arXiv:2601.07137v1 [cs.CC] 12 Jan 2026

从有限域中根据含噪特征值恢复多项式

Swastik Kopparty*

摘要

设 $g(X)$ 是有限域 $\mathbb{F}_q$ 上的多项式，次数为 $o(q^{1/2})$，并设 χ 为二次剩余特征。给定 $\chi \circ g$ 在 $\mathbb{F}_q$上的取值，其中至多有恒定比例的取值存在错误，我们给出一种多项式时间算法，用于恢复 $g(X)$（忽略完全平方因子）。即便在没有错误的情况下，此问题此前也未得到解决。

对于特征为 2 的域上的多项式的加性特征，我们给出了类似的算法。这是首个能够从恒定比例的错误中解码多项式维数对偶 BCH 码的多项式时间算法。

我们的算法借鉴了 Stepanov 多项式方法证明经典特征和 Weil 界的思路，也借鉴了用于 Reed-Solomon 码的 Berlekamp-Welch 解码算法。我们称之为 *pseudopolynomials*的对象起着关键作用：高次多项式，其所有导数在 $\mathbb{F}_q$上都表现得像低次多项式。

这两个结果都可以看作这一情形下 Weil 界的算法版本。

1 引言

本文研究有限域上的一些含噪多项式插值问题的高效算法，其中关于每次求值只能获得少量信息。

设 q 为奇素数幂，并设 $\chi : \mathbb{F}_q \to \{0, \pm 1\}$ 为二次剩余特征（其在 0 上取值 0，在非零完全平方上取值 $+1$，在其他所有元素上取值 -1）。设 $g(X)$ 为一个次数至多为 $d \ll q$ 的未知多项式。我们考虑这样的问题：给定 $\chi \circ g$ 的含噪版本 $\mathbb{F}_q \to \{0, \pm 1\}$，计算 g。具体而言，给定 $r : \mathbb{F}_q \to \{0, \pm 1\}$，使得对于 $\alpha \in \mathbb{F}_q$ 中 99% 的元素，都有 $r(\alpha) = \chi(g(\alpha))$，我们能否高效地恢复 $g(X)$?

恢复 g 面临一个直接障碍：根据 r，它可能无法被唯一确定。这是因为 χ 无法检测 g 的完全平方因子。事实上，如果次数至多为 d 的 $g_1(X)$ $g_2(X)$ 满足：对于 $h(X) \in \mathbb{F}_q[X]$，有 $g_2(X) = g_1(X) \cdot h^2(X)$，那么每当 $h(\alpha) \neq 0$ 时：

$$\chi \circ g_2(\alpha) = (\chi \circ g_1(\alpha)) \cdot \left(\chi \circ h^2(\alpha)\right) = \chi \circ g_1(\alpha),$$

因此，汉明距离 $\Delta(\chi \circ g_1, \ \chi \circ g_2) \leq d \ll q$。

关于特征和的深刻而基本的韦伊界表明，这本质上是唯一的唯一性障碍。它指出，若 $f(X)$ 是次数至多为 d 的多项式，且不能写成 $\lambda \cdot h^2(X)$ 的形式，其中 $\lambda \in \mathbb{F}_q$ 且 $h(X) \in \mathbb{F}_q[X]$，那么：

$$\left| \sum_{\alpha \in \mathbb{F}_q} \chi(f(\alpha)) \right| \leq 2d\sqrt{q}.$$

*多伦多大学数学系和计算机科学系，加拿大。研究获得 NSERC探索基金资助。电子邮箱： swastik.kopparty@utoronto.ca

（换言之，如果 d 较小，随机的 $\alpha \in \mathbb{F}_q$ 满足 $f(\alpha)$为完全平方的概率约为$1/2$。）

因此，如果 $g_1(X)$ $g_2(X)$ $\in \mathbb{F}_q[X]$ 互不相同，且都是首一（首项系数为 1）、无平方因子（没有不可约因子的重数为 ≥ 2），次数至多为 $o(\sqrt{q})$ 的多项式，那么 $\chi \circ g_1$ 和 $\bar{}\chi \circ g_2$ 不仅互不相同，而且几乎正交：

$$|\langle \chi \circ g_1, \chi \circ g_2 \rangle| = \left| \sum_{\alpha \in \mathbb{F}_q} \chi(g_1(\alpha)) \cdot \chi(g_2(\alpha)) \right| = \left| \sum_{\alpha \in \mathbb{F}_q} \chi((g_1 \cdot g_2)(\alpha)) \right| \leq O(d\sqrt{q}) = o(q).$$

这意味着，当 g 遍历次数至多为 $d = o(\sqrt{q})$ 的首一无平方因子多项式时，向量 $\chi \circ g \in \{0, \pm 1\}^q$ 两两之间的汉明距离 $\Delta(\chi \circ g_1,\ \chi \circ g_2)$ 至少为 $\left(\frac{1}{2} - \Omega(\frac{d}{\sqrt{q}})\right) \cdot q$。这定义了一种纠错码，并使得给定 $\chi \circ g$ 的含噪版本来寻找 g 的问题，转化为对该纠错码进行唯一译码的问题。

我们给出一种多项式时间算法，在存在一定比例错误的情况下，从 $\chi \circ g$ 恢复此类 g。

定理 1

令 $\epsilon > 0$。令 $g(X) \in \mathbb{F}_q[X]$ 为首一无平方因子多项式，且 次数$(g) \leq \epsilon\sqrt{q}$。

假设 r： $\mathbb{F}_q \to \{0, \pm 1\}$ 满足：

$$\Delta(r, \chi \circ g) < \left(\frac{1}{8} - \epsilon\right) q.$$

存在一个 多项式(q)时间算法，该算法在输入 r 时计算出 $g(X)$。

如果 $g(X)$ 是次数为 $d \leq \epsilon\sqrt{q}$ 的一般首一多项式，并且 $\bar{r}$ 满足 $\Delta(r, \chi \circ g) < (\frac{1}{8} - \epsilon)q$，那么此算法将找出唯一的次数至多为 d 的首一无平方因子多项式 $\bar{g}(X)$，使得 $\Delta(\chi \circ g, \chi \circ \bar{g}) \leq d$。

即使在没有错误的情况下，此类算法此前也是未知的。此前已知的最快算法由 Russell 和 Shparlinski [RS04] 给出，运行时间为 $O(d^2 \cdot q^{d+o(1)})$。该算法将 Weil 界作为黑箱使用，并改进了平凡的 $O(q^{d+1})$ 时间暴力搜索。

在 [VDHI06], 中，van Dam、Hallgren 和 Ip 给出了高效的 量子 算法，可在 poly$(\log q)$ 时间内解决 $d = 1$ 情形，其时间复杂度低于输入规模。Russell 和 Shparlinski [RS04] 证明了一般 d情形可以通过 $O(d)$ 次量子查询求解，但据我们所知，这并不会导出快速的量子算法。 [BGKS12、IKS+18]给出了这一方向上的进一步结果。

我们还证明了特征 2 的域上加性特征的一个类似结果。这里的底层码是经典的对偶 BCH 码，即经典 BCH 码的对偶码 [BRC60、Hoc59]。

设 $q = 2^b$，并令 Tr： $\mathbb{F}_q \to \mathbb{F}_2$ 为 $\mathbb{F}_2$-线性域迹映射，定义为 $\mathrm{Tr}(\beta) = \sum_{i=0}^{b-1} \beta^{2^i}$。 $\mathbb{F}_q$ 上的加性特征 ψ 与 Tr 密切相关（它们具有如下形式： $\psi(\beta) = (-1)^{\mathrm{Tr}(a \cdot \beta)}$）；为方便记号，我们用 Tr 而非 ψ来表述问题。

令 $g(X) \in \mathbb{F}_q[X]$ 为一个次数至多为 d的未知多项式。假设对于每个 $\alpha \in \mathbb{F}_q$，我们都得到一个值 $r(\alpha)$，使得 对于 99% 的 $\alpha \in \mathbb{F}_q$， $r(\alpha) = \mathrm{Tr}(g(\alpha))$。我们能高效地恢复 $g(X)$吗?

同样，一个直接的障碍来自这样一个事实： r（甚至 Tr $\circ g$）无法唯一确定$g(X)$。这是因为迹无法区分多项式及其平方。事实上，若 $g_1(X)$ $g_2(X)$ 满足 $g_2(X) = g_1(X) + h(X) + h^2(X)$，其中某个 $h(X) \in \mathbb{F}_q[X]$，那么[1] 对所有 $\alpha \in \mathbb{F}_q$ 都成立：

$$\mathrm{Tr} \circ g_2(\alpha) = (\mathrm{Tr} \circ g_1(\alpha)) + \left(\mathrm{Tr} \circ (h + h^2)(\alpha)\right) = \mathrm{Tr} \circ g_1(\alpha),$$

[1]这是因为对所有 $\beta \in \mathbb{F}_q$， $\mathrm{Tr}(\beta + \beta^2) = 0$。

因此 $\mathsf{Tr} \circ g_1 = \mathsf{Tr} \circ g_2$。

加性特征和的 Weil 界告诉我们，这是唯一妨碍唯一性的因素。它指出，若 $f(X) \in \mathbb{F}_q[X]$ 的次数至多为 d，且不能写成 $\lambda + h(X) + h(X)^2$ 的形式，其中 $\lambda \in \mathbb{F}_q$ 且 $h(X) \in \mathbb{F}_q[X]$，那么：

$$\left| \sum_{\alpha \in \mathbb{F}_q} (-1)^{\mathsf{Tr}(f(\alpha))} \right| \leq (d-1)\sqrt{q}.$$

（换句话说，如果 d 很小，那么随机的 $\alpha \in \mathbb{F}_q$ 使 $\mathsf{Tr}(f(\alpha))$ 等于 0 和 1 的概率大致相同。）

因此，若 $g_1(X)$ $g_2(X) \in \mathbb{F}_q[X]$ 是次数为奇数的单项式组成的不同多项式，且次数为$d = o(\sqrt{q})$，那么 $\mathsf{Tr} \circ g_1$ 和 $\overline{\mathsf{Tr}} \circ g_2$ 不仅彼此不同，而且几乎像随机向量一样相距甚远：

$$\left| \sum_{\alpha \in \mathbb{F}_q} (-1)^{\mathsf{Tr}(g_1(\alpha) - g_2(\alpha))} \right| = \left| \sum_{\alpha \in \mathbb{F}_q} (-1)^{\mathsf{Tr}((g_1 - g_2)(\alpha))} \right| \leq O(d\sqrt{q}) = o(q),$$

因此：

$$\Delta(\mathsf{Tr} \circ g_1, \mathsf{Tr} \circ g_2) \in \left(\frac{1}{2} \pm O\left(\frac{d}{\sqrt{q}}\right) \right) \cdot q.$$

由此可得对偶 BCH 码的定义。对于奇整数 d，码字由次数至多为 d 且只含奇数次单项式的多项式$g(X)$索引：

$$g(X) = a_1 X + a_3 X^3 + \ldots + a_d X^d,$$

而码字本身就是函数 $\mathsf{Tr} \circ g : \mathbb{F}_q \to \mathbb{F}_2$。这是一个定义在 $\mathbb{F}_2$ 上的线性码，长度为 q，维数为 $\mathbb{F}_2 \log_2 q$。因此，给定 $\mathsf{Tr} \circ g$ 的含噪版本来寻找 g，就是对这个对偶 BCH 码进行唯一译码的问题。

我们给出一种多项式时间算法，在存在一定比例错误的情况下，从 $\mathsf{Tr} \circ g$ 中恢复 g。

定理 2

设 $\epsilon > 0$。设 $g(X) \in \mathbb{F}_q[X]$ 是一个只含奇数次单项式的多项式，且 $\deg(g) \leq \epsilon\sqrt{q}$。假设 $r : \mathbb{F}_q \to \mathbb{F}_2$ 满足：

$$\Delta(r, \mathsf{Tr} \circ g) < \left(\frac{1}{8} - \epsilon \right) q.$$

存在一个 $\mathrm{poly}(q)$ 时间算法，在输入 r 时，计算出 $g(X)$。

若 $g(X)$ 是一个次数为 $d \leq \epsilon\sqrt{q}$ 且常数项为 0 的一般多项式，并且 r 满足 $\Delta(r, \mathsf{Tr} \circ g) < (\frac{1}{8} - \epsilon)q$，那么该算法将找到唯一的多项式 $\bar{g}(X)$，其次数至多为 d，且只含奇数次单项式，使得 $\mathsf{Tr} \circ g = \mathsf{Tr} \circ \bar{g}$。

针对这个问题（即对偶 BCH 码译码问题），此前已有若干已知结果。

- 对于所有 $d < O(\sqrt{q})$，如果完全没有错误，那么可以在 $\mathrm{poly}(q)$ 时间内找到 $g(X)$。这是因为映射 $g(X) \mapsto \mathsf{Tr} \circ g$ 是 $\mathbb{F}_2$-线性的；因此可以通过求解关于 $\mathbb{F}_2$ 的线性方程组，从 $\mathsf{Tr} \circ g$ 中找到 $g(X)$。

