}$$

对于这个问题，一个自然而然的初步尝试仍然是通过递归恢复 f_0，f_1 来恢复 f，如同在 $r = 0$ 情形中那样。然而，这里存在一个问题——不同于 $r = 0$ 情形，形如 (11) 的方程可能有多个解。因此，即便我们为 f_0 和 f_1 建立模方程并求解，由此组合得到的原问题候选解 f 的数量也可能达到 f_0 和 f_1 的解集合大小之积。潜在解数量的这种激增似乎是这一策略要奏效就必须处理的问题。

为了解决这个问题，我们利用这样一个事实：方程 (11) 的解空间是 $\mathbb{F}_q$ 上一个维数为 1 的仿射空间。此外，引理 4.3 的证明（参见断言 4.4）还揭示了这个仿射空间的更多结构：如果 $B_1(0) \neq 0$（这里我们不失一般性地作此假设），那么方程 (11) 的任意解 f 都由其常数项唯一确定，即 $f(0)$。[6] 这一简单观察结合初等线性代数，便得到下面这个非常有用的断言。

断言 6.12. *令 $g(X)$ $h(X)$ 为方程 (11) 的唯一多项式，其次数小于 k，且常数项分别为零和一（假设 $B_1(0) \neq 0$）。那么，g, h 构成方程 (11) 中次数小于 k 的解所成仿射空间（在域 $\mathbb{F}$ 上）的一个基。换言之，此类解的集合等于集合 $\{\lambda g + (1-\lambda)h : \lambda \in \mathbb{F}\}$。*

证明。设 g, h 是 (11) 的任意解。因此，我们有 $A + gB_0 + g^{(1)}B_1 \equiv 0 \mod X^k$ and $A + hB_0 + h^{(1)}B_1 \equiv 0 \mod X^k$。现在，对于任意 $\lambda \in \mathbb{F}$，我们声称 $\lambda g + (1-\lambda)h$ 也是 (11) 的一个解。为此，我们利用导数算子的线性性观察到

$$A + (\lambda g + (1-\lambda)h)B_0 + (\lambda g + (1-\lambda)h)^{(1)}B_1 = A + \lambda\left(gB_0 + g^{(1)}B_1\right) + (1-\lambda)\left(hB_0 + h^{(1)}B_1\right).$$

由于 g, h 是 (11) 的解，我们观察到 $\left(gB_0 + g^{(1)}B_1 \equiv -A \mod X^k\right)$ and $\left(hB_0 + h^{(1)}B_1 \equiv -A \mod X^k\right)$。因此，

$$A + \lambda\left(gB_0 + g^{(1)}B_1\right) + (1-\lambda)\left(hB_0 + h^{(1)}B_1\right) \equiv A + \lambda(-A) + (1-\lambda)(-A) \mod X^k,$$

它模 X^k 同余于 0。因此，如果 g 和 h 是解，那么集合 $\{\lambda g + (1-\lambda)h : \lambda \in \mathbb{F}\}$ 中的每个元素都是 (11) 的解。

此外，我们注意到

$$\{\lambda g + (1-\lambda)h : \lambda \in \mathbb{F}\} = \{\lambda(g-h) + h : \lambda \in \mathbb{F}\}$$

[6] 注意，这里我们仍在考察模 X^k 意义下的解。

因此，只要 $(g-h)$ 非零，该集合确实是一个一维仿射空间（此处正是如此，因为 g 与 h 的常数项互不相同）。由于我们已经论证过，(11) 的解构成一个维数至多为一的仿射空间，故 $\{\lambda g+(1-\lambda)h:\ \lambda\in\mathbb{F}\}$ 确实是所有这些解的集合。

□

根据上述断言，求解 (11) 的一种自然策略是尝试找出次数小于 k、常数项分别为零和一且满足该方程的唯一多项式 f_0, f_1。事实证明，一旦常数项固定，(11) 的解具有唯一性，这使得该子问题适合采用类似分治的策略。

考虑 (11) 的一个解 f，其次数小于 k，常数项为 α。因此，$f(X)$ 可以写成 $f(X)=\alpha+Xg(X)$，其中 g 是次数小于 $k-1$ 的多项式。由于 f 是一个解，我们得到以下一系列等式。

$$\begin{aligned} A+fB_0+f^{(1)}B_1 &\equiv 0 \mod X^k \\ \implies A+(\alpha+Xg)B_0+(\alpha+Xg)^{(1)}B_1 &\equiv 0 \mod X^k \\ \implies (A+\alpha B_0)+(XB_0+B_1)g+XB_1g^{(1)} &\equiv 0 \mod X^k \end{aligned}$$

因此，对于每个满足 $f=\alpha+Xg$ 是 (11) 的一个解的 α，g 必须满足

$$(A+\alpha B_0)+(XB_0+B_1)g+XB_1g^{(1)}\equiv 0 \mod X^k. \tag{12}$$

上述新的微分方程虽然在结构上与 (11) 类似，却有一个有用的性质：满足该方程且次数小于 $(k-1)$ 的多项式 $g(X)$ 唯一。要看出这一点，注意根据引理 4.3 的证明（参见断言 4.4），只需证明 g 的常数项 $g(0)$ 唯一确定。为此，注意将 (12) 的左边在零处取值，可得以下方程：

$$(A(0)+\alpha B_0(0))+B_1(0)g(0)=0.$$

由于 $B_1(0)$ 是一个非零域元素（根据本节开头的假设），因此上述关于 $g(0)$ 的一次方程有唯一解，即 $g(0)=-\frac{A(0)+\alpha B_0(0)}{B_1(0)}$。

解的唯一性使我们现在能够采用一种自然的分治式算法，这与我们在 $r=0$ 情形中讨论的算法几乎完全相同。我们将 g 写作 $g=g_0+X^{k/2}g_1$，其中g_0，g_1是次数小于$\frac{k}{2}$的多项式，并尝试理解 g_0，g_1必须满足的条件。若 g是方程 (12) 的一个解，那么对 $X^{k/2}$ 取模并舍去可被 $X^{k/2}$整除的项后，可得 g_0必须满足

$$(A+\alpha B_0)+(XB_0+B_1)g_0+XB_1g_0^{(1)}\equiv 0 \mod X^{k/2}.$$

此外，对于任何满足上述方程的 g_0，$(A+\alpha B_0)+(XB_0+B_1)g_0+XB_1g_0^{(1)}$ 都可被 $X^{k/2}$整除，因此等于某个多项式 $\tilde{A}$乘以 $X^{k/2}\tilde{A}$，而 g_1必须满足

$$X^{k/2}\tilde{A}+X^{k/2}\left(XB_0+\left(1+\frac{k}{2}\right)B_1\right)g_1+X^{k/2}\cdot XB_1g_1^{(1)}\equiv 0 \mod X^k.$$

这等价于

$$\tilde{A}+\left(XB_0+\left(1+\frac{k}{2}\right)B_1\right)g_1+XB_1g_1^{(1)}\equiv 0 \mod X^{k/2}.$$

因此，我们已将求 g的问题转化为求 g_0， g_1的问题，这些对象满足类似的微分方程，但现在我们是在模 $X^{k/2}$的意义下进行运算。因此，实例规模实际上减半了。此外，这些新实例可以在关于输入规模的近线性时间内生成。因此，基于分治的算法将在近线性时间内求得 g。

如上所述，较大的 r can 也可以用非常相似的思路处理，但需要稍加注意。此处略去细节，有兴趣的读者可参阅 [GHKS24]。

6.3 文献注记

设计近线性时间的编码和解码算法，一直是代数编码理论中的重要研究主题。20世纪60年代提出的 Berlekamp-Massey 算法（ [vzGG13]中的第7章）能够在唯一译码范围内，以近线性时间译码里德-所罗门码（以及 BCH 码）。该算法以 Berlekamp 的一种用于译码 BCH 码的算法为基础 [Ber68a]。Massey [Mas69] 给出了该算法的简化描述，并指出它还可用于解决计算代数中的其他问题，尤其是计算线性递推序列的最小多项式。实质上，这些算法将唯一译码范围内里德-所罗门码（或 BCH 码）的译码问题，归约为一个经过充分研究的问题：有理函数重构。随后，人们证明，利用一种能够以近线性时间计算一元多项式最大公因式的算法，可以在近线性时间内完成有理函数重构，从而得到唯一译码里德-所罗门码的近线性时间算法。半GCD算法也称为 Knuth-Schönhage 算法；有关该算法的介绍和详细参考文献，请读者参阅[vzGG13] 中的第11章。

在列表译码的背景下，Roth与Ruckenstein [RR00] 为 Sudan 和 Guruswami-Sudan 的里德-所罗门码列表译码算法提供了更快的实现方案（尽管尚未达到近线性时间）。在设计其算法的过程中，他们为二元多项式的根计算设计了一种更快的算法，具体见定理 6.7。随后，Alekhnovich [Ale05]引入了基于格的技术，并借鉴了 [RR00] 中的一些思想，为常数码率的里德-所罗门码列表译码提供了近线性时间算法，其参数范围逼近 Johnson界。对于重数码（以及折叠 Reed-Solomon 码），Goyal、Harsha、Kumar 和 Shankar [GHKS24]的工作描述了在常数码率情形下将列表译码推进至容量的近线性时间算法。本章的讲解遵循 [GHKS24]中的论述。

7 局部列表译码

本节将展示如何在亚线性时间内对多项式码进行列表译码。亚线性时间算法（也称为局部算法）是高效算法，其运行时间远小于输入长度。特别是，这类算法甚至无法读取整个输入，而且很多时候也无法承担写出完整输出的开销。为了使这一点成为可能，我们需要放宽计算模型，为算法提供对输入的查询访问；同样，当输出过长时，只要求算法提供对输出的查询访问。亚线性时间算法通常也是随机化的，并且存在较小的出错概率。

在（唯一）译码算法的语境中，这意味着局部算法的运行时间远小于该码的码长 n。为此，我们向算法提供对接收字 $w \in \Sigma^n$的查询访问，并且只要求对于任意给定的码字条目 $i \in [n]$,

该算法都能以高概率正确恢复最近码字 c 的第 i个条目。形式化地说，我们有如下定义。

定义 7.1（局部可纠错码 （LCC））。 设 $C \subseteq \Sigma^n$ 是相对距离为 δ 的一个码，并设$\alpha \in (0, \frac{\delta}{2})$。我们称 C 是（Q, α）-局部可纠错的 （LCC），如果存在一个随机算法 A 满足以下要求：

- 输入： A 以码字条目 $i \in [n]$ 作为输入，并且还获得对字符串 $w \in \Sigma^n$ 的查询访问，使得 $\delta(w, c) \leq \alpha$，其中 $c \in C$ 是某个码字。
- 查询复杂度： A 向预言机 w至多进行 Q 次查询。
- 输出： A 以至少 $\frac{3}{4}$ 的概率输出 c_i。

备注 7.2。 下面给出几点说明：

1. 成功概率可以取任意大于$\frac{1}{2}$的常数，因为通过独立重复局部纠错过程常数次并输出多数值，可以提高成功概率（代价是查询复杂度增加一个常数倍）。为简单起见，在上述定义中，我们将成功概率固定为$\frac{3}{4}$。

2. 人们通常也关心局部纠错算法的运行时间 。通常情况下，本节给出的所有算法，其运行时间都是查询复杂度 Q的多项式。

3. 局部纠错的一种有用（而且可以说更为自然）的变体是局部解码。局部可解码码的定义与局部可纠错码类似，不同之处在于，我们将码字 c 视为某条消息 m 的编码（通过固定某个单射编码映射 Φ： $\Sigma^k \to C$，其中 k 满足 $|C| = |\Sigma|^k$），并且局部译码器需要译出 m中的各个分量。如果我们仅限于线性码，那么局部可解码码是比局部可纠错码更弱的对象，因为任何线性局部可纠错码都可以通过选择系统编码映射转化为局部可解码码。[7] 为简单起见，本节重点讨论局部纠错模型，但我们指出，所给出的所有算法也都可以很容易地改用于局部解码模型。

我们将关注上述局部纠错定义在列表译码情形下的扩展。不过，实际定义需要一些细微处理：我们希望返回一个列表，其中包含与所有近邻码字对应的答案，同时希望算法具有局部性；但对于近邻码字中的单个位置，返回 Σ 处可能符号的列表几乎毫无用处，因为通常会有许多位置 $i \in [n]$，使得所有近邻码字的第 i个位置上的取值覆盖整个 Σ。此外，在应用中通常需要某种形式的一致性，也就是说，对于列表中的任意固定码字c，都能以高概率一致地局部纠错 c的各个位置。为确保这一点，我们要求局部列表译码算法返回一列随机局部算法 A_1， A_2，……， A_L，使得对于列表中的每个近邻码字 c，列表中都存在某个算法 A_j，能够局部纠错 c。形式化地说，我们有如下定义。

[7]如果任意 $m \in \Sigma^k$ 都是 $\Phi(m)$ 的前缀，则编码映射 $\Phi: \Sigma^k \to C$ 是系统的。对于线性码，可以通过将生成矩阵 G 化为简化列阶梯形，并令 $\Phi(m) = G \cdot m$，来找到这样的映射。

定义 7.3 (局部列表可解码码（局部列表可解码码）**)**。 如果存在一个随机算法 A ，它输出 L 个随机算法A_1、A_2、.....、 A_L，且对任意 $w \in \Sigma^n$均满足以下要求，则称码 $C \subseteq \Sigma^n$ 为（Q、 α、 L）-局部列表可解码码（局部列表可解码码）：

- 输入： 每个 A_j 都以一个码字条目 $i \in [n]$作为输入，并且还可以查询访问 w。
- 查询复杂度： 每个 A_j 最多对 w进行 Q 次查询。
- 输出： 对于每个满足$\delta(c, w) \leq \alpha$的码字 $c \in C$，以至少 $\frac{1}{2}$ 的概率（对 A 的随机性而言），以下事件会发生：存在某个 $j \in [L]$，使得对所有 $i \in [n]$,

$$\Pr[A_j(i) = c_i] \geq \frac{3}{4},$$

其中，概率是针对 A_j的内部随机性而言的。

注 7.4。 注 *7.2* 中的相同评论也适用于上述定义。我们还指出以下几点：

1. 对于上述定义中的局部列表译码算法 A ，其成功概率 $\frac{1}{2}$ 可以通过多次独立调用局部列表译码算法 A来放大，并输出任意一次调用所输出的所有随机算法 A_j 的并集，代价是增加列表大小（具体而言，要将成功概率放大到 $1 - 2^{-t}$ ，列表大小需要乘以因子 $O(t)$）。

2. 在上述定义中，我们要求对于任意一个固定的邻近码字 c，局部算法 A_j 的列表以高概率包含一个针对 c 的局部纠错器。我们还可以保证更强的要求：以高概率，输出列表包含针对任意邻近码字 c 的局部纠错器。具体做法是先将 A 的成功概率提升至 $1 - \frac{1}{4L}$，然后对所有邻近码字应用并集界（注意，根据局部列表译码的定义，这类码字至多有 $2L$ 个）。

乍看之下，上述局部列表译码的定义或许有些奇怪且复杂，但事实证明，对于编码理论和理论计算机科学中的各种应用来说，这恰恰是合适的定义。

要使一个码能够进行局部（列表）译码，其码字条目必须满足某些非平凡的局部关系。对于基于多项式的码，可以考虑基于多元多项式的码来实现这一性质。这里用到的主要性质是：低次多元多项式在任意直线（或更一般地说，曲线或低维子空间）上的限制是一个低次单变量多项式。因此，给定一个码字条目，可以经过该点作一条随机直线，并在这条直线上恢复最接近的低次单变量多项式，从而恢复该条目的值（更一般地说，也可以使用曲线或低维子空间）。

接下来，我们首先聚焦于*Reed-Muller*（里德-穆勒码）码这一类码，它将 Reed-Solomon 码扩展到了多元多项式的情形。我们先在下文第 7.1 节中介绍一个预备步骤；由于这也会作为局部列表译码算法中的一个子程序，我们将说明如何从较小比例的错误中（错误数低于该码最小距离的一半）局部纠正Reed-Muller 码。随后，在第 7.2 节中，我们将说明如何在超过最小距离一半的情况下对 Reed-Muller 码进行局部列表译码；在第 7.3 节中，我们将介绍一种改进算法，它能够对达到 *Johnson* 界的 Reed-Muller 码进行局部列表译码。最后，在第 7.4 节中，我们将考察多变量重数码这一类码

它通过计算多元多项式的多元导数来扩展 Reed-Muller 码；我们将概述这些码的一种局部列表译码算法，该算法可达到其最小距离，并进一步说明如何利用这一方法构造容量可达的局部列表可译码码。

7.1 Reed-Muller码的局部纠错

本节首先将展示如何从少量错误中（错误数量低于该码最小距离的一半）对 Reed-Muller码进行局部纠错，以此作为预热；此外，这也将作为下一节所述局部列表译码算法的一个子过程。更具体地，固定一个素数幂 q，以及正整数 k，m，使得 $k < q$。回顾一下，*Reed-Muller*（RM）码 $\mathrm{RM}_{q,m}(k)$ 是这样一种码：它将每个次数（总次数）小于k 的 m 元多项式 $f(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ 映射为一个码字 $(f(\mathbf{a}))_{\mathbf{a}\in\mathbb{F}_q^m} \in \mathbb{F}_q^{q^m}$。令 $\delta := 1 - \frac{k}{q}$ 表示该码的相对距离。下文将证明，对于 $\alpha := \frac{\delta}{8} - \frac{1}{q}$，该码是一个 (q, α)-局部可纠错码。注意，对于 $m > 1$，q 的查询复杂度远小于该码的码长 q^m。

假设一个接收字，接下来为方便起见，我们将 w 视为一个函数$w\colon \mathbb{F}_q^m \to \mathbb{F}_q$。假设存在一个（唯一的）多项式 $f(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$，其次数小于 k，使得 $f(\mathbf{a}) \neq w(\mathbf{a})$ 的情况至多出现在条目 $\mathbf{a} \in \mathbb{F}_q^m$ 中比例为 α 的部分。下面将介绍一个随机化局部纠错算法：给定一个条目 $\mathbf{a} \in \mathbb{F}_q^m$ 作为输入，该算法对 w进行少量查询，并以至少 $\frac{3}{4}$ 的概率输出 $f(\mathbf{a})$。

概述。为解码 $f(\mathbf{a})$，我们随机选取一条经过 $\mathbf{a}$ 的直线，并查询 w 在这条直线上的限制。然后，我们求出在该直线上与 w 最接近的、次数小于 k 的一元多项式 $g(X) \in \mathbb{F}_q[X]$（可使用图1中的算法高效求出），并返回 g 在$\mathbf{a}$处的值。为证明正确性，我们利用的主要性质是：f 在任意直线上的限制都是次数小于 k的一元多项式；此外，随机直线具有良好的采样性质，即随机直线上的错误比例通常接近总体错误比例。算法的正式描述见下文图7，随后将进行正确性分析。

里德-穆勒码里德-穆勒码$_{q,m}(k)$**的局部纠错：**

- **输入：** 对函数 w 的查询访问：$\mathbb{F}_q^m \to \mathbb{F}_q$该函数与某个多项式 $f(X_1, \ldots, X_m) \in (\mathbb{F}_q)_{<k}[X_1, \ldots, X_m]$ 的距离不超过 $(\frac{\delta}{8} - \frac{1}{q})$（即，对于至多占点集 $\in \mathbb{F}_q^m$ 中 $(\frac{\delta}{8} - \frac{1}{q})$比例的点 $\mathbf{a} \neq w(\mathbf{a}) = f(\mathbf{a})$），给定一个点 $\mathbf{a} \in \mathbb{F}_q^m$。

- **输出：** $f(\mathbf{a})$。1. 选取一个$\mathbf{b} \in \mathbb{F}_q^m$随机点。2. 查询经过$\mathbf{a}$和$\mathbf{b}$的直线 $\lambda_{\mathbf{a},\mathbf{b}}(T)$ 上的所有点：$=(1 - T) \cdot \mathbf{a} + T \cdot \mathbf{b}$。3. 求一个次数小于 k 的一元多项式 $g(T) \in \mathbb{F}_q[T]$，使其与 $w|_{\lambda_{\mathbf{a},\mathbf{b}}(T)} :=(w \circ \lambda_{\mathbf{a},\mathbf{b}})(T)$ 的距离不超过 $\frac{\delta}{2}$；使用图1中的算法。如果不存在这样的多项式，则输出 $\perp$。4. 输出 $g(0)$。

图7：Reed-Muller码的局部纠错

正确性。 注意，对于随机点$\mathbf{b} \in \mathbb{F}_q^m$，直线$\lambda_{\mathbf{a},\mathbf{b}}(T)$上除零点以外的任意点都是均匀随机的。因此，该直线上的期望错误比例至多为$(\frac{\delta}{8} - \frac{1}{q}) + \frac{1}{q} = \frac{\delta}{8}$。根据马尔可夫不等式，这又意味着，在选择$\mathbf{b}$时，以至少$3/4$的概率，直线$\lambda_{\mathbf{a},\mathbf{b}}$上的错误比例小于$\frac{\delta}{2}$。最后，假设后一事件发生，根据图1中的算法的正确性（注意到$f|_{\lambda_{\mathbf{a},\mathbf{b}}}$是一个次数小于$k$的一元多项式），我们有$g(T) = f|_{\lambda_{\mathbf{a},\mathbf{b}}}(T)$，特别是$g(0) = f(\mathbf{a})$。因此，我们得出结论：该算法以至少$3/4$的概率输出$f(\mathbf{a})$。

查询复杂度。 查询复杂度显然就是直线上的点数q。

注 7.5。 虽然我们没有尝试优化上述局部纠错算法的译码半径，但值得注意的是，若要获得大于$1/2$的非平凡成功概率，必须将译码半径设为小于$\frac{\delta}{4}$。这是因为，只有在低于这一半径时，才能利用马尔可夫不等式保证：对于随机直线经过$\mathbf{a}$的选择，错误数小于$\frac{\delta}{2}$的概率至少为$1/2$。

若要对错误比例更大的*Reed-Muller*码进行局部纠错，可以将图7中的算法里的随机直线$\lambda_{\mathbf{a},\mathbf{b}}(T)$替换为一条经过$\mathbf{a}$的随机曲线，其形式为$\chi_{\mathbf{a},\mathbf{b},\mathbf{c}}(T) = \mathbf{a} + \mathbf{b}T + \mathbf{c}T^2$，其中$\mathbf{b}$、$\mathbf{c} \in \mathbb{F}_q^m$是均匀随机选取的。在曲线上进行译码的优点是，经过$\mathbf{a}$的随机曲线上任意两点都两两独立，因此可以利用切比雪夫不等式更好地界定曲线上的错误数。不过，采用曲线也会增加f在曲线上的限制次数，因此曲线上可容忍的错误会更少。但事实证明，这种权衡是有利的，可以实现半径约为$\delta - \frac{1}{2}$的局部纠错；对于δ，该半径接近其最小相对距离的一半，而最小相对距离接近1（有关此算法的完整描述和分析，请参见*[Yek12，第2.2节。3]*）。

7.2 超越唯一译码半径的 Reed-Muller码局部列表译码

接下来，我们将展示如何对超过唯一译码半径的 Reed-Muller码进行局部列表译码。回顾一下，在局部列表译码中，我们要求局部列表译码算法返回一个由随机局部算法组成的列表$A_1, A_2, \ldots, A_L$，使得对于列表中的每个近邻码字c，列表中都存在某个算法A_j能够对c进行局部纠错。事实上，由于我们已经证明 Reed-Muller码是局部可纠错的，只需证明它们是近似局部列表可译码的，也就是说，只要求局部算法A_j能够正确恢复c大部分条目。随后，将每个局部算法A_j与上一节介绍的局部纠错算法组合，就可以把这种近似局部列表译码算法转化为局部列表译码算法。此外，利用平均论证可以证明，在近似局部列表译码中，可以假设每个局部算法A_j都是确定性的。形式化地说，我们有以下定义。

定义 7.6（近似局部列表可译码码（ALLDC））。 我们称码$C \subseteq \Sigma^n$是(Q, α, ϵ, L)-近似局部列表可译码（ALLDC），如果存在一个随机化算法A，它输出L个确定性的算法$A_1, A_2, \ldots, A_L$，并且对于任意$w \in \Sigma^n$，这些算法均满足以下要求：

- 输入：每个A_j都以码字条目$i \in [n]$作为输入，并且还可以查询访问w。
- 查询复杂度：每个A_j对w的查询次数最多为Q次。

• 输出：对于每个码字 $c \in C$，使得 $\delta(c, w) \leq \alpha$，以至少1/2的概率，在 A 的随机性下，以下事件会发生：存在某个 $j \in [L]$ 使得

$$\Pr_{i \in [n]}[A_j(i) = c_i] \geq 1 - \epsilon,$$

其中，概率是针对随机选取的条目 $i \in [n]$而言的。

注 7.7。注 *7.4* 中的相同说明也适用于上述定义。不过，我们注意到，对于 ***ALLDC***，每个局部算法 A_j 的成功概率无法通过重复来放大，因此我们没有像之前的LLDC定义（定义 *7.3*）那样，将其固定为3/4。