- 对于所有 $d < O(\sqrt{q})$，如果错误数量至多为 $O(\frac{q}{d})$，那么就存在一个 $\mathrm{poly}(q)$ 时间算法来恢复 $g(X)$。这是高效译码 Reed–Muller码（$\mathbb{F}_2^b$上的多元多项式码）算法的推论。关键事实是，当通过一个 $\mathbb{F}_2$-线性同构将 $\mathbb{F}_q$ 视为 $\mathbb{F}_2^b$ 时，函数 $\mathsf{Tr} \circ g$ 是一个 b元 $\mathbb{F}_2$多项式，其次数至多为 $\lceil \log_2 d \rceil$。

• 对于较小的 d，Kaufman-Litsyn [KL05], 、Kaufman-Sudan [KS07] 以及 Kopparty-Saraf [KS10]的工作给出了亚线性时间算法，可以从固定比例的错误中译码对偶 BCH 码。这些算法的运行时间为 $O(d^d \cdot \text{poly}(\log q))$。对于 $d = O(\log q \log\log q)$，其运行时间为 poly(q)；而对于稍小的 d，其运行时间为 $q^{o(1)}$。

这些算法利用了一个事实：码字各坐标之间存在许多短的线性依赖；也就是说，它们的对偶码中有许多低重量码字。有趣的是，它们将 BCH 码的译码算法用作子程序。

定理 2 给出了首个在 $\text{poly}(q)$ 时间内从恒定比例错误中解码的算法，适用于 $d > \omega(\log q \log\log q)$。

我们的结果可以看作是特征和的 Weil 型界的算法版本。据我们所知，唯一已知的证明表明，定理 1（对于 $d \geq 3$）和定理 2（对于 $d \geq \Omega(\log q)$）所对应的纠错码具有 $\Omega(q)$ 的距离，而该证明依赖于 Weil 界。任何能够从 $\Omega(q)$ 个错误中解码这些码的算法，都必须使用 Weil 型界，或证明一个 Weil 型界。我们的结果属于后一类。

我们借鉴了 Stepanov 多项式方法中证明 Weil 界的思路，也借鉴了用于 Reed-Solomon 码的 Berlekamp-Welch 译码算法。我们称为伪多项式的对象发挥了关键作用：它们是高次多项式，其所有导数在 $\mathbb{F}_q$ 上都表现得像低次多项式。

这些算法能够处理的错误数量达不到这些码的唯一译码半径，该半径约为 $\left(\frac{1}{4} - \epsilon\right) q$。如何针对如此多的错误实现高效译码，将是一个有趣的问题。

1.1 相关工作

Weil [Wei41, Wei48, Wei49] 证明了特征和的 Weil 界，这是他证明有限域上曲线的黎曼假设的一个推论。这些界以非常精确的定量形式，揭示了有限域中一些非常基本的伪随机性现象。因此，它们在伪随机对象的显式构造中得到了广泛应用。我们列举理论计算机科学中的一些重要应用：Graham 和 Spencer [GS71], 证明了 Paley 图的普适性；Alon、Goldreich、Håstad 和 Peralta [AGHP92], 构造了 ε-偏置集合；Gabizon 和 Raz [GR08]构造了仿射提取器。

另一个非凡的应用是上文提到的对偶 BCH 码。对偶 BCH 码是长度为 q 的 $\mathbb{F}_2$ 线性码，具有 $q^{(d+1)/2}$ 个码字，且最小距离至少为 $\left(\frac{1}{2} - \frac{d-1}{\sqrt{q}}\right) \cdot q$。对于较小的 d，这些是无匹配码：如果没有 Weil 界，对于所有常数 t，目前尚无已知证明能够证明存在长度为 n、具有 n^t 个码字且最小距离为 $\left(\frac{1}{2} - O_t\left(\frac{1}{\sqrt{n}}\right)\right) \cdot n$ 的二元码。（利用在奇特征域上的无平方因子多项式所对应的二次剩余特征，也可以构造出具有类似强参数的非线性二元码；只需将少量的 0 坐标任意替换为 $+1$ 或 -1 即可。）这还可以得到 n^t 个位于 $\mathbb{R}^n$ 中的单位向量，其两两内积均至多为 $O(t/\sqrt{n})$。这比随机向量所能达到的最大内积上界还要小，后者为 $O(\sqrt{(\log n)/n})$。

Weil 界的原始证明用到了代数几何中的工具。多年后，Stepanov [Ste69, Ste70, Ste74]发现了 Weil 型界的一个初等证明。该证明巧妙地运用了如今称为多项式方法（带重数）的思想：先通过插值构造一个在所关注集合上消失（且具有高重数）的多项式，再研究该多项式。此后，Schmidt [Sch76], Bombieri [Bom73] 和 Stohr-Voloch [SV86]大大改进、简化并推广了 Stepanov 方法。 [Sch76, HKT08, LN97] 提供了这一主题及相关课题的精彩入门介绍。我们的算法深受 Stepanov 方法思想的影响。

近年来，为了应用于理论计算机科学和编码理论，人们发展出了多种针对特征和的韦伊界的扩展，参见 [Kop11, KL11, CGS16, KTSY24, CDGM25] 和

[Kop10，第 6] 章。

本文所研究的问题属于含噪多项式插值问题。这是编码理论和理论计算机科学中一个历史悠久且研究充分的课题。我们的算法也深受该领域中多项式方法（带重数）技术的影响，尤其是 Reed-Solomon 码的经典 Berlekamp-Welch 和 Guruswami-Sudan 译码算法所采用的“插值 + 代数”框架 [BW86, Sud96, GS99]。

Guruswami-Sudan 算法能够解决一种非常一般的多项式重构问题，它恰好概括了从特征值恢复多项式的问题。现在我们来描述这个问题，它称为 Reed-Solomon 码的列表恢复问题。在 Reed-Solomon 码的列表恢复问题中，对于每个 $\alpha \in \mathbb{F}_q$，给定一个大小至多为 ℓ 的集合 S_α，我们希望找出所有次数至多为 d 的多项式 $f(X) \in \mathbb{F}_q[X]$，使得

$$|\{\alpha \in \mathbb{F}_q \mid f(\alpha) \in S_\alpha\}| \geq 0.99q.$$

Guruswami-Sudan 算法 [GS99] 能在时间 poly(q) 内高效找出所有这样的 $f(X)$，前提是 $\ell < (0.99)^2 \frac{q}{d}$ –（并且特别地，这证明了这样的 $f(X)$ 的数量至多为 poly(q)）。当给定 $r: \mathbb{F}_q \to \{0, \pm 1\}$，且对于某个低次数的 $g(X)$，有 $\Delta(\chi \circ g,\ r) \leq 0.01q$ 时，寻找 $g(X)$ 的问题可转化为如下列表恢复问题。对于每个 $\alpha \in \mathbb{F}_q$，令 $S_\alpha = \chi^{-1}(r(\alpha))$。那么，所有次数至多为 d 且满足以下条件的 $f(X)$ 的集合

$$|\{\alpha \in \mathbb{F}_q \mid f(\alpha) \in S_\alpha\}| \geq 0.99q,$$

包含 $g(X)$（事实上，所有此类 $f(X)$ 都具有 $\lambda \cdot g(X) \cdot h^2(X)$ 的形式）。因此，恢复g 的问题是一种特殊的列表恢复问题。

在这种情况下，$|S_\alpha| \leq \ell = (q-1)/2$，且 $d = \omega(1)$，因此我们所处的范围并不适用于 Guruswami-Sudan 算法。我们的结果可以看作利用 S_α的额外代数结构，从而实现某种列表恢复的方法。

我们的算法利用了关于待插值多项式的高阶导数信息。从这个意义上说，它们与近期蓬勃发展的重数码译码算法研究方向一脉相承 [RT97, Nie01, KSY14, GW13, Kop14, Kop15, KRZSW23, BHKS23, Tam24, BHKS24, GHKS24, CZ25, Sri25, GHK+25, AHS25]（重数码是基于多项式及其导数的求值构造的纠错码）。

对偶 BCH 码 C，其 $d = \Theta(q^{0.1})$ 是一种二元码，具有：(1) 码长 n，(2) 维数 $k = \Omega(n^{0.1} \log n)$，(3) 距离 $\left(\frac{1}{2} - o(1)\right) n$，以及 (4) 对偶距离（即 $C^\perp$ 的距离）$\Omega(n^{0.1})$。定理 2 表明，它还具有：(5) 可高效地解码 $\Omega(n)$ 个错误。

直到最近，人们才构造出具有距离 $\frac{n}{2} - o(1)$、对偶距离 $n^{\Omega(1)}$，且能够高效地解码 $\Omega(n)$ 比例错误的显式二元码。首批此类码由 Kopparty、Shaltiel 和 Silbak [KSS19] 构造。这些码称为原始 *Reed-Solomon* 码，与对偶 BCH 码密切相关；其码字由相关的对偶 BCH 码字拼接而成，而其最小距离则通过引用相同的 Weil 界得到证明。这些码的高效解码算法基于对前文提到的 Guruswami-Sudan 算法作适当实例化，实际上能够对 $(\frac{1}{2} - o(1))n$ 错误进行列表译码。

如果我们将码的距离要求放宽为仅需达到 $\Omega(n)$，那么甚至可以利用代数几何码实现对偶距离 $\Omega(n)$；这是 Ashikhmin、Litsyn 和 Tsfasman 的一项重要成果 [ALT01]，他们是在量子码的背景下发现这一结果的（另请参见 Guruswami 的附录，载于 [Shp09]）。

1.2 技术

设 q 为奇数。设 $g(X)$ 是一个次数为 $d = q^{0.1}$ 的首一无平方因子多项式。首先描述在给定无错误的 $\chi \circ g$ 时恢复 g 的算法。

设 $\widetilde{G}(X) = (g(X))^{(q-1)/2}$。那么，对于每个 $\alpha \in \mathbb{F}_q$，[2] $\chi \circ g(\alpha) = \widetilde{G}(\alpha)$。因此，我们的输入给出了多项式 $G(X)$ 的 q 个取值。然而， $G(X)$ 的次数 $\approx d\frac{q}{2}$ 高得多，仅凭次数考虑，还不足以插值得到 G。

为了说明该算法的动机，我们先指出关于 $\widetilde{G}(X)$ 的导数[3] 有一个引人注目的性质。我们来计算：

$$\widetilde{G}'(X) = \frac{q-1}{2} \cdot g(X)^{(q-3)/2} \cdot g'(X) = -\frac{1}{2} \cdot \frac{g'(X)}{g(X)} \cdot \widetilde{G}(X).$$

因此，对所有 $\alpha \in \mathbb{F}_q$，都有：

$$\widetilde{G}'(\alpha) = -\frac{1}{2} \cdot \frac{g'(\alpha)}{g(\alpha)} \cdot (\chi \circ g(\alpha)).$$

设 S_0, S_1, S_{-1} 分别是 $\mathbb{F}_q$ 中 G 取值为 $0, 1, -1$ 的子集。我们知道 S_0 很小，而 S_1, S_{-1} 的大小都约为 $\frac{q}{2}$（由 Weil 界可知）。上述计算表明，存在一个次数很低的有理函数 $h(X) = -\frac{1}{2}g'(X)/g(X)$，使得高次数多项式 $\tilde{G}'$ 在 S_1 上与 h 相等，在 S_{-1} 上与 $-h$ 相等。这是一种非常特殊的行为：高次数多项式不仅在较大的集合 S_1 和 S_{-1} 上变成了低次数有理函数，而且这两个有理函数本身也密切相关。这种现象在更高阶导数中也会继续出现。我们的算法将以此为基础。

首先做一些小的调整。为避免出现分母，我们选取一个整数 $M = O(d)$，并定义 $G(X) = (g(X))^{(q-1)/2+M}$。我们将使用 Hasse 导数，而非标准导数，因为它在有限域上效果更好。令 $G^{[\ell]}(X)$ 表示 $G(X)$ 的第 ℓ 阶（Hasse）导数。那么有如下事实：对于每个满足 $0 \le \ell < M$ 的 ℓ，都存在一个次数至多为 $O(dM) \ll q$ 的多项式 $V_\ell(X)$，使得：

$$G^{[\ell]}(\alpha) = (\chi \circ g(\alpha)) \cdot V_\ell(\alpha) \tag{1}$$

对所有 $\alpha \in \mathbb{F}_q$ 均成立。

这给出了算法的第一步：通过求解线性方程组，我们寻找一个次数至多为 $d \cdot ((q-1)/2 + M)$ 的多项式$F(X)$，以及次数至多为$O(dM)$ 的多项式 $U_0(X)$ $U_1(X) \ldots, U_{M-1}(X)$，使得对所有 $\alpha \in \mathbb{F}_q$， $F^{[\ell]}(\alpha) = (\chi \circ g(\alpha)) \cdot U_\ell(\alpha)$。

我们知道这些方程有解，因为 G 和 V_ℓ 满足这些方程。但算法找到的任意解 F 和U_ℓ 可能并不等于 G 和 V_ℓ。这种情况确实可能发生：如果 $h_1(X)$和 $h_2(X)$是次数都很低的多项式，而 $f(X)$的形式为 $g(X) \cdot h_2(X)^2$,，那么令 $F(X)$为 $h_1(X) \cdot (f(X))^{(q-1)/2+M}$同样可以得到这些方程的一个有效解。