下面的引理表明，通过将每个局部列表译码算法 A_j 与一个局部纠错算法组合，可以将近似局部列表译码算法转化为局部列表译码算法。

引理 7.8 (ALLDC + 局部可纠错码 $\Rightarrow$ LLDC)。设 $C \subseteq \Sigma^n$ 是一个(Q, α, ϵ, L)-ALLDC，且是(Q', α')-***LCC***，适用于 $\alpha' \geq \epsilon$。那么，C 也是一个$(Q \cdot Q', \alpha, L)$-LLDC。

证明。局部列表译码算法将近似局部列表译码算法 A 生成的每个局部算法 A_j 替换为一个局部算法 A'_j，其运行方式如下：给定输入 $i \in [n]$，局部算法 A'_j 在输入 i上调用局部纠错算法 A'，并将 A' 在 $[n]$ 中的每个查询转发给局部算法 A_j。

正确性源于以下事实：根据我们的假设，$\alpha' \geq \epsilon$、A_j 在 $[n]$中至少 $(1 - \alpha')$ 比例的条目上输出正确值，并且只要码字中至多有 α' 比例的条目被破坏，A' 就以至少 3/4 的概率输出正确值。查询复杂度为$Q \cdot Q'$，因为对于 A' 将进行的每个 Q' 查询，A'_j 都会运行一个 A_j 的副本，而该副本会进行 Q 次查询。

□

给定上述引理，我们现在的任务是设计一种超越其最小距离一半的 Reed-Muller码近似局部列表译码算法。与之前一样，固定一个素数幂 q 和正整数 k、m，使得 $k < q$，并令 $\mathrm{RM}_{q,m}(k)$ 表示相应的 Reed-Muller码。令 $\delta := 1 - \frac{k}{q}$ 表示该码的相对距离，令 $\sigma > 1$ 和 $\xi > 0$ 为参数，并令 $\alpha := 1 - \sqrt{\sigma \cdot (1 - \delta)} - \xi$。我们将证明，对于 $\epsilon = \frac{2\delta}{\sigma - 1} + O(\frac{1}{\xi^2 q})$ 和 $L = q$，该码是一个 (q, α, ϵ, L)-ALLDC。因此，当 σ 和 q 足够大时，失败概率 ϵ 小于 $\frac{\delta}{8}$；由第 7.1 节的结果和引理 7.8 可知，该码也是一个 (q^2, α, L)-局部列表可解码码。注意，对于任意固定的 $\sigma > 1$，当相对距离 δ 足够大时，$1 - \sqrt{\sigma \cdot (1 - \delta)}$ 的译码半径大于最小相对距离的一半。还要注意，对于任意 $m > 2$，q^2 的查询复杂度都远小于该码的码长 q^m。

下面我们将介绍一种随机化的近似局部列表译码算法 A，它会输出一个由确定性的 q-查询局部算法组成的列表 $A_1, \ldots, A_L$，并满足以下保证。假设 $w \in \mathbb{F}_q^{q^m}$ 是一个接收字（与之前一样，将 w 视为函数 $w : \mathbb{F}_q^m \to \mathbb{F}_q$会比较方便），并假设$f(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ 是一个次数小于 k的多项式，使得 $f(\mathbf{a}) \neq w(\mathbf{a})$ 至多在比例为 α的条目上成立。我们将证明，对于 A的随机性，以至少1/2的概率，存在一个局部算法 A_j，它能正确恢复 $f(\mathbf{a})$ 的值，除至多比例为 ϵ的值之外，其中 $\mathbf{a} \in \mathbb{F}_q^m$。

概述。为生成局部算法的列表，算法 A 会选取一个均匀随机点 $\mathbf{b} \in \mathbb{F}_q^m$，并对任意值 $v \in \mathbb{F}_q$，输出一个局部算法 $A_{\mathbf{b}, v}$（注意，局部算法的数量确实是 $L = q$）。我们将值 v 视为对 $f(\mathbf{b})$ 取值的“猜测”或“建议”。有了这个建议后，我们就用它来局部纠正 f。具体而言，为恢复 $f(\mathbf{a})$，局部算法 $A_{\mathbf{b}, v}$ 首先考虑

经过 $\mathbf{a}$ 和 $\mathbf{b}$ 的直线 $\lambda_{\mathbf{a},\,\mathbf{b}}$，并对 w 在这条直线上的限制进行全局列表译码，从而得到一个一元多项式列表$\mathcal{L} \subseteq \mathbb{F}_q[T]$（这可以用图3中的算法高效完成）。这些一元多项式是 $f|_{\lambda_{\mathbf{a},\,\mathbf{b}}}$ 的候选项。哪个一元多项式是 $f|_{\lambda_{\mathbf{a},\,\mathbf{b}}}$? 我们利用对 $f(\mathbf{b})$ 的猜测 v：如果列表中恰有一个一元多项式在 $\mathbf{b}$ 处的取值为 v，那么我们就将其视为 $f|_{\lambda_{\mathbf{a},\,\mathbf{b}}}$ 的候选项，并输出它在点 $\mathbf{a}$ 处的取值，作为对 $f(\mathbf{a})$ 的猜测。

如果满足以下条件，上述算法就能正确恢复 $f(\mathbf{a})$：(1) 经过$\mathbf{a}$ 和 $\mathbf{b}$的直线上错误数量不多；(2) $\mathcal{L}$ 中没有其他多项式在 $\mathbf{b}$ 处取值与 f 相同。正如我们在上一节中已经证明的，根据标准抽样界，第一个事件发生的概率很高。对于第二个事件，利用 $\mathcal{L}$ 中的任意一对多项式在至少占点集 δ比例的点上取值不同这一事实可知，对于任意其他多项式 $h(T) \in \mathcal{L}$，它在 $\mathbf{b}$ 处与 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}$取值相同的概率至多为 $1-\delta$，其中概率是对 $\mathbf{b}$ 的选取而言的。假设列表 $\mathcal{L}$ 足够小（当译码半径充分低于 Johnson界时便会如此），则可以对 $\mathcal{L}$ 中的所有元素应用并集界，从而证明：以高概率，不存在其他多项式 $h(T) \in \mathcal{L}$在 $\mathbf{b}$处与 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}$取值相同。

近似局部列表译码算法的形式化描述见下方图 8，随后给出正确性分析。

里德-穆勒码的近似局部列表译码 $_{q,m}(k)$**：**

近似局部列表译码算法 A**：**

1. 随机选择一个点$\mathbf{b} \in \mathbb{F}_q^m$。
2. 对任意值 $v \in \mathbb{F}_q$，输出下文定义的局部算法 $A_{\mathbf{b},\,v}$。

局部算法 $A_{\mathbf{b},\,v}$**：**

- **输入：** 对函数 w 的查询访问：$\mathbb{F}_q^m \to \mathbb{F}_q$，一个点 $\mathbf{a} \in \mathbb{F}_q^m$。
- **输出：** 一个取值属于 $\mathbb{F}_q$.

1. 查询直线 $\lambda_{\mathbf{a},\mathbf{b}}(T) := (1-T)\cdot\mathbf{a} + T\cdot\mathbf{b}$ 上经过 $\mathbf{a}$ 和 $\mathbf{b}$ 的所有点。
2. 求列表 $\mathcal{L}$，其中包含所有次数小于 k 的一元多项式 $g(T) \in \mathbb{F}_q[T]$，它们与 $(1-\sqrt{\sigma\cdot(1-\delta)})$-接近 $w|_{\lambda_{\mathbf{a},\mathbf{b}}}(T)$，使用图3中给出的算法。
3. 如果存在唯一的多项式 $g(T) \in \mathcal{L}$ 使得 $g(1) = v$，则输出 $g(0)$；否则，输出 $\perp$。

图 8：Reed-Muller码的局部列表译码

正确性。设 $f(X_1,\ldots,X_m) \in \mathbb{F}_q[X_1,\ldots,X_m]$是一个次数小于 k的多项式，使得$f(\mathbf{a}) \neq w(\mathbf{a})$在至多占 α比例的条目上成立 $\mathbf{a} \in \mathbb{F}_q^m$。我们希望证明，对于所选的 $\mathbf{b}$，局部算法 $A_{\mathbf{b},f(\mathbf{b})}$ 以至少 $1\ 2$ 的概率正确恢复 $f(\mathbf{a})$，除至多占ϵ比例的 $\mathbf{a} \in \mathbb{F}_q^m$外。为此，我们先证明，对于所选的两个随机 $\mathbf{a} \in \mathbb{F}_q^m$和随机 $\mathbf{b} \in \mathbb{F}_q^m$，以高概率有：$A_{\mathbf{b},f(\mathbf{b})}$ 在输入 $\mathbf{a}$时正确计算 $f(\mathbf{a})$。

我们首先证明，对于$\mathbf{a},\mathbf{b}$的选取，以高概率存在一个多项式 $g(T) \in \mathcal{L}$，它在直线$\lambda_{\mathbf{a},\mathbf{b}}$上与 f 一致。

断言 7.9。 对于$1-\frac{1}{\xi^2 q}$的随机选取，至少以$\mathbf{a},\mathbf{b}\in\mathbb{F}_q^m$的概率，有$f|_{\lambda_{\mathbf{a},\mathbf{b}}}\in\mathcal{L}$。证明。 注意，对于随机点$\mathbf{a}$,$\mathbf{b}\in\mathbb{F}_q^m$，直线$\lambda_{\mathbf{a},\mathbf{b}}$是均匀随机直线。因此，直线上的任意单个点都是均匀随机的，且直线上任意一对点都两两独立。令 $Z_1,\ldots,Z_q$为指示随机变量，其中若 w在直线上的第 t个点处与 f不同，则 $Z_t=1$，令 $Z:=\frac{\sum_{t=1}^{q}Z_t}{q}$，并注意到，根据图3中算法的正确性，若 $Z\le 1-\sqrt{\sigma\cdot(1-\delta)}$，则有$f|_{\lambda_{\mathbf{a},\mathbf{b}}}\in\mathcal{L}$。此外，由于期望线性性且直线上的任意点均为均匀随机点，我们有

$$\mathbb{E}[Z]=\frac{\sum_{t=1}^{q}\mathbb{E}[Z_t]}{q}\le 1-\sqrt{\sigma\cdot(1-\delta)}-\xi,$$

由两两独立性可知，

$$\mathrm{Var}(Z)=\frac{\sum_{t=1}^{q}\mathrm{Var}[Z_t]}{q^2}\le\frac{\sum_{t=1}^{q}\mathbb{E}[Z_t]}{q^2}\le\frac{1}{q}.$$

因此，由切比雪夫不等式可得，

$$\Pr\left[Z>1-\sqrt{\sigma\cdot(1-\delta)}\right]\le\Pr\left[Z-\mathbb{E}[Z]>\xi\right]\le\frac{\mathrm{Var}(Z)}{\xi^2}\le\frac{1}{\xi^2 q}.$$

因此，我们得出结论：以至少$1-\frac{1}{\xi^2 q}$的概率，$Z\le 1-\sqrt{\sigma\cdot(1-\delta)}$，在此情况下有$f|_{\lambda_{\mathbf{a},\mathbf{b}}}\in\mathcal{L}$。□

接下来，我们证明：以高概率，在选择$\mathbf{a}$、$\mathbf{b}$后，$\mathcal{L}$中除$f|_{\lambda_{\mathbf{a},\mathbf{b}}}$之外，不存在任何在$\mathbf{b}$上与 f一致的多项式。

断言 7.10。 在随机选择$\mathbf{a}$、$\mathbf{b}\in\mathbb{F}_q^m$时，以至少 $1-\frac{\delta}{\sigma-1}$ 的概率，不存在多项式$h(T)\in\mathcal{L}$，使得它不同于 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}$，且满足 $h(1)=f(b)$。

证明。 我们可以将随机选择$\mathbf{a}$、$\mathbf{b}\in\mathbb{F}_q^m$的过程视为：先随机选择$\mathbf{a}\in\mathbb{F}_q^m$，再选择一条经过$\mathbf{a}$的随机直线 λ，最后令$\mathbf{b}\in\mathbb{F}_q^m$为直线 λ上的随机点。因此，以下固定一点$\mathbf{a}$ 和一条经过它的直线 λ，并令 $\mathcal{L}$ 为在该直线上与 w 的距离至多为 $(1-\sqrt{\sigma(1-\delta)})$ 的次数小于 k 的一元多项式列表。我们将证明，在随机选择$\mathbf{b}$时，以至少 $1-\frac{\delta}{\sigma-1}$的概率，不存在多项式 $h(T)\in\mathcal{L}$，使得它不同于 $f|_\lambda$，且 h 与 f 在$\mathbf{b}$上一致。