算法的下一步是通过分解 $F(X)$ 并检查 $F(X)$ 的因子重数，从 $F(X)$ 中恢复出 $g(X)$。设 $g(X) = \prod_i g_i(X)$ 是将 $g(X)$ 分解为互异不可约因子所得的分解。我们证明， $g_i(X)$ 的集合恰好是 $F(X)$ 的所有不可约因子中，在模 q 约化后其因子重数近似为 $q/2$ 的那些因子所组成的集合。如果 $F(X) = G(X)$，这一点显然成立。证明由算法第一步找到的任意$F(X)$都满足这一点，是分析的主要步骤。

对此的证明相当间接。首先，借助多项式插值论证，我们证明存在特殊的多项式 $A(X)$ $B(X) \in \mathbb{F}_q[X]$ 使得：

$$A(X) \cdot F(X) = B(X) \cdot G(X). \tag{2}$$

这些特殊多项式就是我们所称的 伪多项式。它们的形式为 $C(X) = \sum_i C_i(X)(X^q - X)^i$，其中 $C_i(X)$ 的次数较低 k（远低于 q）。选择这类多项式以及插值论证的思路都源自 Stepanov 方法。伪多项式有两个我们会用到的关键性质：

[2]现在我们将特征标 χ 视为取值于 $\mathbb{F}_q$ 的函数。[3]这就是多项式的标准导数，定义为 $(X^i)' = iX^{i-1}$，并通过线性性延拓。

- 对于每个 ℓ，都存在一个次数至多为 k 的多项式 $C_{\langle \ell \rangle}(X)$，使得 ℓ 阶导数 $C^{[\ell]}$ 与 $C_{\langle \ell \rangle}$ 在 $\mathbb{F}_q$ 的所有点上相等。我们在插值论证中利用这一点来得到恒等式 (2)。
- $C(X)$ 的每个不可约因子的因子重数都近似为 q 的倍数。根据 (2)，这确保了 F 中重数近似为 $q/2 \mod q$ 的因子，只有那些 G 中重数近似为 $q/2 \mod q$ 的因子，正如我们所希望的那样。

至此，便完成了无错误情形下证明的概要。

为处理错误，我们借鉴 Reed-Solomon 码的 Berlekamp-Welch 解码算法的思路。不过，我们不能使用错误定位多项式将错误归零，而必须使用高重数错误定位伪多项式 $E(X)$。这样便能确保 $E(X)\cdot G(X)$ 的导数也具有类似于方程 (1) 中给出的 $G(X)$ 的性质。

对于加性特征标情形，算法会稍微复杂一些。为了根据 $\mathrm{Tr} \circ g$ 的含噪版本 r 恢复 g，我们建立一个线性方程组，以捕捉多项式 $G(X) = \sum_{i=0}^{b-1} g^{2^i}(X)$ 的导数所具有的某种特殊低次数性质。具体来说，我们要寻找非零多项式 $F(X)$ 和 $E(X)$，其中 $E(X)$ 是一个伪多项式，使得存在低次多项式 $U_0(X), \ldots, U_{M-1}(X)$，满足：

$$F^{[\ell]}(\alpha) = E^{[\ell]}(\alpha) \cdot r(\alpha) + U_\ell(\alpha)$$

对所有 $\alpha \in \mathbb{F}_q$。如果 $E(X)$ 是一个高重数错误定位伪多项式，且 $F(X) = E(X) \cdot G(X)$，那么上述方程都成立。然而，算法找到的解未必是这个解。

从这个方程组的解出发，我们尝试恢复 $g(X)$；然而，不同于二次剩余特征的情形（相关问题是多项式因式分解，而且已有现成的算法），我们还得多费些功夫。这里，我们只能利用方程组的解提取 $g(X)$ 的最高次项系数。随后，我们可以将其剥离并重复这一过程，从而得到完整的 $g(X)$。分析再次用到了涉及伪多项式的插值论证。

我们从头开始介绍第3节和第4节中的算法及其分析，并未明确使用伪多项式这一术语。稍后，在第5节中，我们将正式定义伪多项式和伪次数，陈述一些基本性质，并在更清晰的背景下解释前几节中的一些想法。我们还将用这一语言表述 Stepanov 对 Weil 界的证明。

在附录中，我们简要说明这些算法如何推广到有限域上的 m次幂剩余特征标和小特征下的加性特征。

1.3 问题

下面我们重点介绍一些有趣的问题。

1. 是否存在一种高效算法，能够纠正这些码中比例为 $(\frac{1}{4} - \epsilon)$ 的错误？这是这些码的唯一译码半径。2. 更进一步，我们可以问，是否存在一种高效算法，能够对这些码进行列表解码，纠正比例为 $\left(\frac{1}{2} - O(\sqrt{\epsilon})\right)$ 的错误？这是这些码的（二元）Johnson 半径，因此我们知道，对于任意给定的函数，在此半径内的码字只有 $O_\epsilon(1)$ 个 r。在某些方面，我们的结果类似于用于 Reed-Solomon 码的 Berlekamp-Welch 算法解码算法。在这一背景下，是否存在 Guruswami-Sudan 算法的对应算法？3. 我们给出算法解决的这两个解码问题，都是以下更一般问题的实例。设 $G(X, Y) \in \mathbb{F}_q[X, Y]$ 是一个次数为 d 的未知多项式。假设输入为其投影 $S = \Pi_X(G)$，其中：

$$\Pi_X(G) = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \text{ with } G(x, y) = 0\}.$$

我们能否在 poly(q) 时间内找到某个次数至多为 d 的多项式 $F(X,Y)$，使得 $|\Pi_X(F)\triangle S| \leq O_d(1)$?

这类集合是 Chatzidakis、van den Dries 和 Macintyre [CVDDM92] 以及陶哲轩 [Tao14, Tao13]意义下复杂度为 $O_d(1)$ 的可定义集。基于更一般形式的 Weil 界，[CVDDM92], 的结果表明，任意两个这类可定义集的对称差大小要么为 $O_d(1)$，要么为 $\Omega_d(q)$。这表明，甚至可以希望仅凭 $\Pi_X(G)$ 的含噪版本来解决这个问题。

4. 令 q为素数，并令 $H \subset \mathbb{F}_q$为集合 $\{0,1,\ldots,(q-1)/2\}$，且令 $1_H\colon \mathbb{F}_q \to \{0,1\}$ 为其示性函数。设 $g(X)$ 是 $\mathbb{F}_q[X]$ 中的一个次数至多为 d的未知多项式，并且已知 $(1_H)\circ g\colon \mathbb{F}_q \to \{0,1\}$ 的所有取值。

加性特征和的 Weil 界表明，对于 $\mathbb{F}_q$，如果 $d < O(q^{\frac{1}{2}-\epsilon})$，那么函数 $1_{\bar{H}} \circ g$ 唯一确定 $g(X)$，但不包括常数项。

我们能否在 poly(q) 时间内求出 $g(X)$（不包括常数项）？

据我们所知，上述唯一性结论唯一的初等证明都非常迂回，涉及在多个扩域 $\mathbb{F}_{q^c}$ 中使用 Stepanov 方法。若能找到更直接的证明，并将其用于上述算法问题，将会非常有趣。

致谢

我要感谢 Ronen Shaltiel 和 Divesh Aggarwal，他们曾分别向我询问如何高效译码对偶 BCH 码。

多年来，我非常感谢 Divesh Aggarwal、Mitali Bafna、Eli Ben-Sasson、Ariel Gabizon、Mrinal Kumar、Shub- hangi Saraf、Ronen Shaltiel、Madhu Sudan、Amnon Ta-Shma、Santoshini Velusamy、Avi Wigderson 和 Kedem Yakirevitch 就这些主题展开的宝贵讨论。我尤其要感谢 Amnon Ta-Shma，感谢他围绕 Stepanov 方法进行的许多启发性讨论。

2 预备知识

$\mathbb{F}_q^*$ 表示 $\mathbb{F}_q \setminus \{0\}$。

对于两个函数 r_1，$r_2\colon \mathbb{F}_q \to \mathbb{F}_q$，我们将它们的汉明距离定义为取值不同的点的数量：

$$\Delta(r_1,r_2) = |\{\alpha \in \mathbb{F}_q \mid r_1(\alpha) \neq r_2(\alpha)\}|.$$

我们用 poly(n) 表示一个由绝对常数 A，B界定的 $A \cdot n^B$ 表达式。

2.1 多项式、Hasse 导数与重数

设 $\mathbb{F}$ 是一个域。

我们用 deg(A) 表示多项式 $A(X) \in \mathbb{F}[X]$ 的次数。对于多项式 $A(X)$ $B(X) \in \mathbb{F}[X]$，我们将使用 $A(X)$ mod $B(X)$ 表示 $A(X)$ 除以 $B(X)$ 所得的余式。

现在我们定义 Hasse 导数，这是一种适用于有限域上多项式的高阶导数概念。有关更多信息，请参见 [HKT08、DKSS13]。

定义 2.1 (Hasse 导数)。对于多项式 $A(X) \in \mathbb{F}[X]$，我们将$A(X)$的 ℓ 阶 ***Hasse*** 导数记作 $A^{[\ell]}(X)$，定义为展开式中 Z^ℓ 的系数 $A_\ell(X) \in \mathbb{F}[X]$：

$$A(X+Z) = A_0(X) + A_1(X)Z + \ldots + A_\ell(X)Z^\ell + \ldots.$$

定义 2.2 (重数)。 对于非零多项式 $A(X) \in \mathbb{F}[X]$ 和 $\alpha \in \mathbb{F}$，我们将 $A(X)$的消失重数记作 $\mathsf{mult}(A, \alpha)$，它是满足 $(X-\alpha)^r$ 整除 $A(X)$的最大 $r \in \mathbb{N}$。

等价地，它是满足对所有 ℓ，若 $0 \le \ell < r$，

$$A^{[\ell]}(\alpha) = 0,$$

且 $A^{[r]}(\alpha) \neq 0$ 的最大 $A^{[r]}$。

引理 2.3 （Hasse 导数法则）。设 $A(X)$ $B(X) \in \mathbb{F}[X]$，且 α，$\beta \in \mathbb{F}$。那么对所有 $\ell \ge 0$:

- $$(\alpha A + \beta B)^{[\ell]}(X) = \alpha A^{[\ell]}(X) + \beta B^{[\ell]}(X).$$
- $$(A \cdot B)^{[\ell]}(X) = \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1,\ell_2 \ge 0}} A^{[\ell_1]}(X) \cdot B^{[\ell_2]}(X).$$

现在我们将讨论特例：有限域 $\mathbb{F}_q$。这里，多项式

$$\Lambda(X) = X^q - X$$

起着特殊作用。

我们回顾一些基本的导数计算。

对于 $A(X) = X^i$:

$$A^{[\ell]}(X) = \binom{i}{\ell} X^{i-\ell}.$$

对于 $\Lambda(X)$:

$$\Lambda^{[\ell]}(X) = \begin{cases} \Lambda(X) & \ell = 0 \\ -1 & \ell = 1 \\ 1 & \ell = q \\ 0 & \text{otherwise} \end{cases}.$$

引理 2.4. 假设 $U(X)$ $V(X) \in \mathbb{F}_q[X]$, 次数$(V) < q$, $i \ge 0$，并且:

$$U(X) = V(X) \cdot \Lambda^i(X),$$

那么对于 $0 \le \ell < q$:

$$U^{[\ell]}(X) \equiv (-1)^i \cdot V^{[\ell-i]}(X) \mod \Lambda(X),$$

（其中我们采用约定：若 $j < 0$，则 $V^{[j]}(X) = 0$。）

证明. 根据 Hasse 导数的乘积法则:

$$U^{[\ell]}(X) = \sum_{\substack{\ell_0,\ell_1,\ldots,\ell_i \\ \sum \ell_j = \ell}} V^{[\ell_0]}(X) \cdot \prod_{j=1}^{i} \Lambda^{[\ell_j]}(X).$$

若 $\ell < i$，则在该和式的每一项中，ℓ_1、.....、ℓ_i 中必有一个等于 0，因此所有项都是 $\Lambda(X)$ 的倍数。所以，正如所要证明的，$U^{[\ell]}(X)$ 是 $\Lambda(X)$ 的倍数。

若 $\ell \geq i$，那么我们将看到，这些项中至多有一项不是 $\Lambda(X)$ 的倍数。

由于 $\ell < q$，每一项都具有全部的 $\ell_j < q$。

根据我们对 Λ 的导数的计算，非零的项必须满足 $\ell_1, \ldots, \ell_i$ 全部等于 0 或 1。

如果 $\ell_1, \ldots, \ell_i$ 中至少有一个等于 0，那么 $\Lambda(X)$ 就是该项的一个因子。

剩下的唯一一项是 $\ell_1 = \ell_2 = \ldots = \ell_i = 1$ 和 $\ell_0 = \ell - i$，这一项等于：

$$V^{[\ell-i]}(X) \cdot (-1)^i.$$

至此，引理得证。 □

2.2 奇特征域上的二次剩余特征

设 q 为奇素数幂。

设 $\chi : \mathbb{F}_q \to \{0, \pm 1\}$ 为二次剩余特征：

$$\chi(\beta) = \begin{cases} +1 & \beta \in \mathbb{F}_q^* \text{ is the square of an element of } \mathbb{F}_q \\ -1 & \beta \text{ is not the square of an element of } \mathbb{F}_q \\ 0 & \beta = 0. \end{cases}$$