固定一个多项式 $h(T)\in\mathcal{L}$，使得 $h(T)\ne f|_\lambda(T)$。由于 h和 $f|_\lambda$都是次数小于 k的多项式，因此它们在直线上的点至少有 δ 的比例不相同。因此，h 和 $f|_\lambda$ 在点 $\mathbf{b}$ 处相同的概率至多为 $1-\delta$，其中概率取自对 $\mathbf{b}$ 的选择。此外，注意到根据 Johnson界（参见定理 2.1），我们有

$$|\mathcal{L}|\le\frac{\delta}{\sigma\cdot(1-\delta)-(1-\delta)}\le\frac{\delta}{(\sigma-1)(1-\delta)}.\tag{13}$$

因此，对 $\mathcal{L}$中的所有元素应用并集界，存在一个不同于 $f|_\lambda$的多项式$h(T)\in\mathcal{L}$，使得 h和 f在$\mathbf{b}$处相同的概率至多为 $\frac{\delta}{\sigma-1}$。□

根据上述命题 7.9 和 7.10，对于a 和$\mathbf{a}$与$\mathbf{b}$的选择，以至少 $1-\frac{\delta}{\sigma-1}-\frac{1}{\xi^2 q}$ 的概率，有 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}\in\mathcal{L}$，并且不存在除 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}$之外的多项式 $h(T)\in\mathcal{L}$，使得 $h(1)=f(b)$。在这种情况下，局部算法 $A_{\mathbf{b},\,f(\mathbf{b})}$ 会在步骤 3 中设置 $g=f|_{\lambda_{\mathbf{a},\mathbf{b}}}$，并输出$f|_{\lambda_{\mathbf{a},\mathbf{b}}}(0)=f(\mathbf{b})$。根据马尔可夫不等式，这又意味着，对于$\mathbf{b}$的选择，以至少$1/2$的概率，局部算法 $A_{\mathbf{b},\,f(\mathbf{b})}$会对至少占 $(1-\epsilon)$ 比例的点输出 $f(\mathbf{a})$，其中$\mathbf{a}$满足 $\epsilon=\frac{2\delta}{\sigma-1}+\frac{2}{\xi^2 q}$.

查询复杂度和列表大小。 列表大小显然是 $\mathbb{F}_q$ 中可能取值的数量 q，查询复杂度显然是一条直线上的点数 q。

7.3 Reed-Muller码的局部列表译码达到Johnson界

上一节介绍的 Reed-Muller码局部列表译码算法，只能达到趋近于 $1-\sqrt{\sigma}\cdot(1-\delta)$ 的译码半径（其中常数 $\sigma>1$ 足够大），这小于 $1-\sqrt{1-\delta}$ 的 Johnson界。虽然我们没有尝试优化 σ 的取值，但注意到它不可能小于 2。原因是，为了在断言 7.10 中应用并集界，我们需要列表大小 $L':=|\mathcal{L}|$ 小于 $\frac{1}{1-\delta}$（因为列表中每个多项式的失败概率最高可达 $1-\delta$），而根据式 (13)，只有当译码半径小于 $1-\sqrt{2(1-\delta)}$ 时，才能保证这样的列表大小。

本节将介绍一种改进的算法，能够对 Reed-Muller码进行局部列表译码，达到 Johnson界。具体而言，和之前一样，固定一个素数幂 q 以及正整数 k,m，使得 $k<q$，并令 $\mathrm{RM}_{q,m}(k)$ 表示相应的 Reed-Muller码。令 $\delta:=1-\frac{k}{q}$ 表示该码的相对距离，设 $\gamma,\xi>0$ 为参数，并令 $\alpha:=1-\sqrt{(1+\gamma)\cdot(1-\delta)-\xi}$。我们将证明，对于任意 $s\geq 1$，当 $Q=r^m\cdot q,\epsilon=\frac{2\delta}{\gamma s}+O\left(\frac{1}{\xi^2 q}\right)$ 且 $L=\binom{r}{s}^s$ 时，该码是一个 (Q,α,ϵ,L)-ALLDC，其中 $r:=\frac{8\delta s}{\gamma(1-\delta)}$。因此，对于 $s>\frac{16\delta}{\gamma}$ 且 q 足够大时，失败概率 ϵ 小于 $\frac{\delta}{8}$，所以根据第 7.1 节的结果和引理 7.8，该码也是一个 $(r^m\cdot q^2,\alpha,L)$-局部列表可解码码。注意，对于常数 m,s,γ 和 δ，查询复杂度为 $r^m\cdot q=O(q^2)$；当 $m>2$ 且 q 增长时，这远小于该码的码长 q^m。

概述。 改进算法的核心思路是同时利用导数来消除列表中的歧义。具体而言，与之前一样，建议通过选择一个均匀随机点$\mathbf{b}\in\mathbb{F}_q^m$来生成；但现在，猜测 v 应当等于某个整数 $s\geq 1$ 对应的 $f(X_1,\ldots,X_m)$ 在 $\mathbf{b}$ 处所有阶数小于 s 的多元导数（多元导数的定义见第 2.2 节）。为了利用导数，我们回顾一下，根据事实 2.3，任意一对次数为 k 的单变量多项式，其阶数小于 s 的导数在至多占所有点 $\frac{k}{sq}=\frac{1-\delta}{s}$ 这一比例的点上相同。因此，建议无法消除 $\mathcal{L}$中任意一对多项式歧义的概率至多为 $\frac{1-\delta}{s}$；此时取 $s\gg L'$，便可以对 $\mathcal{L}$应用并集界。

然而，这种方法的一个缺点是，它会显著增大局部列表译码算法的列表大小，也就是点$\mathbf{b}$处所有 m元、阶数小于 s的导数的不同猜测数量。具体来说，不同猜测的数量为 $q^{\binom{m+s-1}{m}}$（远大于该码的码长 q^m！），因为阶数小于 s 的 m元导数共有 $\binom{m+s-1}{m}$个，而且每个这样的导数都可以取 $\mathbb{F}_q$中的任意值。

为了减小列表大小，我们略微扩展局部列表译码模型，向局部列表译码算法 A 提供对接收字 w 的查询访问（从而使算法 A 能够在输出局部算法列表 $A_1,\ldots,A_L$之前对 w进行少量查询）。为利用该模型，局部列表译码算法 A 首先选取经过$\mathbf{b}$的 t 条随机直线，然后（全局地）对 f 在这些直线上的限制进行列表译码，最后仅输出那些与这些直线在$\mathbf{b}$ 处的方向导数在相当大比例的直线上相一致的、关于 $f^{(<s)}(\mathbf{b})$的猜测 v。通过对 t 条随机直线的联合分布进行审慎选择，对猜测数量的界定可归结为Reed-Muller码的一个列表恢复问题实例（列表译码的某种推广），特别地，我们可以利用Johnson界在列表恢复设定下的一个推广来界定此类

猜测。

近似局部列表译码算法的正式描述见下文图 9，随后给出正确性分析。在正式陈述该算法之前，我们先固定一些记号。这些记号的动机来自以下 Hasse 导数的链式法则，该法则将多元多项式在直线上的方向导数与其全局导数联系起来（证明直接由 Hasse 导数的定义得出，留作练习）。

事实 7.11 (Hasse 导数链式法则)。设 $f(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$，设 $\mathbf{a}$、$\mathbf{u} \in \mathbb{F}^m$，并设$\lambda(T) = \mathbf{a} + T\mathbf{u}$为经过 $\mathbf{a}$且方向为 $\mathbf{u}$的直线。那么，对于任意非负整数 i和 $T \in \mathbb{F}$，

$$(f|_\lambda)^{(i)}(T) = \sum_{\mathbf{i}:\mathsf{wt}(\mathbf{i})=i} f^{(\mathbf{i})}(\mathbf{a} + T\mathbf{u}) \cdot \mathbf{u}^{\mathbf{i}}. \tag{14}$$

对于整数 m, s，设 $I_{m,s} := \{\mathbf{i} \in \mathbb{N}^m \mid \mathsf{wt}(\mathbf{i}) < s\}$；对于元素 $v \in \mathbb{F}^{I_{m,s}}$和方向$\mathbf{u} \in \mathbb{F}_q^m$，我们将 v沿方向 $\mathbf{u}$的限制 $v|_{\mathbf{u}} \in \mathbb{F}_q^s$定义为 $v|_{\mathbf{u}} := \left(\sum_{\mathbf{i}:\mathsf{wt}(\mathbf{i})=i} v_{\mathbf{i}} \cdot \mathbf{u}^{\mathbf{i}}\right)_{i=0,1,\ldots,s-1}$注意，采用这种记号，式 (14) 可改写为

$$(f|_\lambda)^{(<s)}(T) = \left(f^{(<s)}(\mathbf{a} + T\mathbf{u})\right)|_{\mathbf{u}}. \tag{15}$$

现在我们来描述该算法。

近似局部列表译码 里德-穆勒码$_{q,\ m}(k)$**：**

▷ 令 $s \geq 1$ 为一个参数，令 $r := \gamma \frac{8\delta s}{1-\delta()}$，并令 U 为 $\mathbb{F}_q$ 中任意一个大小为 r 的子集。

近似局部列表译码算法 A**：**

- **输入：** 对函数 w 进行查询访问： $\mathbb{F}_q^m \to \mathbb{F}_q$。
- **输出：** 局部算法列表。

1. 选取随机点 $\mathbf{b} \in \mathbb{F}_q^m$和$\mathbf{u}_0 \in \mathbb{F}_q^m$。
2. 对每个 $\mathbf{u} \in U^m$：

   (a) 查询直线 $\lambda_{\mathbf{u}}(T) := \mathbf{b} + T(\mathbf{u}_0 + \mathbf{u})$ 上的所有点，该直线经过 $\mathbf{b}$ 且方向为 $\mathbf{u}_0 + \mathbf{u}$。(b) 使用图3中给出的算法，求所有次数小于 k 且与 $w|_{\lambda_{\mathbf{u}}}$ 的距离不超过 $(1 - \sqrt{(1+\gamma)\cdot(1-\delta)})$ 的单变量多项式 $g(T) \in \mathbb{F}_q[T]$ 的列表 $\mathcal{L}_{\mathbf{u}}$。(c) 令 $S_{\mathbf{u}} = \left\{g^{(<s)}(0) \mid g(T) \in \mathcal{L}_{\mathbf{u}}\right\}$。

3. 令 V 为包含所有满足以下条件的 $v \in \mathbb{F}^{I_{m,\ q}\ \ s}$ 的集合：对于点 $\mathbf{u} \in U^m$ 中至少 $\frac{1}{2}$ 的点，$v|_{\mathbf{u}_0+\mathbf{u}} \in S_{\mathbf{u}}$。
4. 对于任意 $v \in V$，输出下文定义的局部算法 $A_{\mathbf{b},\ v}$。

局部算法 $A_{\mathbf{b},\ v}$**：**

- **输入：** 对函数 w：$\mathbb{F}_q^m \to \mathbb{F}_q$ 的查询访问，给定一点 $\mathbf{a} \in \mathbb{F}_q^m$。
- **输出：** $\mathbb{F}_q$中的一个值。1. 查询直线 $\lambda_{\mathbf{a},\ \mathbf{b}}(T)$：$=(1-T)\cdot\mathbf{a} + T\cdot\mathbf{b} = \mathbf{a} + T(\mathbf{b}-\mathbf{a})$ 上经过 $\mathbf{a}$和 $\mathbf{b}$ 的所有点。

2. 使用图3中给出的算法，求列表 $\mathcal{L}$，其中包含所有次数小于 k 的一元多项式 $g(T) \in \mathbb{F}_q[T]$，它们与 $\overline{w|_{\lambda_{\mathbf{a},\ \mathbf{b}}(T)}}$ 的距离不超过（$1 - \sqrt{(1+\gamma)\cdot(1-\delta)}$）。
3. 如果存在唯一的多项式 $g(T) \in \mathcal{L}$，使得 $g^{(<s)}(1) = v|_{\mathbf{b}-\mathbf{a}}$，则输出 $g(0)$；否则，输出$\perp$。

图 9：Reed-Muller码达到Johnson界的局部列表译码

正确性。设 $f(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ 是一个次数小于 k 的多项式，使得 $f(\mathbf{a}) \neq w(\mathbf{a})$ 对至多 α 比例的项成立，其中$\mathbf{a} \in \mathbb{F}_q^m$。首先证明，对于随机选取的 $\mathbf{b}$，$\mathbf{u}_0 \in \mathbb{F}_q^m$，以高概率有 $f^{(<s)}(\mathbf{b}) \in V$。

命题7.12。对于 $\mathbf{b}$、$\mathbf{u}_0 \in \mathbb{F}_q^m$ 的选取，以至少 $1 - \frac{2}{\xi^2 q}$ 的概率，有 $f^{(<s)}(\mathbf{b}) \in V$。