通常将值域视为 $\mathbb{C}$ 的子集，但我们将其视为 $\mathbb{F}_q$ 的子集。于是有公式：

$$\chi(\beta) = \beta^{(q-1)/2}.$$

设 $g(X) \in \mathbb{F}_q[X]$，其中 g 的次数为 d。我们用 $\chi \circ g$ 表示从 $\mathbb{F}_q$ 到 $\{0, \pm 1\} \subseteq \mathbb{F}_q$ 的函数，其取值由下式给出：

$$\chi \circ g(\alpha) = \chi(g(\alpha)).$$

（我们绝不会用 $\chi \circ g$ 指代多项式 $g^{(q-1)/2}(X)$。）

对于任意次数为 d 的非零 $g(X)$，我们可以将其写为：

$$g(X) = \lambda \cdot \bar{g}(X) \cdot h(X)^2$$

其中 $\lambda \in \mathbb{F}_q^*$, $\bar{g}(X)$ $h(X) \in \mathbb{F}_q[X]$，满足：

- $\bar{g}(X)$ 是首一且无平方因子的，
- $h(X)$ 是首一的。

$\bar{g}(X)$ 是 $g(X)$ 的“无平方因子核”，并且在本质上决定了 $\chi \circ g$。

事实上，对于所有 α，其中 $h(\alpha) \neq 0$，

$$\chi \circ g(\alpha) = \chi(\lambda) \cdot \chi \circ \bar{g}(\alpha).$$

因此，要么为 $\Delta(\chi \circ g,\ \chi \circ \bar{g}) \leq d$，要么为 $\Delta(\chi \circ g,\ -\chi \circ \bar{g}) \leq d$。

2.3 特征为2的域中的加性特征

设 q 为 2 的幂，即 $q = 2^b$。

令 $\mathsf{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ 为域迹映射：

$$\mathsf{Tr}(\beta) = \sum_{i=0}^{b-1} \beta^{2^i}.$$

令 $\mathbf{TR}(X) \in \mathbb{F}_q[X]$ 为多项式：

$$\mathbf{TR}(X) = \sum_{i=0}^{b-1} X^{2^i}.$$

对于多项式 $g(X) \in \mathbb{F}_q[X]$，我们用 $\mathsf{Tr} \circ g$ 表示从 $\mathbb{F}_q$ 到 $\mathbb{F}_2$ 的函数，其取值定义如下：

$$\mathsf{Tr} \circ g(\alpha) = \mathsf{Tr}(g(\alpha)).$$

（我们绝不会用 $\mathsf{Tr} \circ g$ 指多项式 $\mathbf{TR}(g(X)) = \sum_{i=0}^{b-1} (g(X))^{2^i}$.）

对于任意非零的 $g(X)$，若其次数为 d，我们可以将其写为：

$$g(X) = \lambda + \bar{g}(X) + h(X) + h^2(X),$$

其中 $\lambda \in \mathbb{F}_q$ 和 $\bar{g}(X)$ $h(X) \in \mathbb{F}_q[X]$ 满足：

- $\bar{g}(X)$ 仅含奇数次单项式，
- $h(X)$ 的常数项为 0。

证明方法是反复取次数最高的偶次单项式 $a_{2i}X^{2i}$，并将其写成 $(a_{2i}^{1/2}X^i)$ 和 $(a_{2i}^{1/2}X^i + a_{2i}X^{2i})$ 之和——前者的次数较低，后者则具有$h(X) + h^2(X)$的形式。

$\bar{g}(X)$ 是 $g(X)$ 的“奇数次核心”，并且基本上决定了 $\mathsf{Tr} \circ g$。

事实上，对于所有 $\alpha \in \mathbb{F}_q$,

$$\mathsf{Tr} \circ g(\alpha) = \mathsf{Tr}(\lambda) + \mathsf{Tr} \circ \bar{g}(\alpha).$$

因此，要么 $\mathsf{Tr} \circ g = \mathsf{Tr} \circ \bar{g}$，要么 $\mathsf{Tr} \circ g = 1 + \mathsf{Tr} \circ \bar{g}$。

3 $\chi \circ g$

设 q 为奇素数幂。

设 $g(X) \in \mathbb{F}_q[X]$ 是一个首一无平方因子多项式。本节给出一种高效算法，在能够访问 $\chi \circ g$ 的含噪版本 r 的情况下，恢复 $g(X)$。

算法 A:
参数：次数 $d \leq O(\epsilon\sqrt{q})$，误差界 $e \leq \left(\frac{1}{8} - \epsilon\right) q$。输入 r：
$\mathbb{F}_q \to \{0, \pm 1\}$

1. 令
   - $M = \frac{16}{\epsilon} d$
   - $c = \frac{M}{2}$
   - $h = 2 \cdot e$。
   - $D = d \cdot ((q-1)/2 + M) + cq = (1 + O(\epsilon)) \cdot \frac{1}{2} \cdot M \cdot q$,
   - $u = h + dM = 2e + O(\frac{d^2}{\epsilon})$。
2. 求解一个 $\mathbb{F}_q$ 线性方程组，以求出多项式 $F(X)$ $U_0(X) \ldots, U_{M-1}(X) \in \mathbb{F}_q[X]$，其中这些多项式不全为零，且满足：
   - 度$(F) \leq D$
   - 对每个 ℓ，$\deg(U_\ell) \leq u$
   - 对于所有 $\alpha \in \mathbb{F}_q$, $0 \leq \ell < M$：

$$F^{[\ell]}(\alpha) = r(\alpha) \cdot U_\ell(\alpha). \tag{3}$$

3. 将 $F(X)$ 分解为不可约因子：

$$F(X) = \lambda \prod_j H_j^{\mu_j}(X),$$

   其中 $H_j(X) \in \mathbb{F}_q[X]$ 互不相同且为首一多项式，并且 $\lambda \in \mathbb{F}_q^*$。
4. 定义

$$J = \left\{ j \text{ such that } \mu_j \in \left[\frac{3}{8}q, \frac{7}{8}q\right] \mod q \right\}.$$

5. 设

$$f(X) = \prod_{j \in J} H_j(X).$$

6. 返回 $f(X)$。

从算法的描述（以及在时间 poly(q, D) 内可以对 $\mathbb{F}_q$ 上次数为 D 的单变量多项式进行因式分解这一事实）可以清楚看出，按照 Ber70]，该算法可以在时间 poly(q) 内实现。
现在我们证明正确性。

3.1 算法的正确性

定理 3.1. 设 $\epsilon > 0$，并假设：

- $d \leq \frac{\epsilon}{16}\sqrt{q}$
- $e \leq \left(\frac{1}{8} - \epsilon\right) q$。

*Supp*若 $g(X) \in \mathbb{F}_q[X]$ 是次数为 $\leq d$ 的首一无平方因子多项式，使得 $\Delta(\chi \circ g, r) \leq e.$

则算法 *A* 返回 $g(X)$。

证明。 证明分为三个步骤。

Let $G(X) = (g(X))^{(q-1)/2+M}$.

首先，利用 r 接近 $\chi \circ g$ 这一假设，我们证明步骤 2 中的线性方程组存在非零解。具体而言，我们精心设计多项式 $E(X)$（这是一种高重数错误定位伪多项式）和 $V_0(X)$.....，$V_{M-1}(X)$，使得 $F(X) = E(X) \cdot G(X)$ 以及 $U_i(X) = V_i(X)$ 满足这些线性方程。因此，算法将在该步骤中找到一个非零解。

该算法 可能无法找到上述"预期"的解。在证明的第二步中，我们
证明无论找到了什么解 $(F, U_0, \ldots\ldots, U_{M-1})$， $F(X)$ 都与 $G(X)$ 存在某种非平凡关系。

最后，我们利用这种非平凡关系证明， F 的不可约因子的重数与 G 的不可约因子的重数密切相关，因此也与 g 的不可约因子的重数密切相关，并据此推出结论。

现在我们继续介绍详细内容。

第 1 步：线性方程组有非零解。

关键的观察是，如果接收字 $r: \mathbb{F}_q \to \{0, \pm 1\}$ 恰好是 Tr $\circ g$，那么 $F = G$ 就会给出方程组的一个有效解。但实际上，我们的接收字 r 只是接近 $\chi \circ g$。因此，仿照 Reed-Solomon 码的 Berlekamp-Welch 解码算法的思路，我们将在错误位置处将G 置零，从而得到一个有效解。

令 $S = \{\alpha \in \mathbb{F}_q \mid \chi \circ g(\alpha) \neq r(\alpha)\}$ 为错误集合。令 $Z_S(X)$ 为错误定位多项式 l:

$$Z_S(X) = \prod_{\alpha \in S} (X - \alpha).$$

回想一下， $c = M/2$ 且 $h = \frac{eM}{c} = 2e$。现在我们取 $E(X)$ 为 $Z_S^M(X)$ 的一个非零倍数，其形式为 rm:

$$E(X) = \sum_{i=0}^{c-1} E_i(X) \Lambda^i(X),$$

其次数为 $E_i \leq h$。（回想一下， $\Lambda(X) = X^q - X$）。这样的 $E(X)$ 存在，因为模 $Z_S^M(X)$ 消失会在 $c \cdot (h+1)$ 维的 $\mathbb{F}_q$-线性空间 $\{(E_0(X) \ldots, E_{c-1}(X))$ 上施加 eM 个约束，而 $\in \mathbb{F}_q[X]^c \mid \deg(E_i) \leq h\}$，且 $c \cdot (h+1) > ch = eM$。

这带来了两个很好的性质：

- $E^{[\ell]}(\alpha) = 0$ 对所有满足 $0 \leq \ell < M$ 的 $\alpha \in S$ 和 ℓ 都成立。这是因为 E 是 $Z_S^M(X)$ 的倍数，因此也是 $(X - \alpha)^M$ 的倍数。
- 对于每个满足 $0 \leq \ell < M$ 的 ℓ，都存在一个次数至多为 $h = 2e$ 的多项式 $E_{\langle \ell \rangle}(X) \in \mathbb{F}_q[X]$，使得对所有 $\alpha \in \mathbb{F}_q$:

$$E_{\langle \ell \rangle}(\alpha) = E^{[\ell]}(\alpha).$$

事实上，由引理 2.4 可得：

$$E^{[\ell]}(X) = \sum_{i=0}^{c-1} (-1)^i E_i^{[\ell-i]}(X) \mod \Lambda(X),$$

因此，如果我们定义：

$$E_{\langle \ell \rangle}(X) = \sum_{i=0}^{c-1} (-1)^i E_i^{[\ell-i]}(X),$$

对于所有 $\alpha \in \mathbb{F}_q$，我们都有：

$$E^{[\ell]}(\alpha) = \sum_{i=0}^{c-1} (-1)^i E_i^{[\ell-i]}(\alpha) = E_{\langle \ell \rangle}(\alpha).$$

我们将取解 $F(X)$ 为：

$$F(X) = E(X) \cdot G(X),$$

（回想一下，$G(X) = g^{(q-1)/2+M}(X)$）。

在计算其导数之前，我们先需要一个简单的引理。

引理 3.2。设 $g(X) \in \mathbb{F}_q[X]$ 是一个次数至多为 d 的多项式。那么，$g^j(X)$ 的 ℓ 阶导数具有如下形式：

$$(g^j)^{[\ell]}(X) = H_{g,j,\ell}(X) \cdot g(X)^{j-\ell},$$

其中 $H_{g,\ j,\ \ell}(X) \in \mathbb{F}_q[X]$ 的次数至多为 $d\ell - \ell$。

证明。利用 Hasse 导数的乘积法则。 □

令 $w = (q-1)/2 + M$。由上述引理可得：

$$G^{[\ell]}(X) = H_{g,w,\ell}(X) \cdot g^{w-\ell}(X) = H_{g,w,\ell}(X) \cdot g^{M-\ell}(X) \cdot g^{(q-1)/2}(X),$$

因此，对所有 $\alpha \in \mathbb{F}_q$：

$$G^{[\ell]}(\alpha) = H_{g,w,\ell}(\alpha) \cdot g^{M-\ell}(\alpha) \cdot g^{(q-1)/2}(\alpha) = \left(H_{g,w,\ell}(\alpha) \cdot g^{M-\ell}(\alpha)\right) \cdot \chi \circ g(\alpha). \tag{4}$$

现在我们计算 $E \cdot G$ 在 $\alpha \in \mathbb{F}_q$处的导数：

$$\begin{aligned}
(E \cdot G)^{[\ell]}(\alpha) &= \sum_{\ell_1+\ell_2=\ell} E^{[\ell_1]}(\alpha) \cdot G^{[\ell_2]}(\alpha) \\
&= \sum_{\ell_1+\ell_2=\ell} E_{\langle \ell_1 \rangle}(\alpha) \cdot H_{g,w,\ell_2}(\alpha) \cdot g^{M-\ell_2}(\alpha) \cdot \chi \circ g(\alpha) \\
&= \left(\sum_{\ell_1+\ell_2=\ell} E_{\langle \ell_1 \rangle}(\alpha) \cdot H_{g,w,\ell_2}(\alpha) \cdot g^{M-\ell_2}(\alpha) \right) \cdot \chi \circ g(\alpha) \\
&= \chi \circ g(\alpha) \cdot V_\ell(\alpha),
\end{aligned} \tag{5}$$