证明。 首先注意到，对于任意固定的 $\mathbf{u} \in U^m$，由于 $\mathbf{b}$ 和 $\mathbf{u}_0$ 是均匀随机选取的，因此直线$\lambda_{\mathbf{u}}(T) = \mathbf{b} + T(\mathbf{u}_0 + \mathbf{u})$是均匀随机的。因此，对于任意固定的 $\mathbf{u} \in U^m$，与断言 7.9 中相同的分析表明，在 $\mathbf{b}$ 和 $\mathbf{u}_0$,的选取上，以至少 $1 - \frac{1}{\xi^2 q}$ 的概率成立 $f|_{\lambda_{\mathbf{u}}} \in \mathcal{L}_{\mathbf{u}}$。由马尔可夫不等式，这进而意味着，在 $\mathbf{b}$ 和$\mathbf{u}_0$,的选取上，以至少 $1 - \frac{2}{\xi^2 q}$ 的概率，对至少 $\frac{1}{2}$的点 $\mathbf{u} \in U^m$成立 $\overline{f|_{\lambda_{\mathbf{u}}} \in \mathcal{L}_{\mathbf{u}}}$。

接下来观察到，对于任意满足 $f|_{\lambda_{\mathbf{u}}} \in \mathcal{L}_{\mathbf{u}}$的 $\mathbf{u} \in U^m$，我们有 $(f|_{\lambda_{\mathbf{u}}})^{(<s)}(0) \in S_{\mathbf{u}}$。此外，由 (15) 可知，对每个这样的 $\mathbf{u}$，成立 $(f|_{\lambda_{\mathbf{u}}})^{(<s)}(0) = \left(f^{(<s)}(\mathbf{b})\right)|_{\mathbf{u}_0+\mathbf{u}}$。我们得出结论：在 $\mathbf{b}$和 $\mathbf{u}_0$,的选取上，以至少 $1 - \frac{2}{\xi^2 q}$的概率，我们有 $\left(f^{(<s)}(\mathbf{b})\right)|_{\mathbf{u}_0+\mathbf{u}} \in S_{\mathbf{u}}$对至少 $1/2$的 $\mathbf{u} \in U^m$成立，此时 $f^{(\preceq s)}(\mathbf{b})$ 将被包含在 V中。 □

接下来我们想要证明：对于 $\mathbf{b}$ 的选择，以至少 $1/2$ 的概率，局部算法$A_{\mathbf{b},f^{(<s)}(\mathbf{b})}$ 能够为大多数点 $\mathbf{a} \in \mathbb{F}_q^m$正确恢复 $f(\mathbf{a})$。这部分分析与对图 8 中算法的分析非常相似，主要区别在于：我们用低次多项式零点最大数量的更强版本替代了标准界限；该版本还考虑了重数，由事实 2.3 给出，从而使我们能够处理更大的列表 $\mathcal{L}$。

更具体地说，与之前一样，为证明上述结论，我们首先要证明：对于 *both* 随机 $\mathbf{a} \in \mathbb{F}_q^m$ 和随机 $\mathbf{b} \in \mathbb{F}_q^m$ 的选择，以高概率有 $A_{\mathbf{b},f^{(<s)}(\mathbf{b})}$ 在输入$\mathbf{a}$上正确计算 $f(\mathbf{a})$。下面的断言表明：对于 $\mathbf{a}$,$\mathbf{b}$ 的选择，以高概率存在一个多项式$g(T) \in \mathcal{L}$，它在直线 $\lambda_{\mathbf{a},\mathbf{b}}$ 上与 f 一致。证明与断言 7.9 的证明非常相似。

断言 7.13。 在随机选择$\mathbf{a}$、$\mathbf{b}\in \mathbb{F}_q^m$时，以至少 $1 - \frac{1}{\xi^2 q}$ 的概率，有 $f|_{\lambda_{\mathbf{a},\mathbf{b}}} \in \mathcal{L}$。

下一个断言说明，随机选择$\mathbf{a}$、$\mathbf{b}$时，以高概率不存在多项式 $h(T) \in \mathcal{L}$，除 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}$之外，使得 $h^{(<s)}(1) = f^{(<s)}(\mathbf{b})|_{\mathbf{b}-\mathbf{a}}$。

断言 7.14。 随机选择$\mathbf{a}$、$\mathbf{b} \in \mathbb{F}_q^m$时，以至少 $1 - \frac{\delta}{\gamma s}$ 的概率，不存在多项式$h(T) \in \mathcal{L}$，除 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}$ 之外，使得 $h^{(<s)}(1) = f^{(<s)}(\mathbf{b})|_{\mathbf{b}-\mathbf{a}}$。

证明。 证明与断言 7.10 的证明类似，不同之处在于，我们使用事实 2.3 来界定 h 与 $f|_\lambda$ 在$\mathbf{b}$ 上所有低于 s 阶导数都相同的概率。具体而言，与断言 7.10 的证明一样，我们可以将随机选择$\mathbf{a}$,$\mathbf{b} \in \mathbb{F}_q^m$的过程视为：先随机选择$\mathbf{a} \in \mathbb{F}_q^m$，再选择一条经过$\mathbf{a}$的随机直线 λ，最后令$\mathbf{b} \in \mathbb{F}_q^m$为该直线 λ上的随机点。因此，接下来固定一点$\mathbf{a}$和一条经过它的直线 λ，并令 $\mathcal{L}$ 为次数小于 k、且在该直线上与 w 的差异为 $(1 - \sqrt{(1+\gamma)(1-\delta)})$-close 的一元多项式列表。我们将证明，随机选择$\mathbf{b}$时，以至少 $1 - \frac{\delta}{\gamma s}$ 的概率，不存在多项式 $h(T) \in \mathcal{L}$，除 $f|_\lambda$之外，使得 h与 $f|_\lambda$在$\mathbf{b}$上的所有低于 s阶导数都相同。

固定一个多项式 $h(T) \in \mathcal{L}$，使得 $h(T) \neq f|_\lambda(T)$。那么，由于 h和 $f|_\lambda$都是次数小于 k的多项式，根据事实 2.3，它们在这条直线上至多 $\frac{1-\delta}{s}$ 比例的点上，所有阶数小于 s 的导数都相同。此外，注意到根据 Johnson界（参见定理 2.1），我们有

$$|\mathcal{L}| \leq \frac{\delta}{(1+\gamma)\cdot(1-\delta) - (1-\delta)} \leq \frac{\delta}{\gamma(1-\delta)}. \tag{16}$$

因此，对 $\mathcal{L}$中的所有元素应用并集界可知，存在一个多项式$h(T) \in \mathcal{L}$不同于 $f|_\lambda$，且在 $\mathbf{b}$处所有阶数小于 s的导数都与 $f|_\lambda$相同的概率至多为 $\frac{\delta}{\gamma s}$。由 (15) 可知，这进一步意味着，对 $\mathbf{a}$,$\mathbf{b} \in \mathbb{F}_q^m$ 的选取，至少以 $1 - \frac{\delta}{\gamma s}$ 的概率有$h^{(<s)}(1) \neq f^{(<s)}(\mathbf{b})|_{\mathbf{b}-\mathbf{a}}$成立。

□

根据上述断言 7.12、7.13 和 7.14，我们得出：对 $\mathbf{a}$、$\mathbf{b}$ 和 $\mathbf{u}$ 的选择，至少以 $1 - \frac{\delta}{\gamma s} - \frac{3}{\xi^2 q}$ 的概率，$f^{(<s)}(\mathbf{b}) \in V$；并且在执行 $A_{\mathbf{b}}$ 的过程中，$f^{(<s)}(\mathbf{b})$ 满足 $f|_{\lambda_{\mathbf{a}、\mathbf{b}}} \in \mathcal{L}$，且不存在除 $f|_{\lambda_{\mathbf{a}}}$ 之外的多项式 $h(T) \in \mathcal{L}$，使得 $h^{(<s)}(1) = f^{(<s)}(\mathbf{b})|_{\mathbf{b}-\mathbf{a}}$。在这种情况下，局部算法 $A_{\mathbf{b},f^{(<s)}(\mathbf{b})}$ 将在步骤 3 中设置 $g = f|_{\lambda_{\mathbf{a},\mathbf{b}}}$，并输出 $f|_{\lambda_{\mathbf{a},\mathbf{b}}}(0) = f(\mathbf{a})$。

根据马尔可夫不等式，这又意味着：对 $\mathbf{b}$ 和 $\mathbf{u}$ 的选择，至少以 $1\ 2$ 的概率，$_0$，局部算法 $A_{\mathbf{b},\ f^{(<s)}}$ $(\mathbf{b})$ 将由 A 输出，并且对于至少占 $1-\epsilon$ 比例的点 $\mathbf{a}$（其中 $\epsilon = \frac{2\delta}{\gamma s} + \frac{6}{\xi^2 q}$），输出 $f(\mathbf{a})$。

查询复杂度。近似局部列表译码算法 A 的查询复杂度为 $r^m \cdot q$，因为它查询 r^m 条直线，每条直线上有 q 个点；而每个局部算法$A_{\mathbf{b},\ v}$ 的查询复杂度是直线上的点数 q。

列表大小。还需对 A输出的局部算法数量进行上界估计，这相当于对集合 V的大小进行上界估计。为此，固定 $\mathbf{b}$、$\mathbf{u}_0 \in \mathbb{F}_q^m$，并回顾：对于任意 $v \in V$，至少有一半的点 $\mathbf{u} \in U^m$满足$v|_{\mathbf{u}_0+\mathbf{u}} = \left(\sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} v_{\mathbf{i}} \cdot (\mathbf{u}_0+\mathbf{u})^{\mathbf{i}}\right)_{i=0,1,\ldots,s-1} \in S_{\mathbf{u}}$，其中 $S_{\mathbf{u}} = \left\{g^{(<s)}(0) \mid g(T) \in \mathcal{L}_{\mathbf{u}}\right\} \subseteq \mathbb{F}_q^s$。对于 $\mathbf{u} \in U^m$和 $i \in \{0,1,\ldots,s-1\}$，令 $S_{\mathbf{u},i} := \left\{g^{(i)}(0) \mid g(T) \in \mathcal{L}_{\mathbf{u}}\right\} \subseteq \mathbb{F}_q$，并令 V_i 为包含所有向量 $v \in \mathbb{F}_q^{\{\mathbf{i}|\mathrm{wt}(\mathbf{i})=i\}}$的集合，使得至少有一半的点 $\mathbf{u} \in U^m$满足$\sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} v_{\mathbf{i}} \cdot (\mathbf{u}_0+\mathbf{u})^{\mathbf{i}} \in S_{\mathbf{u},i}$。注意，由 (16) 以及我们对$r = \frac{8\delta s}{\gamma(1-\delta)}$ 的选择可知，

$$|S_{\mathbf{u},i}| \le |S_{\mathbf{u}}| \le |\mathcal{L}_{\mathbf{u}}| \le \frac{\delta}{(1-\delta)\gamma} = \frac{r}{8s}.$$

我们将证明，对于任意 $i \in \{0,1,\ldots,s-1\}$，V_i的大小至多为 $\frac{r}{s}$，因此 V的大小至多为$\binom{r}{s}^s$。为证明上述结论，固定 $i \in \{0,1,\ldots,s-1\}$，并令

$$\mathcal{L}_i := \{h \in (\mathbb{F}_q)_{<s}[X_1,\ldots,X_m] \mid h(\mathbf{u}_0+\mathbf{u}) \in S_{\mathbf{u},i} \text{ for at least half of the points } \mathbf{u} \in U^m\}.$$

接下来我们观察到 $|V_i| \le |\mathcal{L}_i|$。为此，将每个 $v \in V_i$ 映射为多项式 $h_v(\mathbf{X}) := \sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} v_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$，并注意到，对于任意不同的 $v, v' \in V_i$，$h_v \in \mathcal{L}_i$ 且 $h_v \ne h_{v'}$。因此，只需对 $\mathcal{L}_i$的大小给出上界。

对 $\mathcal{L}_i$ 大小进行界定的问题可表述如下。给定素数幂 q、正整数k, m以及一个大小为 r的子集 $U \subseteq \mathbb{F}_q$，令$\mathrm{RM}_{q,m}(U;\ k)$表示定义在 $\mathbb{F}_q$上的码，其码长为 r^m；该码将任意多项式 $f(X_1,\ldots,X_m) \in (\mathbb{F}_q)_{<k}[X_1,\ldots,X_m]$ 关联到一个码字$(f(\mathbf{u}))_{\mathbf{u}\in U^m} \in \mathbb{F}_q^{r^m}$。注意，Reed-Muller码 $\mathrm{RM}_{q,m}(k)$对应于 $U = \mathbb{F}_q$这一特殊情形。众所周知，$\mathrm{RM}_{q,m}(U;\ k)$的相对距离至少为$1 - \frac{k}{r}$ [Sch80, Zip79, DL78]。