其中我们定义：

$$V_\ell(X) = \sum_{\ell_1+\ell_2=\ell} E_{\langle \ell_1 \rangle}(X) \cdot H_{g,w,\ell_2}(X) \cdot g^{M-\ell_2}(X).$$

很容易验证：

$$\deg(E \cdot G) \le d \cdot \left(\frac{q-1}{2} + M\right) + c \cdot q = D,$$
$$\deg(V_\ell) \le h + d \cdot M = u.$$

现在我们证明，对于所有 $\alpha \in \mathbb{F}_q$ 以及所有满足 $0 \le \ell < M$ 的 ℓ：

$$(E \cdot G)^{[\ell]}(\alpha) = r(\alpha) \cdot V_\ell(\alpha). \tag{6}$$

对于 $\alpha \notin S$，我们有 $r(\alpha) = \chi \circ g(\alpha)$，因此（6）由方程（5）推出。

对于 $\alpha \in S$，我们有 $V_\ell(\alpha) = 0$（因为对于所有 $\ell_1 \le \ell < M$，$E_{\langle \ell_1 \rangle}(\alpha) = E^{[\ell_1]}(\alpha) = 0$）。因此（$E \cdot G$）$^{[\ell]}(\alpha) = 0$ 也成立（根据方程（5））， 对于这种情况我们同样得到（6）。

因此，元组（$E \cdot G$、V_0、.....、V_{M-1}）满足方程组（3），正如所要求的那样。

步骤 2：建立 F 与 G 的关系

事实证明，无论算法找到哪个 $F(X)$，它都必定与某种程度上相关的 $G(X)$ 有关。

首先，我们快速注意到 $F(X)$ 必须是一个非零多项式。我们知道， F 和 U_ℓ 中至少有一个非零。如果某个 $U_\ell(X)$ 非零，那么利用以下事实：(1) $\chi \circ g$ 至多有 d 个零点；(2)$\Delta(\chi \circ g,\ r) < \frac{1}{8}q$；(3) $U_\ell(X)$ 至多有 $h < \frac{1}{4}q$ 个零点，我们得到对于某个α，$(\chi \circ g(\bar{\alpha})) \cdot U_\ell(\alpha)$ 必须非零；而方程（3）告诉我们， $F(X)$ 非零。

现在按如下方式选取 t，$k \in \mathbb{N}$：

$$t = \frac{3}{8}M.$$
$$k = e + 4dM.$$

我们将证明存在如下形式的非零多项式 $A(X)$、 $B(X)$：

$$A(X) = \sum_{i=0}^{t-1} A_i(X)\Lambda^i(X),$$

$$B(X) = \sum_{i=0}^{t+c-1} B_i(X)\Lambda^i(X),$$

满足 $\deg(A_i) \le k$、$\deg(B_i) \le k + 2e$，且：

$$A(X) \cdot F(X) = B(X) \cdot G(X).$$

我们再次通过维数计数来完成证明。 A_i 和 B_i 的系数总数为：

$$\begin{aligned} N &= (t) \cdot (k+1) + (t+c) \cdot (k+2e+1) \\ &> \frac{3}{8}M \cdot (e + 4dM) + \frac{7}{8}M \cdot (3e + 4dM) \\ &= 3Me + 5dM^2. \end{aligned} \tag{7}$$

并将它们视为未知数。通过对这些未知数施加至多 $N-1$ 齐次线性约束，我们可以确保对于每个满足 $0 \le \ell < M$ 的 ℓ，以及每个 $\alpha \in \mathbb{F}_q \setminus S$：

$$(A \cdot F)^{[\ell]}(\alpha) = (B \cdot G)^{[\ell]}(\alpha). \tag{8}$$

后一个方程意味着多项式 $(A \cdot F - B \cdot G)(X)$ 在每个 $\alpha \in \mathbb{F}_q \setminus S$ 处都以 M 为重数消失，因此至少有

$$M \cdot |\mathbb{F}_q \setminus S| \geq M \cdot (q - e) > \left(\frac{7}{8} + \epsilon\right) Mq$$

根，按重数计数。但 $(A \cdot F - B \cdot G)(X)$ 的次数可以界定为：

$$\begin{aligned}
\mathsf{deg}(A \cdot F - B \cdot G) &\leq \max(\mathsf{deg}(A \cdot F), \mathsf{deg}(B \cdot G)) \\
&\leq \max(tq + D, (t + c)q + ((q-1)/2 + M) \cdot d) \\
&\leq \max(tq + D, tq + D) \\
&= \frac{3}{8} Mq + d \cdot ((q-1)/2 + M) + cq \\
&< \left(\frac{7}{8} + \frac{\epsilon}{2}\right) Mq
\end{aligned}$$

这意味着 $(A \cdot F - B \cdot G)(X) = 0$。

剩下要说明的是，如何仅使用至多 $N - 1$ 个线性约束，作用于 A_i 和 B_i的系数，以确保方程 (8) 成立。

首先，注意对于每个 ℓ，都存在次数至多分别为 k，$k+2e$ 的多项式 $A_{\langle \ell \rangle}(X)$、$B_{\langle \ell \rangle}(X)$（其系数是 A，B的系数的齐次线性组合），定义如下：

$$A_{\langle \ell \rangle}(X) = \sum_{i=0}^{t-1} (-1)^i A_i^{[\ell - i]}(X)$$

$$B_{\langle \ell \rangle}(X) = \sum_{i=0}^{t+c-1} (-1)^i B_i^{[\ell - i]}(X)$$

使得对所有 $\alpha \in \mathbb{F}_q$：

$$A^{[\ell]}(\alpha) = A_{\langle \ell \rangle}(\alpha).$$

$$B^{[\ell]}(\alpha) = B_{\langle \ell \rangle}(\alpha).$$

（这里我们使用引理 2.4 计算了 $A^{[\ell]}$ 和 $B^{[\ell]}$，并在 $\alpha \in \mathbb{F}_q$ 处对它们求值。）接下来，回顾一下，对于所有 $\alpha \in \mathbb{F}_q$以及所有满足 $0 \leq \ell < M$ 的 ℓ，都有 $F^{[\ell]}(\alpha) = r(\alpha) U_\ell(\alpha)$。于是：

$$\begin{aligned}
(A \cdot F)^{[\ell]}(\alpha) &= \sum_{\ell_1 + \ell_2 = \ell} A^{[\ell_1]}(\alpha) F^{[\ell_2]}(\alpha) \\
&= r(\alpha) \cdot \sum_{\ell_1 + \ell_2 = \ell} A_{\langle \ell_1 \rangle}(\alpha) U_{\ell_2}(\alpha).
\end{aligned} \tag{9}$$

Simi类似地，对于所有 $\alpha \in \mathbb{F}_q$ 以及所有满足 $0 \leq \ell < M$ 的 ℓ，有 $G^{[\ell]}(\alpha) = \chi \circ g(\alpha) \cdot H_{g,\ w,\ \ell}(\alpha) \cdot g^{M-\ell}(\alpha)$。然后 ：

$$\begin{aligned}
(B \cdot G)^{[\ell]}(\alpha) &= \sum_{\ell_1 + \ell_2 = \ell} B^{[\ell_1]}(\alpha) G^{[\ell_2]}(\alpha) \\
&= \chi \circ g(\alpha) \cdot \sum_{\ell_1 + \ell_2 = \ell} B_{\langle \ell_1 \rangle}(\alpha) H_{g,w,\ell_2}(\alpha) \cdot g^{M - \ell_2}(\alpha).
\end{aligned} \tag{10}$$

现在，我们可以写出施加于 A_i 和 B_i 的系数的线性约束。我们要求，对于每个满足 $0 \le \ell < M$ 的 ℓ，以下多项式等式成立：

$$\sum_{\ell_1+\ell_2=\ell} A_{\langle \ell_1 \rangle}(X) U_{\ell_2}(X) = \sum_{\ell_1+\ell_2=\ell} B_{\langle \ell_1 \rangle}(X) H_{g,w,\ell_2}(X) g^{M-\ell_2}(X). \tag{11}$$

所有这些多项式的系数都是 A_i和 B_i的系数的齐次线性组合。

等式左侧的多项式次数至多为

$$k + u = k + dM + h = 3e + dM.$$

等式右侧的多项式次数至多为

$$(k + 2e) + dM = 3e + dM.$$

因此，这些 M 个等式施加的 $\mathbb{F}_q$-线性约束总数至多为：

$$M \cdot (3e + dM + 1) < 3Me + 5dM^2.$$

将此结果与方程（7）结合，可得存在 $A(X)$ $B(X)$，且不全为 0，满足方程（11）。最后，由方程（9）、（10）和（11），并利用以下事实：对于每个 $\alpha \in \mathbb{F}_q \setminus S$， $r(\alpha) = \chi \circ g(\alpha)$，我们得出方程（8）成立。由此得到所需的多项式恒等式：

$$A(X) \cdot F(X) = B(X) \cdot G(X).$$

步骤 3：关联 F 和 G的因子重数

最后，我们利用恒等式以及 A和 B 的特殊形式，来关联 F 和G的因子重数。下面的引理 3.3 表明， A 和 B 都具有这样的特殊性质：每个不可约因子的重数都近似为 q的倍数。另一方面， g（X）的不可约因子在 G 中的重数模 q 后近似为 $q/2$ （这是我们利用 g（X）无平方因子性的关键步骤）。由此我们可以确定 g（X）的非平方因子，进而确定 g（X）。

引理 3.3。 设 $k < q$。设 $C(X) \in \mathbb{F}_q[X]$ 是如下形式的非零多项式：

$$\sum_{i=0}^{t-1} C_i(X) \Lambda^i(X),$$

其中，对所有 i，均有$\deg(C_i) \le k$ 。

令 $H(X) \in \mathbb{F}_q[X]$ 是一个不可约多项式。设 μ 是整除 $C(X$的 $H(X)$ 的最高次幂 ）.

那么 μ 模 $q \in [0, k + t - 1]$。

证明。 令 $\alpha \in \overline{\mathbb{F}}_q$ （ $\mathbb{F}_q$ 的代数闭包）为 $H(X)$ 的一个根。

于是我们有：

$$\mu = \mathsf{mult}(C, \alpha).$$

根据重数的定义，

$$C^{[\mu]}(\alpha) \neq 0.$$

我们将证明 即当 ℓ 模 $q \in [k+t, q-1]$时， $C^{[\ell]}(X) = 0$。这意味着 μ 模 $q \in [0, k+t-$ 1].

假设 ℓ 模 $q \in [k+t, q-1]$。

现在我们利用 Hasse 导数的乘积法则进行计算[4],:

$$\begin{aligned} C^{[\ell]}(X) &= \sum_{i=0}^{t-1} \left(C_i \cdot \Lambda^i\right)^{[\ell]}(X) \\ &= \sum_{i=0}^{t-1} \left(\sum_{\substack{\ell_0,\ell_1,\ldots,\ell_i \\ \sum \ell_j = \ell}} C_i^{[\ell_0]}(X) \cdot \prod_{j=1}^{i} \Lambda^{[\ell_j]}(X) \right) \end{aligned}$$

现在我们看到，这个和中的所有项都是 0。

- 每个满足 $\ell_0 > k$ 的被加项都是 0，因为每个 C_i 的次数都是 $\leq k$。
- 对于至少有一个 ℓ_1、.....、ℓ_j 不属于集合 $\{0,1,q\}$ 的每个被加项，其值都是 0（因为 Λ 的那个导数为 0）。

因此，如果某个被加项非零，那么它必须满足 $\ell_0 \in [0,k]$ 和 ℓ_1、.....、$\ell_i \in \{0,1,q\}$。

但是，如果 ℓ 模 $q \in [k+t, q-1]$，那么我们不可能将 ℓ 写成 $[0,k]$ 中的一个整数与集合 $\{0,1,q\}$ 中至多 $i \leq t-1$ 个整数之和。

因此，如果 $\ell \bmod q \in [k+t, q-1]$, $C^{[\ell]}(X) = 0$，则如所声称。 □

现在令 $H(X)$ 为 $\mathbb{F}_q[X]$ 中的任意不可约多项式。令 μ_F、μ_A、μ_B、μ_G、μ_g 分别为整除 $F(X)$ $A(X)$ $B(X)$ $G(X)$ $g(X)$ 的 $H(X)$ 的最高次幂。根据我们对 g 作出的无平方因子性假设，有 $\mu_g \in \{0,1\}$。

然后根据恒等式 $AF = BG$,

$$\mu_F = \mu_G + \mu_B - \mu_A.$$

根据引理 3.3,

$$\mu_B \in q \cdot \mathbb{Z} + [0, 3e + 4dM + \frac{7}{8}M],$$

$$\mu_A \in q \cdot \mathbb{Z} + [0, e + 4dM + \frac{3}{8}M].$$

因此 $\mu_F \in \mu_G + q \cdot \mathbb{Z} + [-e - 5dM, 3e + 5dM]$。

注意， $\mu_G = ((q-1)/2 + M) \cdot \mu_g$，因此:

- 如果 $\mu_g = 1$，那么:

$$\mu_G = q/2 + (M-1)/2,$$

因此:

$$\mu_F \in q \cdot \mathbb{Z} + q/2 + [-e - 5dM, 3e + 6dM] \subseteq q \cdot \mathbb{Z} + (3q/8, 7q/8).$$

- 如果 $\mu_g = 0$，那么:

$$\mu_G = 0,$$

因此:

$$\mu_F \in q \cdot \mathbb{Z} + [-e - 5dM, 3e + 5dM] \subseteq q \cdot \mathbb{Z} + (-q/8, 3q/8).$$

[4]这里不能使用引理 2.4，因为它只讨论 $< q$ 阶导数。但思路是相同的。

这里我们用到了以下事实： $e \leq \left(\frac{1}{8} - \epsilon\right) q$和 $6dM < 96\frac{d^2}{\epsilon} < \epsilon q$。

因此，步骤 4 中创建的集合 J 可确保 $\{H_j \mid j \in J\}$ 恰好是所有整除无平方因子多项式 $g(X)$的不可约因子 $H(X)$ 的集合。
这意味着，步骤 5 中找到的 $f(X)$ 等于 $g(X)$，正如所需。 □

3.2 备注

第 5.6 节给出了一种替代分析方法，在定量上略弱一些，在概念上则略为简单。它用再次使用高重数错误定位伪多项式，取代了步骤 2 中略显晦涩的插值论证。

4 迹 $\circ g$

令 q 为 2 的幂。

设 $g(X) \in \mathbb{F}_q[X]$ 是一个次数至多为 d 且只含奇数次单项式的多项式：

$$g(X) = a_1 X + a_3 X^3 + \ldots + a_d X^d.$$

本节 中，我们给出一种高效算法，在已知 Tr $\circ$的含噪版本 r 的情况下恢复 $g(X)$ g.

主要子程序——算法 B——找出 $g(X)$中次数为 d的单项式。知道该单项式后，我们可以从 r 中减去该单项式的迹并重复此过程：这样就能恢复完整的多项式 g。

算法 B：
参数：次数 $d \leq O(\epsilon\sqrt{q})$（奇整数），误差界 $e \leq \left(\frac{1}{8} - \epsilon\right) q$。输入 r：$\mathbb{F}_q \to \mathbb{F}_2$

1. 令
   - $M = \frac{16}{\epsilon} d$
   - $c = \frac{1}{2} \cdot M$
   - $h = 2 \cdot e$
   - $u = h + dM = 2e + O(\frac{d^2}{\epsilon})$。
2. 对每个 $h^* \in [0, h]$
   - 尝试求解一个 $\mathbb{F}_q$-线性方程组，以求得多项式 $F(X)$ $E(X)$、 $U_0(X)$ $U_1(X) \ldots, U_{M-1}(X)$ $\in \mathbb{F}_q[X]$，其中：
     - $F(X)$的次数恰为 $(d/2 + c)q + h^*$。
     - $E(X)$的次数恰好为 $cq + h^*$，其形式为：

       $$\sum_{i=0}^{c} E_i(X) \Lambda^i(X),$$

       其中每个 $\deg(E_i) \leq h$。
     - 每个 $U_\ell(X)$的次数至多为 u。
     - 对于所有 $\alpha \in \mathbb{F}_q$、 $0 \leq \ell < M$：

       $$F^{[\ell]}(\alpha) = r(\alpha) \cdot E^{[\ell]}(\alpha) + U_\ell(\alpha), \tag{12}$$

3. 如果不存在这样的 h^*，则返回 $0 \cdot X^d$。
4. 否则取一个解 $E(X)$ $F(X)$，其次数为 D_E， D_F。
5. 设 $a \cdot X^{D_F}$、 $b \cdot X^{D_E}$分别为 $F(X)$ $E(X)$ 的首项单项式。
   令 $a_d = (a/b)^2$。
6. 返回 $a_d X^d$。

现在给出主要算法，该算法会反复调用上述子程序。

算法 C:
参数：次数 $d \le O(\epsilon\sqrt{q})$（一个奇整数），误差界 $e \le \left(\frac{1}{8} - \epsilon\right) q$。输入 r：
$\mathbb{F}_q \to \mathbb{F}_2$

1. 初始化：
   - $f(X) = 0$.
   - $d = d$.
   - $r = r$.

2. 当 $d > 0$ 时：
   - 使用参数 d 在 $\widetilde{r}$ 上运行算法 B，e。
   - 令 $a_{\widetilde{d}} X^d$ 为其返回的单项式。
   - 更新 $f(X) = f(X) + a_{\widetilde{d}} X^d$。
   - 对每个 $\alpha \in \mathbb{F}_q$，更新：

$$\widetilde{r}(\alpha) = \widetilde{r}(\alpha) - \mathsf{Tr}(a_{\widetilde{d}} \alpha^{\widetilde{d}})$$

   - 更新 $d = d - 2$。

3. 返回 $f(X)$。

从算法的描述中可以清楚看出，它可以在 poly(q) 时间内运行。下一小节将证明其正确性。

4.1 算法的正确性

关于算法 C 的主要定理如下。

定理 4.1. 设 $\epsilon > 0$，并假设：

- $d \le \frac{\epsilon}{16}\sqrt{q}$ 是奇整数，
- $e = \left(\frac{1}{8} - \epsilon\right) q$。

假设 $g(X) \in \mathbb{F}_q[X]$ 是一个次数为 $\le d$ 且仅含奇数次单项式的多项式，满足 $\Delta(\text{迹} \circ g, r) \le e$。

那么算法 *C* 返回 $g(X)$。

关键断言涉及算法 B 的行为。

定理 4.2。设 $\epsilon > 0$，并假设：

- $d \le \frac{\epsilon}{16}\sqrt{q}$ 是一个奇整数，
- $e = \left(\frac{1}{8} - \epsilon\right) q$。

假设 $g(X) \in \mathbb{F}_q[X]$ 是一个次数为 $\le d$ 且仅含奇数次单项式的多项式，使得 $\Delta(\text{迹} \circ g, r) \le e$。

然后算法 *B* 返回 $a_d X^d$。

根据定理 4.2，定理 4.1 的正确性很容易证明。

该算法保持以下不变量：

$$\Delta(\widetilde{r}, \mathsf{Tr} \circ (g - f)) \leq \left(\frac{1}{8} - \epsilon\right) q,$$

and:

$$\mathsf{deg}(g - f) \leq \widetilde{d}.$$

最终，我们得到 $f = g$。

下面仅演示第一步。假设 $g(X)$ 仅含奇数次单项式，且等于 $a_1 X + a_3 X^3 + \ldots + a_d X^d$。令 $g'(X) = a_1 X + a_3 X^3 + \ldots + a_{d-2} X^{d-2}$。且 $g''(X) = a_d X^d$。因此 $g' = g - g''$。

那么，定理 4.2 表明，算法 B 在输入 r 时返回 $a_d X^d$。接着，它更新 $\widetilde{r} = r$ –迹 $\circ g''$。于是我们有：

$$\Delta(\widetilde{r}, \mathsf{Tr} \circ g') = \Delta(r - \mathsf{Tr} \circ g'', \mathsf{Tr} \circ g - \mathsf{Tr} \circ g'') = \Delta(r, \mathsf{Tr} \circ g) \leq \left(\frac{1}{8} - \epsilon\right) q,$$

并且 $\mathsf{deg}(g') = \mathsf{deg}(g - g'') \leq d - 2$，如所需。

现在我们证明定理 4.2，该定理论述了算法 B 的正确性。

证明。 我们首先处理 $a_d \neq 0$ 的（主要）情形。

证明分为三个步骤。

回顾一下，$\mathbf{TR}(X)$ 是迹多项式：

$$\mathbf{TR}(X) = \sum_{i=0}^{b-1} X^{2^i},$$

其中 $q = 2^b$。

Let $G(X) = \mathbf{TR}(g(X))$，其次数恰为 $d \cdot \frac{q}{2}$（因为我们假设 $a_d \neq 0$）。

首先，利用假设 r 与 $\mathsf{Tr} \circ g$ 接近，我们证明存在某个 h^*，使算法 B 的步骤 2 中的线性方程组有非零解。与二次剩余特征的情形类似，我们找到多项式 $E_0(X) \ldots, E_c(X)$，使得 $E(X)$ 是高重数错误定位伪多项式；并找到 $V_0(X) \ldots, V_{M-1}(X)$，使得在选择该 $E_i(X)$ 后，$F(X) = E(X) \cdot G(X)$ 和 $U_i(X) = V_i(X)$ 满足这些线性方程。因此，算法将在该步骤中找到一个非零解。

算法可能找不到上述“预期的”解。在证明的第二步中，我们证明，无论它找到什么解（F，E，U_0，……，U_{M-1}），$F(X)$和 $E(X)$都与 $G(X)$存在某种非平凡关系。

最后，我们利用这一非平凡关系，从 F 和 E中提取 X^d 在 $g(X)$中的系数，并据此推导出结果。

现在我们来详细说明。

步骤 1：线性方程组有非零解。

现在我们证明，对于某个 $h^* \in [0, h]$，步骤 2 中的线性方程组存在非零解。

关键观察是，如果接收字 $r : \mathbb{F}_q \to \mathbb{F}_2$ 恰好是 $\chi \circ g$，那么 $F(X) = G(X)$，$E(X) = 1$，$U_\ell(X) = 0$ 就会给出方程组的一个有效解。但实际上，我们收到的字 r 只是接近 $\mathrm{Tr} \circ g$。因此，借鉴 Reed-Solomon 码的 Berlekamp-Welch 解码算法的思路，我们将在错误位置处将 G 置零，从而得到一个有效解。

令 $S = \{\alpha \in \mathbb{F}_q \mid \mathrm{Tr} \circ g(\alpha) \neq r(\alpha)\}$ 为错误集合。令 $Z_S(X)$ 为错误定位多项式：

$$Z_S(X) = \prod_{\alpha \in S} (X - \alpha).$$

回想一下，$c = M/2$ 以及 $h = \frac{eM}{c} = 2e$。现在我们取 $E(X)$ 为 $Z_S^M(X)$ 的一个非零倍数，其形式为 m:

$$E(X) = \sum_{i=0}^{c} E_i(X) \Lambda^i(X),$$

且 $\deg(E_i) \leq h$。这样的 $E(X)$ 存在，因为模 $Z_S^M(X)$ 消失会对 $(c+1) \cdot (h+1)$ 维的 $\mathbb{F}_q$-线性空间 $\{(E_0(X) \ldots, E_c(X)) \in \mathbb{F}_q[X]^{c+1} \mid \deg(E_i) \leq h\}$施加 eM 个约束，而 $(c+1) \cdot (h+1) > ch = eM$。

无论 $E(X)$ 的次数是多少，它都具有 $iq + j$ 的形式，其中 $i \in [0, c]$ 和 $j \in [0, h]$。将这个$E(X)$乘以 $\Lambda^{c-i}(X)$ 后，次数就变为 $cq + j$。我们将证明，当$h^* = j$时，这些线性方程有解。

与二次特征的情形完全相同，这个 $E(X)$ 有两个很好的性质：

- $E^{[\ell]}(\alpha) = 0$ 对所有满足 $0 \leq \ell < M$ 的 $\alpha \in S$ 和 ℓ 都成立。
- 存在一个次数至多为 $h = 2e$ 的多项式 $E_{\langle \ell \rangle}(X) \in \mathbb{F}_q[X]$，使得对所有 $\alpha \in \mathbb{F}_q$：

$$E_{\langle \ell \rangle}(\alpha) = E^{[\ell]}(\alpha).$$

我们将解 $F(X)$ 取为：

$$F(X) = E(X) \cdot G(X),$$

（回想一下，$G(X) = \mathbf{TR}(g(X))$.