用上述术语来说，对于码 $\mathrm{RM}_{q,m}(U;\ s)$（相对距离为 $\delta' := 1 - \frac{s}{r}$）中的每个码字条目$\mathbf{u} \in U^m$，我们都给定一个小的输入列表$S_{\mathbf{u},i}$，其中包含 $\mathbb{F}_q$中的若干可能取值，大小至多为 $\ell := \frac{r}{8s}$；目标是界定满足以下条件的 $\mathrm{RM}_{q,m}(U;\ k)$ 码字数量：对于至多 $\alpha' := \frac{1}{2}$ 个码字条目$\mathbf{u}$，$c_{\mathbf{u}} \notin S_{\mathbf{u},i}$。这是一个著名的问题，称为列表恢复，它推广了列表译码问题；当所有输入列表 $S_{\mathbf{u}}$ 的大小均为 1 时，就对应列表译码问题。特别地，将 Johnson 界推广到列表恢复情形的结果（例如，参见 [GKO+18，引理 5.2]）表明，码字数量至多为

$$\frac{\delta'\ell}{(1-\alpha')^2 - \ell(1-\delta')} \le \frac{\ell}{\frac{1}{4} - \frac{\ell s}{r}} = \frac{r}{s}.$$

7.4 多变量重数码达到最小距离时的局部列表译码

在上一节中，我们展示了如何将Reed-Muller码局部列表译码至*Johnson*界。阻止我们突破Johnson界的主要障碍在于，Reed-Muller码的局部列表译码算法将里德-所罗门码的列表译码算法用作子程序，而其译码范围从

大致相同的译码半径开始，而且我们目前尚不知道如何在列表规模较小的情况下，将里德-所罗门码列表译码到超出Johnson界的范围。

然而，对于重数足够大的（单变量）重数码 s，第4.2节和第5.2节的结果表明，它们可在达到其 最小距离 时实现常数列表大小的列表译码，因此我们有理由预期，也可以对重数足够大的多变量 重数码 s 进行局部列表译码，直至其最小距离。事实上，可以使用一种与图 9 中算法非常相似的算法，对多变量重数码进行局部列表译码，直至其最小距离。由于多变量重数码的局部列表译码算法与 Reed-Muller码的算法非常相似，但符号表示要繁复得多，因此我们不在此正式描述多变量重数码的算法，而只指出将图 9 中的算法应用于多变量重数码时需要进行的主要改动。有关该算法的正式描述，请读者参见[KRSW23，第 4] 节。

首先，我们注意到，在多变量重数码的情形下，为了对 $w|_\lambda$在某条直线 λ上的限制进行列表译码，我们还需要获得该直线上的方向导数的预言机访问权限，而 w只提供全局导数的预言机访问权限。不过，我们可以利用 (15)，根据 w 在直线上任意一点的全局导数，计算出 w 在该点的方向导数。

其次，在多变量重数码的情形下，局部算法 $A_{\mathbf{b},\ v}$需要输出 f在$\mathbf{a}$处的全局导数 $f^{(<s)}(\mathbf{a})$，而不只是值 $f(\mathbf{a})$。利用算法 $A_{\mathbf{b},\ v}$ 的步骤 3 中确定的多项式 $g(T)$，我们可以以较高概率恢复 f 在$\mathbf{a}$处沿直线 $\lambda_{\mathbf{a},\ \mathbf{b}}$方向的方向导数；然而，这些导数通常无法确定全局导数。为了解决这个问题，我们可以先采用与近似局部列表译码算法 A 完全相同的流程，得到 $f^{(<s)}(\mathbf{a})$ 值的少数几个可能猜测 V'；然后，不再在步骤 3 中输出 $g(0)$，而是将满足 $v'|_{\mathbf{b}-\mathbf{a}} = g^{(<s)}(0)$ 的唯一 $v' \in V'$ 作为 $f^{(<s)}(\mathbf{a})$ 的猜测输出（如果存在这样的 v'）。

为了证明上述解法有效，我们首先回顾，根据命题7.12，我们以高概率有 $v_0 := f^{(<s)}(\mathbf{a}) \in V'$。因此，只需证明对于任意不同于$v_0$ 的 $v' \in V'$，以高概率都有 $v'|_{\mathbf{b}-\mathbf{a}} \neq v_0|_{\mathbf{b}-\mathbf{a}}$。为此，固定一个不同于 v_0的 $v' \in V'$，并回顾 $v'|_{\mathbf{b}-\mathbf{a}} = \left(\sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} v'_{\mathbf{i}} \cdot (\mathbf{b}-\mathbf{a})^{\mathbf{i}}\right)_{i=0,1,\ldots,s-1}$ 以及 $v_0|_{\mathbf{b}-\mathbf{a}} = \left(\sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} (v_0)_{\mathbf{i}} \cdot (\mathbf{b}-\mathbf{a})^{\mathbf{i}}\right)_{i=0,1,\ldots,s-1}$。由于 $v' \neq v_0$，存在某个 $i \in \{0,1,\ldots,s-1\}$，使得多项式 $h_{v'}(\mathbf{X}) := \sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} v'_{\mathbf{i}} \cdot \mathbf{X}^{\mathbf{i}}$ 和 $h_{v_0}(\mathbf{X}) := \sum_{\mathbf{i}:\mathrm{wt}(\mathbf{i})=i} (v_0)_{\mathbf{i}} \cdot \mathbf{X}^{\mathbf{i}}$ 不同。但由于这两个多项式的次数都至多为 s，由此可知，对 $\mathbf{a}$ 和 $\mathbf{b}$ 的选择，以至少 $1 - \frac{s}{q}$ 的概率有 $h_{v'}(\mathbf{b}-\mathbf{a}) \neq h_{v_0}(\mathbf{b}-\mathbf{a})$，此时我们也有 $v'|_{\mathbf{b}-\mathbf{a}} \neq v_0|_{\mathbf{b}-\mathbf{a}}$。对 V' 的所有元素应用并集界，我们得出结论：以至少 $1 - \frac{s|V'|}{q}$ 的概率，不存在不同于 $v_0 = f^{(<s)}(\mathbf{a})$的 $v' \in V'$使得 $v'|_{\mathbf{b}-\mathbf{a}} = v_0|_{\mathbf{b}-\mathbf{a}}$。

局部列表译码达到容量。上文概述了一种算法，可对重数足够大的 s 元多变量重数码进行局部列表译码，达到其 $\delta := 1 - \frac{k}{sq}$ 的最小相对距离。不过请回顾一下，重数为 s 的 m元重数码的码率为 —

$$\frac{\binom{m+k-1}{m}}{\binom{m+s-1}{m} \cdot q^m} \leq \frac{\frac{1}{m!} \cdot (m+k)^m}{\frac{1}{m!} \cdot s^m \cdot q^m} = \left(\frac{k+m}{k}\right)^m \cdot \left(\frac{k}{sq}\right)^m = \left(1 + \frac{m}{k}\right)^m \cdot (1-\delta)^m,$$

因此，对于固定的 $m > 1$ 和增长的 k，上述算法所达到的译码半径远低于列表译码容量。尽管如此，该算法可用于得到另一族直至容量均可局部列表译码的码。

更详细地说，回想一下，在第 7.3 节中我们遇到了列表恢复的概念，它扩展了列表译码的概念。回想一下，在列表恢复中，对于每个码字条目，给定一个由可能取值构成的小输入列表，目标是返回与这些输入列表中大多数相一致的所有码字的列表。更形式化地说，对于 $\alpha \in (0, 1)$ 以及正整数 ℓ， L，我们称码 $C \subseteq \Sigma^n$ 是 (α, ℓ, L)-列表可恢复 的，如果对于任意子集 $S_1, \ldots\ldots, S_n \subseteq \Sigma$，且每个子集的大小至多为 ℓ，则至多有 L 个不同的码字$c \in C$ 满足 $w_i \notin S_i$ 对至多 α 比例的指标 $i \in [n]$ 成立。注意，列表译码对应于 $\ell = 1$ 的特殊情形。所谓从 α错误比例进行列表恢复的问题，就是求出这些码字的列表。

我们在第 7.3 节中已经看到，列表恢复的概念可能对局部列表译码有用。考虑列表恢复这一概念的另一个动机是，已知高码率码（码率接近 1）若能从恒定的错误比例以及恒定大小的输入列表 S_i 中进行列表恢复，则可被变换为达到容量的列表可译码码，而且该变换还保持局部性（该变换基于扩展图，超出了本综述的范围，更多细节见[KRSW23，附录 C] ）。

通常情况下，上述所有局部列表译码算法都可以以相近的性能推广到列表恢复的设定中。此外，多变量重数码相对于 Reed-Muller码的另一个优势是它们可以达到更高的码率。具体而言，尽管重数为 s 、相对距离为 δ 的 m元重数码的码率：$= 1 - \frac{k}{sq}$ 至少为

$$\frac{\binom{m+k-1}{m}}{\binom{m+s-1}{m} \cdot q^m} \geq \frac{\frac{1}{m!} \cdot k^m}{\frac{1}{m!} \cdot (s+m)^m \cdot q^m} = \left(\frac{s}{s+m}\right)^m \cdot \left(\frac{k}{sq}\right)^m = \left(1 - \frac{m}{s+m}\right)^m \cdot (1-\delta)^m,$$

m元 Reed-Muller码的相对距离为 $\delta' := 1 - \frac{k}{q}$ 时，其码率仅为 _

$$\frac{\binom{m+k-1}{m}}{q^m} \leq \frac{\frac{1}{m!} \cdot (m+k)^m}{q^m} = \frac{1}{m!} \cdot \left(\frac{k+m}{k}\right)^m \cdot \left(\frac{k}{q}\right)^m = \frac{1}{m!} \cdot \left(1 + \frac{m}{k}\right)^m \cdot (1-\delta')^m,$$

特别是，这意味着对于任意 $m > 1$，Reed-Muller码的码率至多为12；而对于$\delta \approx \frac{1}{m}$、 $s \approx m^2$和不断增长的 m，多变量重数码的码率可以接近 1。 因此，可以将多变量重数码的局部列表译码算法扩展到列表恢复的情形，从而得到高码率局部列表可恢复码，再将其转化为达到容量的局部列表可译码码。更多细节请参阅 [KRSW23，附录 C] 。

7.5 文献注记

局部可译码码和局部可纠错码分别由 [BFLS91、KT00、STV01] 和 [Lip90、BK95], 提出。关于局部可译码码和局部可纠错码的全面综述，参见 [Yek12] 。局部列表可译码码由 [GL89、STV01], 提出，自问世以来，已在理论计算机科学、密码学 [GL89], 、学习理论 [KM93],、平均情形到最坏情形归约 [Lip90], 以及困难性放大 [BFNW93、STV01]等领域得到多种应用。

第 7.1 节介绍的 Reed-Muller码局部纠错 算法由[Lip90, BF90, GLR+91] 提出（另见 [Yek12, 第 2.2 节.2]）；而备注 7.5 中介绍的利用曲线进行改进的方法由 Gemmell 和 Sudan [GS92] 提出（另见 [Yek12, 第 2.2 节.3]）。第 7.2 节介绍的、超出唯一译码半径的 Reed-Muller码局部列表译码 算法由 Arora 和 Sudan [AS03] 以及 Sudan、Trevisan 和 Vadhan [STV01]提出。第 7.3 节介绍的、达到 *Johnson*界的 Reed-Muller码局部列表译码算法沿用了以下思路

这些思路由 Kopparty、Ron-Zewi、Saraf 和 Wootters [KRSW23] 提出，用于对多变量重数码进行最小距离范围内的局部列表译码。这里我们介绍他们的算法的一个更简单版本，用于对 Reed-Muller码进行 Johnson界范围内的局部列表译码。Brander 和 Kopparty 提出了其他方法，通过限制到平面而非直线，对 Reed-Muller码进行 Johnson界范围内的局部列表译码 [BK09]（另见 [GK16a, Kop15]）。

Kopparty、Saraf 和 Yekhanin 提出了针对多变量重数码 的局部纠错算法 [KSY14], ，他们也引入了这类码，并指出其码率可以高于相应的 Reed-Muller 码。第7.4节概述的针对多变量重数码、可译至其最小距离的局部列表译码 算法由 [KRSW23]提出。

第7.4节提到的基于扩张图的变换，可将高码率局部列表可恢复码转化为达到容量的局部列表可译码码；该变换由 Gopi、Kopparty、Oliveira、Ron-Zewi 和 Saraf [GKO+18] 以及 Hemenway、Ron-Zewi 和 Wootters [HRW20]提出。它基于 Alon、Edmonds 和 Luby 在唯一译码设定下提出的基于扩张图的变换 [AEL95, AL96], ，以及 Guruswami 和 Indyk [GI02], 将其扩展到列表译码、Kopparty、Meir、Ron-Zewi 和 Saraf [KMRS17]将其扩展到局部解码的工作。最近，这一变换被用于构造达到容量的（非局部）列表可译码码（不依赖基于多项式的码） [ST25],，甚至构造出达到广义辛格尔顿界的码 [JMST25]。