在计算它的导数之前，我们需要一个简短的引理。

引理 4.3. 设 $g(X) \in \mathbb{F}_q[X]$ 是一个次数至多为 d 的多项式。那么，$G(X) = \mathbf{TR}(g(X))$ 的第 ℓ 阶导数具有如下形式：

$$(G)^{[\ell]}(X) = \begin{cases} G(X) & \ell = 0 \\ H_{g,\ell}(X) & \ell > 0, \end{cases}$$

其中 $H_{g,\ell}(X) \in \mathbb{F}_q[X]$ 是一个次数至多为 $d \cdot \ell$ 的多项式。

证明。 $\ell = 0$ 情形显然。

现在假设 $\ell \geq 1$。利用 Hasse 导数的乘积法则，我们有：

$$\begin{aligned}(g^{2^i})^{[\ell]}(X) &= \sum_{\ell_1+\ell_2=\ell} (g^{2^{i-1}})^{[\ell_1]}(X) \cdot (g^{2^{i-1}})^{[\ell_2]}(X) \\ &= \sum_{\ell_1<\ell/2} 2 \cdot (g^{2^{i-1}})^{[\ell_1]}(X) \cdot (g^{2^{i-1}})^{[\ell-\ell_1]}(X) + \begin{cases} 0 & \ell \text{ is odd} \\ \left(\left(g^{2^{i-1}}\right)^{[\ell/2]}(X)\right)^2 & \ell \text{ is even.} \end{cases} \\ &= \begin{cases} 0 & \ell \text{ is odd} \\ \left(\left(g^{2^{i-1}}\right)^{[\ell/2]}(X)\right)^2 & \ell \text{ is even.} \end{cases}\end{aligned}$$

这意味着

$$(g^{2^i})^{[\ell]}(X) = \begin{cases} \left(g^{[\ell/2^i]}(X)\right)^{2^i} & 2^i \text{ divides } \ell \\ 0 & \text{otherwise.} \end{cases}$$

如果 $\ell = 2^s \cdot (2s'+1) \geq 1$，那么我们可以明确写出：

$$G^{[\ell]}(X) = H_{g,\ell}(X) = \sum_{i=0}^{\min(s,b-1)} \left(g^{[\ell/2^i]}(X)\right)^{2^i}.$$

考察该表达式中各项的 degrees，我们看到 $\deg(H_{g,\ell}) \leq d \cdot 2^s \leq d \cdot \ell$，如所断言。 □

现在我们计算 $E \cdot G$ 在 $\alpha \in \mathbb{F}_q$ 处的导数：

$$\begin{aligned}(E \cdot G)^{[\ell]}(\alpha) &= \sum_{\ell_1+\ell_2=\ell} E^{[\ell_1]}(\alpha) \cdot G^{[\ell_2]}(\alpha) \\ &= E^{[\ell]}(\alpha)G(\alpha) + \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell}} E^{[\ell_1]}(\alpha) \cdot G^{[\ell_2]}(\alpha) \\ &= E^{[\ell]}(\alpha) \cdot G(\alpha) + \left(\sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell}} E_{\langle \ell_1 \rangle}(\alpha) \cdot H_{g,\ell_2}(\alpha) \right) \\ &= \mathsf{Tr} \circ g(\alpha) \cdot E^{[\ell]}(\alpha) + V_\ell(\alpha), \end{aligned} \tag{13}$$

其中我们定义：

$$V_\ell(X) = \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell}} E_{\langle \ell_1 \rangle}(X) \cdot H_{g,\ell_2}(X).$$

那么：

$$\deg(V_\ell) \leq h + d \cdot M = u.$$

由于 $\deg(G) = d \cdot \binom{q}{2}$，因此：

$$\deg(F) = \deg(E \cdot G) = (cq + h^*) + d \cdot \frac{q}{2},$$

现在我们证明，对于所有 $\alpha \in \mathbb{F}_q$ 和所有满足 $0 \leq \ell < M$ 的 ℓ：

$$F^{[\ell]}(\alpha) = (E \cdot G)^{[\ell]}(\alpha) = r(\alpha) \cdot E^{[\ell]}(\alpha) + V_\ell(\alpha). \tag{14}$$

对于 $\alpha \notin S$，有 $r(\alpha) = 迹 \circ g(\alpha)$，因此（14）由方程（13）得出。

对于 $\alpha \in S$，我们有 $E^{[\ell]}(\alpha) = 0$ 以及 $V_\ell(\alpha) = 0$ （因为对于所有 $\ell_1 \le \ell < M$， $E_{\langle \ell_1 \rangle}(\alpha) = E^{[\ell_1]}(\alpha) = 0$ ）。因此 $(E \cdot G)^{[\ell]}(\alpha) = 0$ 也成立（根据方程（13）），在此情况下我们同样得到（14）。

因此， $F = E \cdot G$、 E、 $U_0 = V_0$、……、$U_{M-1} = V_{M-1}$ 满足方程组（12），正如所希望的那样。

步骤 2：关联 F、 E 和 G

设 $F(X)$、 $E(X)$ 是算法找到的多项式。根据我们对次数的约束，$\deg(F) - \deg(E) = dq/2$。事实证明， $F(X)$ 和 $E(X)$ 必须与 $G(X)$ 存在某种关联。

具体而言，按如下方式选择 t、 $k \in \mathbb{N}$：

$$t = \frac{3}{8}M.$$
$$k = e + 4dM.$$

我们将证明，存在如下形式的非零多项式 $A(X)$、 $B(X)$：

$$A(X) = \sum_{i=0}^{t-1} A_i(X)\Lambda^i(X),$$

$$B(X) = \sum_{i=0}^{t+c+\frac{d}{2}-1} B_i(X)\Lambda^i(X),$$

满足 $\deg(A_i) \le k$、$\deg(B_i) \le k + h + dM$，并且：

$$A(X) \cdot \Big(F(X) - E(X) \cdot G(X) \Big) = B(X).$$

证明与二次剩余特征的情形类似；具体来说，我们建立一个未知数多于约束数的齐次 $\mathbb{F}_q$ 线性方程组。

$A(X)$ $B(X)$ 的未知系数总数为：

$$\begin{aligned} N &= t(k+1) + (t + c + (d/2)) \cdot (k + h + dM + 1) \\ &> \frac{3}{8}M \cdot (e + 4dM) + \frac{7}{8}M \cdot (3e + 5dM) \\ &> 3eM + 5dM^2. \end{aligned} \tag{15}$$

通过对这些未知数施加至多 $N - 1$ 个齐次线性约束，我们将确保对于每个满足 $0 \le \ell < M$ 的 ℓ，以及每个 $\alpha \in \mathbb{F}_q \setminus S$：

$$(A \cdot (F - E \cdot G))^{[\ell]}(\alpha) = B^{[\ell]}(\alpha). \tag{16}$$

后一个方程意味着，多项式 $A(X) \cdot (F(X) - E(X) \cdot G(X)) - B(X)$ 在每个 $\alpha \in \mathbb{F}_q \setminus S$ 处都以至少 M 的重数为零，因此其至少有

$$M \cdot |\mathbb{F}_q \setminus S| \ge M \cdot (q - e) > \left(\frac{7}{8} + \epsilon \right) Mq$$

根，计数 个重数。不过， $A(X)\cdot(F(X)-E(X)\cdot G(X))-B(X)$ 的次数可界定为 :

$$\begin{aligned}\deg(A\cdot(F-EG)-B) &\le \max(\deg(A)+\deg(F-EG),\deg(B))\\ &\le \max(tq+((c+(d/2))q+h),(t+c+(d/2))q)\\ &\le (t+c+(d/2))q+h\\ &= \frac{7}{8}Mq+(d/2)q+2e\\ &< \left(\frac{7}{8}+\frac{\epsilon}{2}\right)Mq.\end{aligned}$$

这意味着 $A(X)\cdot(F(X)-E(X)\cdot G(X))=B(X)$。

接下来需要说明，如何仅使用至多 $N-1$ 个关于 A_i 和 B_i 的系数的线性约束来确保方程 (16)。

首先，注意到对于每个 ℓ，存在次数至多为 k、$k+h+dM$ 的多项式 $A_{\langle\ell\rangle}(X)$、$B_{\langle\ell\rangle}(X)$（其系数分别是 A、B 的系数的齐次线性组合），使得：

$$A_{\langle\ell\rangle}(X)=\sum_{i=0}^{t-1}(-1)^i A_i^{[\ell-i]}(X)$$

$$B_{\langle\ell\rangle}(X)=\sum_{i=0}^{t+c+(d/2)-1}(-1)^i B_i^{[\ell-i]}(X)$$

使得对于所有 $\alpha\in\mathbb{F}_q$：

$$A^{[\ell]}(\alpha)=A_{\langle\ell\rangle}(\alpha) \tag{17}$$

$$B^{[\ell]}(\alpha)=B_{\langle\ell\rangle}(\alpha). \tag{18}$$

（同样，我们使用了引理 2.4）。

接下来请注意，我们在 $E(X)$ 上假设的形式意味着存在类似的低次多项式$E_{\langle\ell\rangle}(X)\in\mathbb{F}_q[X]$，其取值在 $\mathbb{F}_q$ 上与 $E^{[\ell]}$ 相匹配。具体而言，（回忆一下 AlgorithmB 中 E_i 的定义）定义：

$$E_{\langle\ell\rangle}(X)=\sum_{i=0}^{c}(-1)^i E_i^{[\ell-i]}(X),$$

并注意到 $\deg(E_{\langle\ell\rangle})\le h$，且：

$$E^{[\ell]}(\alpha)=E_{\langle\ell\rangle}(\alpha).$$

最后，回忆一下，对于所有 $\alpha\in\mathbb{F}_q$，以及所有满足 $0\le\ell<M$ 的 ℓ，$F^{[\ell]}(\alpha)=r(\alpha)E^{[\ell]}(\alpha)+U_\ell(\alpha)$。

因此，对于任意 $\alpha \in \mathbb{F}_q \setminus S$:

$$\begin{aligned}
(F - E \cdot G)^{[\ell]}(\alpha) &= \Big(r(\alpha)E^{[\ell]}(\alpha) + U_\ell(\alpha)\Big) - \sum_{\ell_1+\ell_2=\ell} E^{[\ell_1]}(\alpha)G^{[\ell_2]}(\alpha) \\
&= \big(r(\alpha) \cdot E_{\langle\ell\rangle}(\alpha) + U_\ell(\alpha)\big) - \left(E_{\langle\ell\rangle}(\alpha)G(\alpha) + \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell}} E_{\langle\ell_1\rangle}(\alpha)H_{g,\ell_2}(\alpha)\right) \\
&= (r(\alpha) - G(\alpha)) \cdot E_{\langle\ell\rangle}(\alpha) + \left(U_\ell(\alpha) - \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell}} E_{\langle\ell_1\rangle}(\alpha)H_{g,\ell_2}(\alpha)\right) \\
&= 0 + W_\ell(\alpha) \\
&= W_\ell(\alpha), \qquad (19)
\end{aligned}$$

其中， $W_\ell(X)$ 是次数至多为 $h + dM$ 的多项式，由下式给出:

$$W_\ell(X) = U_\ell(X) - \sum_{\substack{\ell_1+\ell_2=\ell \\ \ell_1<\ell}} E_{\langle\ell_1\rangle}(X)H_{g,\ell_2}(X).$$

并且我们用到了这样一个事实：对于所有 $\alpha \in \mathbb{F}_q \setminus S$， $r(\alpha) = G(\alpha)$。

因此，对于任意 $\alpha \in \mathbb{F}_q \setminus S$，我们有:

$$\begin{aligned}
(A \cdot (F - E \cdot G))^{[\ell]}(\alpha) &= \sum_{\ell_1+\ell_2=\ell} A^{[\ell_1]}(\alpha)\,(F - E \cdot G)^{[\ell_2]}(\alpha) \\
&= \sum_{\ell_1+\ell_2=\ell} A_{\langle\ell_1\rangle}(\alpha) \cdot W_{\ell_2}(\alpha). \qquad (20)
\end{aligned}$$

现在可以写出我们施加于 A_i 和 B_i 的系数上的线性约束。我们要求对于每个满足 $0 \le \ell < M$ 的 ℓ，下列多项式等式成立:

$$\sum_{\ell_1+\ell_2=\ell} A_{\langle\ell_1\rangle}(X)W_{\ell_2}(X) = B_{\langle\ell\rangle}(X). \qquad (21)$$

所有这些多项式的系数，都是 A_i 和 B_i 的系数的齐次线性组合。

等式左侧的多项式的次数至多为

$$k + (h + dM) = 3e + dM.$$

等式右侧的多项式次数至多为

$$k + h + dM = 3e + dM.$$

因此，这些 M 个等式施加的 $\mathbb{F}_q$-线性约束总数至多为:

$$M \cdot (3e + dM + 1) = 3eM + dM^2 + M < 3eM + 5dM^2.$$

结合方程（15），我们得到存在 $A(X)$ $B(X)$，且二者不全为 0，满足方程（21）。

最后，由方程（18）、（20）和（21），我们得出方程（16）成立。由此得到所需的多项式恒等式:

$$A(X) \cdot (F(X) - E(X)G(X)) = B(X).$$

步骤 3：关联 F、 E 和 G 的首项系数

由上述恒等式可得：

$$\mathsf{deg}(A) + \mathsf{deg}(F - E \cdot G) = \mathsf{deg}(B).$$

根据 A 和 B的选取，我们有：

$$\mathsf{deg}(A) \in q \cdot \mathbb{Z} + [0, k] = q \cdot \mathbb{Z} + [0, e + 4dM] \subseteq q \cdot \mathbb{Z} + \left[0, \frac{1}{8}q\right),$$

$$\mathsf{deg}(B) \in q \cdot \mathbb{Z} + [0, k + h + dM] \subseteq q \cdot \mathbb{Z} + [0, 3e + 5dM) \subseteq q \cdot \mathbb{Z} + \left[0, \frac{3}{8}q\right).$$

Thus

$$\mathsf{deg}(F - E \cdot G) = \mathsf{deg}(B) - \mathsf{deg}(A) \in q \cdot \mathbb{Z} + \left(-\frac{1}{8}q, \frac{3}{8}q\right).$$

现在我们研究 $\mathsf{deg}(F)$ 和 $\mathsf{deg}(E \cdot G)$。

根据构造，并利用 d 是奇数这一事实：

$$\mathsf{deg}(F) = \mathsf{deg}(E \cdot G) = (c + d/2)q + h^* \in q \cdot \mathbb{Z} + \left[\frac{q}{2}, \frac{q}{2} + 2e\right] \subseteq q \cdot \mathbb{Z} + \left[\frac{1}{2}q, \frac{3}{4}q\right).$$