本节讨论了多元码的局部列表译码算法。这类算法本质上是随机化的（因为对手很容易破坏确定性算法所有查询的答案），并且只有当码是在整个 $\mathbb{F}_q^m$ 上求值时才有效（因为需要让一条随机直线——或相关的代数低维结构——穿过定义域）。在 $\mathbb{F}_q^m$ 上，Pellikaan 和 Wu [PW04] 给出了一种高效的确定性（全局）列表译码算法，可将 Reed-Muller码译码至 Johnson界；随后，Kopparty [Kop15] 将该算法扩展到任意重数的多变量重数码，使其可译码至 Johnson界。最近，Bhandari、Harsha、Kumar 和 Sudan [BHKS24a] 给出了一种高效的确定性算法，可对变量数为常数且重数足够大的多变量重数码进行列表译码，直至其最小距离。

有趣的是，定理 2.6 给出的带重数根的根的数量上界，在定义域为形如 $A_1 \times \cdots \times A_m$ 的乘积集合时也适用，其中 $A_1, \ldots, A_m$ 是 $\mathbb{F}_q$ 的任意子集。然而，对于任意乘积集合，直到最近才有研究证明，Reed-Muller码可由 Kim 和 Kopparty [KK17], 高效地唯一译码至其最小距离的一半；随后，Bhandari、Harsha、Kumar 和 Shanka [BHKS23] 将该算法扩展到任意乘积集合上的任意重数多变量重数码的唯一译码。据我们所知，目前还没有任何高效算法能够在任意乘积集合上，将 Reed-Muller码或任意重数的多变量重数码列表译码至超过最小距离一半的范围。值得注意的是，前述[BHKS24a] 算法能够在任意乘积集合上，将变量数为常数且重数足够大的重数码列表译码至其最小距离。

8 结论与开放问题

本书综述了多项式码列表译码领域的最新进展。具体而言，我们研究了里德-所罗门码的列表译码性质，证明了重数码等相关多项式码族能够高效地实现接近容量的列表译码，并讨论了如何通过更精细的分析，获得更优的列表大小组合上界。我们还介绍了这些列表译码算法的快速（近线性时间）实现，以及针对 Reed-Muller码和多变量重数码等多变量多项式码的局部（亚线性时间）列表译码算法。

开放问题。本书最后提出了几个引人深思、值得进一步研究的问题；截至本综述撰写之时，这些问题仍未得到解决。

1. **达到列表译码容量的显式且高效列表可译码 Reed-Solomon 码**。在第 3.4 节中，我们展示了 Reed-Solomon 码通常无法在超出 Johnson界太多的范围内进行列表译码；而在第 5.1 节中，我们展示了在随机求值点上取值的 Reed-Solomon 码以较高概率（从组合意义上）可列表译码至容量，并且具有最优列表大小。一个非常有趣的问题是，求出能够使 Reed-Solomon 码列表译码至容量的显式求值点，同时还要设计高效的列表译码算法。

2. **在固定大小字母表上达到列表译码容量的显式且高效列表可译码码**。在第 5.4 节中，我们提到，通过采用代数几何码，可以在常数大小的字母表上获得达到容量的列表可译码码，其码长仅取决于与容量之间的差距 ϵ。一个重要的开放问题是：在与 ϵ 无关的固定大小字母表（例如二元字母表）上，构造达到容量的列表可译码码的显式构造，并设计高效的列表译码算法。在 q 元字母表上，列表译码容量已知为 $H_q^{-1}(1-R)$，其中

$$H_q(\alpha) = \alpha \log_q(q-1) + \alpha \log_q\left(\frac{1}{\alpha}\right) + (1-\alpha)\log_q\left(\frac{1}{1-\alpha}\right)$$

是 q元熵函数。

3. **实现列表译码容量的线性时间可编码、列表可译码码**。在第 6 节中，我们介绍了针对重数码的快速近线性时间列表译码算法，其译码能力可达容量。实现真正的线性时间列表译码算法（以及为达到容量的列表可译码码实现真正的线性时间编码算法）仍是一个开放问题。在唯一译码设定中，扩展码可用于构造线性时间可编码和可译码的码，因此，近期关于扩展码列表译码的研究 [ST25, JMST25] 或许可以用于构造这类码。

4. **在理论计算机科学中的应用**。我们在第 1 节提到，列表可译码码在理论计算机科学中有许多应用（第 1.4 节给出了一些参考文献）。若能探究本书综述的进展是否有助于这些应用，将会很有意义。

致谢。我们谨向 Zeyu Guo、Prahladh Harsha、Swastik Koppparty、Ramprasad Saptharishi、Shubhangi Saraf、Madhu Sudan、Amnon Ta-Shma、S. Venkitesh 和 Mary Wootters 致谢，感谢他们多年来围绕多项式码列表译码展开的诸多启发性讨论，这些讨论启发并影响了本综述的撰写。

Noga Ron-Zewi 在撰写本综述期间获得欧盟（ERC，ECCC，101076663）的部分资助。然而，文中表达的观点和意见仅代表作者本人，并不一定反映欧盟或欧洲研究委员会的观点和意见。欧盟和资助机构均不对此承担责任。

Mrinal Kumar 的工作由印度政府原子能部通过项目编号 RTI4014 提供资助，并部分获得 A NRF、Google Research 和 Premji Invest 的资助。

参考文献

[AEL95] Noga Alon、Jeff Edmonds 和 Michael Luby。具有近乎最优恢复能力的线性时间擦除码。载于第36届IEEE计算机科学基础年会（FOCS）论文集，第512–519页。IEEE计算机学会，1995年。[AGG+25] Omar Alrabiah、Zeyu Guo、Venkatesan Guruswami、Ray Li 和 Zihan Zhang。随机 Reed-Solomon 码以线性规模字母表达到列表译码容量。《组合学进展》，2025年。http://dx.doi.org/10.19086/aic.2025.8。[AHS26] Vikrant Ashvinkumar、Mursalin Habib 和 Shashank Srivastava。折叠 Reed-Solomon 码列表译码的算法改进。载于《2026年 ACM-SIAM 离散算法研讨会论文集》，SODA。SIAM，2026年。[AL96] Noga Alon 和 Michael Luby。具有近乎最优恢复能力的线性时间抗擦除码。《IEEE 信息论汇刊》，42(6):1732–1736，1996年。[Ale05] Michael Alekhnovich。多项式上的线性丢番图方程与 Reed-Solomon 码的软判决译码。《IEEE 信息论汇刊》，51(7):2257–2265，2005年。[AS03] Sanjeev Arora 和 Madhu Sudan。改进的低次测试及其应用。《组合学》，23(3):365–426，2003年。[BCDZ25] Joshua Brakensiek、Yeyuan Chen、Manik Dhar 和 Zihan Zhang。借助子空间设计从随机构造走向显式构造及其在局部性质和拟阵中的应用，2025年。[BDGZ25] Joshua Brakensiek、Manik Dhar、Sivakanth Gopi 和 Zihan Zhang。代数几何码在常数规模有限域上达到列表译码容量。《IEEE信息论汇刊》，71(8):5935–5956，2025年。[Ber68a] E. Berlekamp。非二元 BCH 译码（摘要）。《IEEE 信息论汇刊》，14(2):242–242，1968年。[Ber68b] Elwyn R. Berlekamp。代数编码理论。《系统科学丛书》。McGraw-Hill，1968年。[BF90] Donald Beaver 和 Joan Feigenbaum。在多预言机查询中隐藏实例。载于 Christian Choffrut 和 Thomas Lengauer 编，《STACS 90：第七届计算机科学理论方面年会论文集》，法国鲁昂，1990年2月22日至24日，第415卷《计算机科学讲义》，第37–48页。施普林格，1990年。[BFLS91] László Babai、Lance Fortnow、Leonid A. Levin 和 Mario Szegedy。在多对数时间内检查计算。载于第23届 ACM 计算理论年会（STOC）论文集，第21–31页。ACM出版社，1991年。[BFNW93] László Babai、Lance Fortnow、Noam Nisan 和 Avi Wigderson。除非 EXPTIME 存在可发表证明，否则 BPP 可由亚指数时间模拟。《计算复杂性》，3(4):307–318，1993年。[BGM22] Joshua Brakensiek、Sivakanth Gopi 和 Visu Makam。最大可恢复张量码和高阶 MDS 码的下界。《IEEE 信息论汇刊》，68(11):7125–7140，2022年。

[BGM25] Joshua Brakensiek、Sivakanth Gopi 与 Visu Makam。一般 Reed–Solomon 码达到列表译码容量。SIAM 计算杂志，第 STOC23–118–STOC23–154 页，2025。即将发表，https://doi.org/10.1137/23M1598064。[BHKS23] Siddharth Bhandari、Prahladh Harsha、Mrinal Kumar 与 Ashutosh Shankar。将重数 Schwartz-Zippel 引理算法化。载于 Nikhil Bansal 与 Viswanath Nagarajan 编，2023 年 ACM-SIAM 离散算法研讨会论文集，SODA 2023，意大利佛罗伦萨，2023年1月22日至25日，第2816–2835页。SIAM，2023。[BHKS24a] Siddharth Bhandari、Prahladh Harsha、Mrinal Kumar 与 Madhu Sudan。乘积集合上多变量重数码的译码。IEEE 信息论汇刊，70(1):154–169，2024。[BHKS24b] Siddharth Bhandari、Prahladh Harsha、Mrinal Kumar 与 Madhu Sudan。容量达成译码的理想论解释。IEEE信息论汇刊，70(2):1107–1123，2024。[BK95] Manuel Blum 与 Sampath Kannan。设计可检查自身工作的程序。ACM 杂志，42(1):269–291，1995年。[BK09] Kristian Brander 与 Swastik Koparty。大域上直至 Johnson 半径的里德-穆勒码列表译码。手稿，2009。[BKR10] Eli Ben-Sasson、Swastik Kopparty 与 Jaikumar Radhakrishnan。子空间多项式与里德-所罗门码列表译码的极限。IEEE信息论汇刊，56(1):113–120，2010。[BW87] E. R. Berlekamp 与 L. Welch。代数分组码的纠错。美国专利号 4,633,470，1987。[CX18] Chandra Chekuri 与 Chao Xu。超图中的最小割与稀疏化。SIAM计算杂志，47(6):2118–2156，2018。[CZ25] Yeyuan Chen 与 Zihan Zhang。显式折叠Reed-Solomon码与重数码达到放宽的广义 Singleton 界。载于 Michal Koucký 与 Nikhil Bansal 编，第 57 届 ACM 计算理论年度研讨会论文集，STOC 2025，捷克布拉格，2025年6月23日至27日，第1–12页。ACM，2025。[DKSS13] Zeev Dvir、Swastik Kopparty、Shubhangi Saraf 与 Madhu Sudan。重数法的扩展及其在 Kakeya 集与合并器中的应用。SIAM 计算杂志，42(6):2305–2328，2013。[DL78] Richard A. DeMillo 与 Richard J. Lipton。关于代数程序测试的一个概率性注记。Inf. Process. Lett.，7(4):193–195，1978。[DSY14] Son Hoang Dau、Wentu Song 与 Chau Yuen。关于小域上具有受约束生成矩阵的 MDS 码的存在性。载于 2014 年 IEEE 国际信息论研讨会，第1787–1791页，2014。https://doi.org/10.1109/ISIT.2014.6875141。[Eli57] Peter Elias。噪声信道的列表译码。麻省理工学院电子学研究实验室，技术报告 335，1957。

[FK08] 安德拉什·弗兰克与 Tamás Király。覆盖超模函数综述。载于 William J. Cook、拉斯洛·洛瓦斯与 Jens Vygen 编，组合优化研究趋势，波恩组合优化研讨会，2008年11月3日至7日，德国波恩，第87–126页。施普林格，2008。[FKK03a] 安德拉什·弗兰克、Tamás Király 与 Matthias Kriesell。关于将超图分解为 k 个连通子超图。Discret. Appl. Math.，131(2):373–383，2003。[FKK03b] 安德拉什·弗兰克、Tamás Király 与 Zoltán Király。关于图和超图的定向。离散应用数学，131(2):385–400，2003。[Fra11] 安德拉什·弗兰克。组合优化中的关联，第38卷。牛津大学出版社，2011。[GHKS24] Rohan Goyal、Prahladh Harsha、Mrinal Kumar 与 Ashutosh Shankar。单变量重数码与折叠 Reed-Solomon 码的快速列表译码。载于 Santosh Vempala 编，第65届 IEEE 计算机科学基础研讨会论文集（FOCS），2024。[GI02] Venkatesan Guruswami 与 Piotr Indyk。用于唯一译码的近最优线性时间码以及较小字母表上的新列表可译码码。载于第34届 ACM 计算理论年度研讨会（STOC）论文集，第812–821页。ACM出版社，2002。[GK16a] Alan Guo 与 Swastik Kopparty。提升码的列表解码算法。IEEE 信息论汇刊，62(5):2719–2725，2016。[GK16b] Venkatesan Guruswami 与 Swastik Kopparty。显式子空间设计。Combinatorica，36(2):161–185，2016。[GKO+18] Sivakanth Gopi、Swastik Kopparty、Rafael Oliveira、Noga Ron-Zewi 与 Shubhangi Saraf。逼近 Gilbert-Varshamov 界的局部可测试码与局部可纠错码。IEEE 信息论汇刊，64(8):5813–5831，2018。[GL89] Oded Goldreich 与 Leonid A Levin。适用于所有单向函数的硬核谓词。载于第21届 ACM 计算理论年度研讨会（STOC）论文集，第25–32页。ACM，1989。[GLR+91] Peter Gemmell、Richard J. Lipton、Ronitt Rubinfeld、Madhu Sudan 与 Avi Wigderson。多项式与近似函数的自测试/自纠正。载于 Cris Koutsougeras 与 Jeffrey Scott Vitter 编，第23届 ACM 计算理论年会论文集，1991年5月5日至8日，美国路易斯安那州新奥尔良，第32–42页。ACM，1991。[GLS+24] Zeyu Guo、Ray Li、Chong Shangguan、Itzhak Tamo 与 Mary Wootters。通过树打包改进里德-所罗门码的列表可译码性与列表恢复性。SIAM计算杂志，53(2):389–430，2024。[Gop83] V. D. Goppa。代数几何码。Math. USSR-Izv.，21:75–91，1983。[GR08] Venkatesan Guruswami 与 Atri Rudra。达到列表译码容量的显式码：具有最优冗余的纠错。IEEE 信息论汇刊，54(1):135–150，2008。

[GR22] Zeyu Guo 和 Noga Ron-Zewi。常数字母表和列表大小下的高效列表译码。IEEE信息论汇刊，68(3):1663–1682，2022。[GRS] Venkatesan Guruswami、Atri Rudra 和 Madhu Sudan。编码理论基础。https:// cse.buffalo.edu/faculty/atri/courses/coding-theory/book/。最后访问于：2025年8月。[GRS00] Oded Goldreich、Ronitt Rubinfeld 和 Madhu Sudan。通过查询学习多项式：高噪声情形。SIAM J. Discret. Math.，13(4):535–570，2000。[GS92] Peter Gemmell 和 Madhu Sudan。多项式的高鲁棒性校正器。Inf. Process. Lett.，43(4):169–174，1992。[GS99] Venkatesan Guruswami 和 Madhu Sudan。Reed-Solomon码和代数几何码的改进译码。IEEE 信息论汇刊，45(6):1757–1767，1999。[GST24] Eitan Goldberg、Chong Shangguan 和 Itzhak Tamo。列表译码和列表恢复的Singleton型界及相关结果。J. Comb. Theory A，203:105835，2024。[Gur04] Venkatesan Guruswami。纠错码的列表译码：2002年ACM博士论文竞赛获奖论文，第3282卷。Springer Science & Business Media，2004。[Gur06a] V. Guruswami。平均情形复杂度和伪随机性中的列表译码。载于：2006年IEEE信息论研讨会——ITW '06 Punta del Este，第32–36页，2006。[Gur06b] Venkatesan Guruswami。列表译码中的算法结果。Foundations and Trends in Theoretical Computer Science，2(2)，2006。[GW13] Venkatesan Guruswami 和 Carol Wang。Reed-Solomon码变体的线性代数列表译码。IEEE 信息论汇刊，59(6):3257–3268，2013。[GX22] Venkatesan Guruswami 和 Chaoping Xing。利用代数几何码在有界字母表上实现最优码率列表译码。ACM 杂志，69(2):10:1–10:48，2022。[GZ61] Daniel Gorenstein 和 Neal Zierler。以pm符号表示的一类纠错码。Journal of the Society for Industrial and Applied Mathematics，9(2):207–214，1961。[GZ23] Zeyu Guo 和 Zihan Zhang。随机打孔Reed-Solomon码在多项式规模字母表上达到列表译码容量。载于：第64届IEEE年度计算机科学基础研讨会（FOCS 2023），美国加利福尼亚州Santa Cruz，2023年11月6—9日，第164–176页。IEEE，2023。[Ham50] Richard Hamming。错误检测码和纠错码。Bell System Technical Journal，29(2):147–160，1950。[HRW20] Brett Hemenway、Noga Ron-Zewi 和 Mary Wootters。高码率张量码的局部列表恢复及其应用。SIAM 计算杂志，49(4):157–195，2020。[JMS03] Kamal Jain、Mohammad Mahdian 和 Mohammad R. Salavatipour。Steiner树打包。载于：第十四届ACM-SIAM离散算法年度研讨会论文集，2003年1月12—14日，美国马里兰州Baltimore，第266–274页。ACM/SIAM，2003。

[JMST25] Fernando Granha Jeronimo、Tushant Mittal、Shashank Srivastava 和 Madhur Tulsiani。利用扩张图构造逼近广义辛格尔顿界的显式码。CoRR，abs/2502.07308，2025。[Jos58] D. D. Joshi。关于最小距离码上界的注记。Inf. Control.，1(3):289–295，1958。[Kal85] Erich L. Kaltofen。从多元多项式因式分解到二元和一元整系数多项式因式分解的多项式时间归约。SIAM计算杂志，14(2):469–489，1985。[Kir03] Tamás Király。无向和有向超图的边连通性。博士论文，厄特沃什·罗兰大学，2003。[KK17] John Y. Kim 和 Swastik Kopparty。乘积集合上的里德-穆勒码译码。计算理论，13(21):1–38，2017。[KM93] Eyal Kushilevitz 和 Yishay Mansour。利用傅里叶谱学习决策树。SIAM 计算杂志，22(6):1331–1348，1993。[KMRS17] Swastik Kopparty、Or Meir、Noga Ron-Zewi 和 Shubhangi Saraf。具有次多项式查询复杂度的高码率局部可纠错码和局部可测试码。ACM杂志，64(2):11:1–11:42，2017。[Kop15] Swastik Kopparty。重数码的列表译码。计算理论，11(5):149–182，2015。[KRSW23] Swastik Kopparty、Noga Ron-Zewi、Shubhangi Saraf 和 Mary Wootters。折叠 Reed-Solomon码和重数码的改进列表译码。SIAM计算杂志，52(3):794–840，2023。[KSY14] Swastik Kopparty、Shubhangi Saraf 和 Sergey Yekhanin。具有亚线性时间译码的高码率码。ACM 杂志，61(5):28:1–28:20，2014。[KT00] Jonathan Katz 和 Luca Trevisan。关于纠错码局部译码过程的效率。载于：第32届ACM年度计算理论研讨会论文集（STOC），第80–86页。ACM出版社，2000。[Len85] Arjen K. Lenstra。有限域上的多元多项式因式分解。计算机与系统科学杂志，30(2):235–248，1985。（初步版本发表于第15届STOC，1983年。）[Lip90] Richard J. Lipton。计算验证的高效方法。载于：第7届ACM年度计算机科学理论方面研讨会（STACS）论文集，计算机科学讲义第415卷，第207–215页。施普林格，1990。[LMS25] Matan Levi、Jonathan Mosheiff 和 Nikhil Shagrithaya。随机 Reed-Solomon 码和随机线性码局部等价。载于：第66届IEEE年度计算机科学基础研讨会（FOCS）论文集。IEEE计算机学会，2025。[Lov21] Shachar Lovett。小域上的稀疏MDS矩阵：GM-MDS猜想的证明。SIAM 计算杂志，50(4):1248–1262，2021。https://doi.org/10.1137/ 20M1323345。

[Mas69] James L. Massey。移位寄存器综合与BCH译码。IEEE信息论汇刊，15(1):122–127，1969。[Men27] Karl Menger。关于一般曲线理论。Fundamenta Mathematicae，10(1):96–115，1927。[MRR+24] Jonathan Mosheiff、Nicolas Resch、Noga Ron-Zewi、Shashwat Silas 和 Mary Wootters。低密度奇偶校验码达到列表译码容量。SIAM计算杂志，53(6):S20–38，2024。[Mul54] David Muller。布尔代数在开关电路设计和错误检测中的应用。IRE电子计算专业组汇刊，3(3):6–12，1954。[Pet60] W. Wesley Peterson。Bose-Chaudhuri码的编码与纠错过程。IRE信息论汇刊，6(4):459–470，1960。[PW04] R. Pellikaan 和 Xin-Wen Wu。q元 Reed-Muller码的列表译码。IEEE 信息论汇刊，50(4):679–682，2004。[Ree54] Irving 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，4:38–49，1954。[Rot22] Ron M. Roth。高阶 MDS 码。IEEE信息论汇刊，68(12):7798–7816，2022。[RR00] Ron M. Roth 和 Gitit Ruckenstein。超越最小距离一半的 Reed-Solomon 码高效译码。IEEE信息论汇刊，46(1):246–257，2000。[RS60] Irving S. Reed 和 Gustave Solomon。某些有限域上的多项式码。工业与应用数学学会杂志，8(2):300–304，1960。https: //doi.org/10.1137/0108018。[RT97] Michael Rosenbloom 和 Michael Tsfasman。m度量码。Problemy Peredachi Informatsii，33(1):55–63，1997。[RV25] Nicolas Resch 和 S. Venkitesh。可列表恢复码：优者、劣者与未知者（但愿不是丑者）。arXiv预印本 2510.07597，2025。https://arxiv.org/abs/2510. 07597。[Sch80] Jacob T. Schwartz。用于多项式恒等式验证的快速概率算法。ACM 杂志，27(4):701–717，1980。[Sha48] Claude Shannon。通信的数学理论。Bell System Technical Journal，27:379—-423，623—-656，1948。[Sin64] Richard C. Singleton。最大距离 q元码。IEEE信息论汇刊，10(2):116– 118，1964。[ST20] Chong Shangguan 和 Itzhak Tamo。超越 Johnson 半径的 Reed-Solomon 码组合列表译码。载于 Konstantin Makarychev、Yury Makarychev、Madhur Tulsiani、Gautam Kamath 和 Julia Chuzhoy 编，《第52届年度 ACM SIGACT计算理论研讨会论文集》，STOC 2020，美国伊利诺伊州芝加哥，2020年6月22日至26日，第538–551页。ACM，2020。

[ST25] Shashank Srivastava 和 Madhur Tulsiani。近线性时间内将基于扩展子的码列表译码至容量。*CoRR*，abs/2504.20333，2025。[STV01] Madhu Sudan、Luca Trevisan 和 Salil Vadhan。不使用XOR引理的伪随机生成器。计算机与系统科学杂志，62(2):236–266，2001。[Sud97] Madhu Sudan。超越纠错界的 Reed-Solomon 码译码。复杂性杂志，13(1):180–193，1997。[Sud00] Madhu Sudan。列表译码：算法与应用。*SIGACT News*，31(1):16–27，2000年3月。[Sud25] Madhu Sudan。算法编码理论中的代数，2025。[Tam24] Itzhak Tamo。折叠Reed-Solomon码和重数码列表译码与恢复的更紧列表大小界。*IEEE*信息论汇刊，70(12):8659–8668，2024。[Tre04] Luca Trevisan。编码理论在计算复杂性中的若干应用。电子计算复杂性讨论会，TR04-043，2004。[Vad12] Salil P. Vadhan。伪随机性。理论计算机科学基础与趋势，7(1-3):1–336，2012。[vzGG13] Joachim von zur Gathen 和 Jürgen Gerhard。现代计算机代数。剑桥大学出版社，第3版，2013。[Woz57] John Wozencraft。列表译码。*MIT*电子实验室研究进展报告，48:90–95，1957。[Yek12] Sergey Yekhanin。局部可解码码。理论计算机科学基础与趋势，6(3):139–255，2012。[YH19] Hikmet Yildiz 和 Babak Hassibi。小域上具有支撑约束生成矩阵的最优线性码。*IEEE* 信息论汇刊，65(12):7868–7875，2019。https://doi.org/10.1109/TIT.2019.2932663。[Zip79] Richard Zippel。稀疏多项式的概率算法。载于 Edward W. Ng 编，符号与代数计算，*EUROSAM ’79，1979*年*6*月在法国马赛举行的国际符号与代数计算研讨会论文集，第72卷《计算机科学讲义》，第216–226页。施普林格，1979。