现在来看关键之处。由于区间 $\left(-\frac{1}{8}q,\ \frac{3}{8}q\right)$ 和 $\left(\frac{1}{2}q,\ \frac{3}{4}q\right)$ 在模 q 意义下（相距相当远地）不相交，因此 $\mathsf{deg}(F - E \cdot G) \neq \max(\mathsf{deg}(F),\ \mathsf{deg}(E \cdot G))$。

这意味着 F 和 $E \cdot G$ 必须有相同的首项单项式！

我们手头有 F和 E，它们的首项系数分别为 a、$b \neq 0$，因此 G 的首项系数（我们知道它等于 $a_d^{q/2}$）必定等于 $\frac{a}{b}$。

因此：

$$a_d = a_d^q = (a_d^{q/2})^2 = \left(\frac{a}{b}\right)^2,$$

这与算法计算的结果一致。

这表明，只要 $a_d \neq 0$，算法 B 就能正确返回 $a_d X^d$。

最后，我们需要说明当 $a_d = 0$时会发生什么。我们将证明，不存在使线性方程组有解的 h^*（因此它会按预期返回 $0 \cdot X^d$）。

如果找到了解 F、E，那么 $\mathsf{deg}(F) - \mathsf{deg}(E) = dq/2$；根据上述证明中的步骤 2 和步骤 3，$F(X)$ 和 $E(X)G(X)$具有相同的首项单项式。然而，$a_d = 0$ 意味着 $\mathsf{deg}(G) < dq/2 = \mathsf{deg}(F) - \mathsf{deg}(E)$，这就产生了矛盾。

至此，算法 B 的正确性证明完成。 □

[5]这里还存在一定的改进空间。通过调整算法中的 c，h 以及分析中的 k，t，可以将译码半径略微（但幅度不大）提高到 $\frac{1}{2}\left(1 - \frac{1}{\sqrt{2}} - \epsilon\right) \cdot q \approx (0.145 - \epsilon)q$，代价是计算会稍微复杂一些，但不会引入新的概念。改进后的译码半径等于 $\frac{1}{2}(J(1/2) - \epsilon) \cdot q$，其中 $J(\delta)$ 是相对距离为 δ 的码的无字母表约束的 Johnson 半径。

4.2 一点说明

回顾算法 B 正确性证明中的步骤 2，我们在此推导出 G 与 F, E 之间通过如下形式的关系相关联：

$$A(X) \cdot (F(X) - E(X) \cdot G(X)) = B(X),$$

其中 $A(X)$ $B(X)$ 具有特殊形式。

事实证明，这些信息已经足以确定 g。然而，我们不知道如何仅凭 F 和 E 来高效地求出 g。因此，我们不得不绕更远的路：先求出 g 的首项系数，然后重复这一过程（其中需要求解一个新的 F, E）。

为什么 F 和 E 能唯一确定 g? 反设不然，存在两个不同的多项式 g_1、g_2，它们仅含奇数次单项式，且 $G_1 = \mathbf{TR}(g_1(X))$ $G_2 = \mathbf{TR}(g_2(X))$ 都满足上述方程：

$$A_1(X)(F(X) - E(X)G_1(X)) = B_1(X),$$

$$A_2(X)(F(X) - E(X)G_2(X)) = B_2(X),$$

消去 $F(X)$，得到：

$$A_1(X)A_2(X)E(X)\Big(G_1(X) - G_2(X)\Big) + (B_2(X)A_1(X) - B_1(X)A_2(X)) = 0.$$

Stepanov 曾明确研究过这类多项式，并证明它不可能等于 0。

关键在于，$G_1(X) - G_2(X)$ 是一个次数属于 $q \cdot \mathbb{Z} + q/2$ 的非零多项式。
这意味着两个多项式 $A_1(X)A_2(X)E(X)\cdot\Big(G_1(X)-G_2(X)\Big)$ 和 $B_1(X)A_2(X)-B_2(X)A_1(X)$ 的次数不可能相等：

前者的次数位于模 q 的区间 $[q/2, q/2 + 2k + h]$ 内，而后者的次数位于模 q 的区间 $[0, 2k + h]$ 内，并且这两个区间在模 q 意义下互不相交。

因此，它们的和不可能为零，这与假设 g 并非唯一确定相矛盾。

5 伪多项式理论

前面各节的结果大量运用了高次多项式，而这些多项式的所有导数在 $\mathbb{F}_q$上都表现得像低次数多项式。

我们将这些对象称为伪多项式。本节将对它们进行形式化定义，并建立一些基础理论。我们希望这对其他涉及有限域上多项式的代数问题和算法问题有所帮助。

定义 5.1 (伪导数**)**。 设 $A(X) \in \mathbb{F}_q[X]$。

定义 ℓ 阶伪导数 为 A，记作 $A_{\langle \ell \rangle}(X)$。它是次数至多为 $q-1$ 的唯一多项式，其在 $\mathbb{F}_q$ 上的取值与 $A^{[\ell]}(X)$ 的取值一致。具体而言：

$$A_{\langle \ell \rangle}(X) = \left(A^{[\ell]}(X) \mod \Lambda(X) \right),$$

其中 $\Lambda(X) = X^q - X$。

为简化记法，我们有时用 $A_{\langle \ell \rangle}$ 表示函数

$$A_{\langle \ell \rangle} : \mathbb{F}_q \to \mathbb{F}_q,$$

定义为 $A_{\langle \ell \rangle}(\alpha) = A^{[\ell]}(\alpha)$。

定义 5.2 （伪次数）。 令 $A(X) \in \mathbb{F}_q[X]$。

我们将 A 的伪次数定义为，记作 $\mathsf{pdeg}(A)$：

$$\max_{\ell \geq 0} \mathsf{deg}(A_{\langle \ell \rangle}).$$

我们称 $A(X)$ 是一个 k-伪多项式，如果

$$\mathsf{pdeg}(A) \leq k.$$

Wit采用这一记号后，我们现在列出关于伪多项式的一些有用事实 .

5.1 基本性质

有了这些记号之后，我们现在列出伪多项式的一些基本性质。

- 伪次数$(A+B) \leq$等于 max(伪次数(A),伪次数(B))。
- 伪次数$(A \cdot B) \leq$等于伪次数$(A) +$加伪次数(B)。
- 我们有如下关于伪次数的代数刻画。

  引理 5.3. 设 $A(X) \in \mathbb{F}_q[X]$，并设

  $$A(X) = \sum_{i \geq 0} A_i(X) \Lambda^i(X),$$

  其中每个 次数$(A_i) < q$，是 $A(X)$ 的以 $\Lambda(X)$ 为底的展开。

  Then

  $$\mathsf{pdeg}(A) = \max_{i \geq 0} \mathsf{deg}(A_i).$$

  证明见附录 A。

- 对于次数适中的多项式 $A(X)$，其伪次数可以近似表示为 $A(X)$ 的标准单项式展开。

  如果 A 的伪次数为 $\leq k$，次数为 D，那么 $A(X)$ 可以写成如下形式

$$\sum_{i=0}^{\lfloor D/q \rfloor} \widehat{A}_i(X) X^{iq},$$

  其中 $\deg(A_i(X)) \leq k + \lfloor D/q \rfloor$。反过来，如果 $A(X)$ 可以写成如下形式

$$\sum_{i=0}^{t} \widehat{A}_i(X) X^{iq},$$

  且 $\deg(A_i) \leq k$，那么 $A(X)$ 的伪次数至多为 $k+t$，次数至多为 $tq+k$。

  对于本文中的所有应用，我们都可以使用标准单项式基，而不会造成显著损失。

- 假设 $A(X) \in \mathbb{F}_q[X]$，且 $\deg(A) < Mq$。再假设，对于所有满足 $0 \leq \ell < M$ 的 ℓ，都有 $\deg(A_{\langle \ell \rangle}) \leq k$。那么 A的伪次数为 $\leq k$。

  也就是说，要验证 A 的伪次数较小，只需验证当 ℓ 不超过$\lceil \deg(A)/q \rceil$时， $A_{\langle \ell \rangle}$ 具有低次数性。

  这可由引理 5.3 的证明得出。

5.2 重数

- 设 $A(X) \in \mathbb{F}_q[X]$ 的伪次数为 $\leq k$，次数不超过 D。设 $H(X) \in \mathbb{F}_q[X]$ 不可约，并设 μ 是整除 $A(X)$ 的 $H(X)$ 的最高次幂。那么：

$$\mu \mod q \in \left[0, k + \frac{D}{q}\right].$$

  这是引理 3.3。

- 设 $A(X) \in \mathbb{F}_q[X]$ 的伪次数为 $\leq k$。那么：

$$\deg(A) \mod q \in [0, k].$$

  这可直接由引理 5.3 得出。

  这是无穷远点处对应于前一个事实的类比。

5.3 高重数零点的数量

- 对于任意 $S \subseteq \mathbb{F}_q$，以及任意 c，k，M 满足：

$$|S| < \frac{c}{M} \cdot k,$$

  存在一个非零的 $A(X) \in \mathbb{F}_q[X]$，其 $\deg(A) < cq$ 且 $\mathrm{pdeg}(A) < k$，使得对于所有 $\alpha \in S$，

$$\mathsf{mult}(A, \alpha) \geq M.$$

  这源于维数与约束计数。在定理 3.1 和定理 4.2 的证明中，我们在第 1 步构造用于纠错的伪多项式时已经看到了这一点。

- 反过来，下一个定理表明，当 q 为素数时，任意非零的 $A(X)$，只要 $\deg(A) < cq$ 且 $\mathrm{pdeg}(A) < k$，其重数至少为 M的根至多有 $2\frac{c}{M}k$ 个。当 $c < O(\epsilon)M$ 或 $c > (1 - O(\epsilon))M$时，该上界可改进为几乎 $(1+\epsilon)\frac{c}{M}k$。

定理 5.4。令 q 为素数。

令 $A(X) \in \mathbb{F}_q[X]$ 为非零多项式，其次数$(A) < cq$ 且 $\mathrm{pdeg}(A) < k$。令 M 满足$c < M < q$。

那么：

$$|\{\alpha \in \mathbb{F}_q \mid \mathrm{mult}(A, \alpha) \geq M\}| \leq \min\left(\frac{c}{M - c + 1} \cdot k + c, \quad k\right).$$

证明采用了 Guruswami 和 Kopparty [GK16] 关于朗斯基行列式秩的一个论证，该论证最初是在子空间设计和重数码的背景下发现的。

看起来存在一个更接近 $\frac{c}{M} \cdot k$的上界是合理的。我们不知道此类结论是否需要 q 的素性。

- 这里有一种自然的纠错码，与重数码密切相关。它由 4 个参数控制： q, M, c, k。

令 $\Sigma = \mathbb{F}_q^M$。此码的码字属于 $\Sigma^{\mathbb{F}_q}$。对于每个 $A(X) \in \mathbb{F}_q[X]$ 满足 $\deg(A) < cq$且 $\mathrm{pdeg}(A) < k$ 的对象，我们定义码字 y_A： $\mathbb{F}_q \to \Sigma$ 如下：

$$y_A(\alpha) = (A^{[0]}(\alpha), A^{[1]}(\alpha), \ldots, A^{[M-1]}(\alpha)).$$

此码的基数为 $|\Sigma|^{ck/M}$，码长为 q，码率为 $R = \frac{c}{M} \cdot \frac{k}{q}$，最小距离至少为

$$\left(1 - \min\left(\frac{k}{q}, \quad \frac{c}{M - c + 1} \cdot \frac{k}{q} + \frac{c}{q}, \quad \frac{c}{M}\right)\right) \cdot q,$$

其始终至少为 $(1 - 2R) \cdot q$。

当 $k = q$ 时，这是一个重数码，其距离为 $(1 - R) \cdot q$。当 $c = M$ 时，这是一个交织 Reed-Solomon 码，其距离为 $(1 - R) \cdot q$。此码的距离是否总是 $(1 - R)q$?

5.4 扭曲伪多项式

为了介绍 Stepanov 关于乘法特征和的 Weil 界证明（的一种小幅变体），我们现在定义扭曲伪多项式，并展示第 3 节中所见插值论证的一个简洁版本。

- 设 r： $\mathbb{F}_q \to \mathbb{F}_q$是一个函数。令 $k < q$。如果对所有 $\ell < M$，都存在某个 $U_\ell(X) \in \mathbb{F}_q[X]$，其次数至多为 h，使得：我们称 $F(X) \in \mathbb{F}_q[X]$是一个 r-扭曲的 (h, M)-伪多项式，

$$F_{\langle \ell \rangle} = r \cdot U_\ell.$$

- 下面的引理表明，任意两个次数至多为 cq的 r-扭曲 (h, M)-伪多项式都密切相关，前提是 h和 c足够小。

引理 5.5。 **</style}设 、、为参数，且 。令：** $\mathbb{F}_q \to \mathbb{F}_q$。

假设 $F(X)$ $G(X) \in \mathbb{F}_q[X]$与 $\deg(F)$、$\deg(G) < cq$均为 r-扭曲的 (h, M)-伪多项式。假设

$$k > \frac{M}{M - 2c} \cdot (h + 1).$$

然后 *th* 存在非零的 k-伪多项式 $A(X)$ $B(X)$，其 $\deg(A)$、$\deg(B) < Mq$满足：

$$A(X) \cdot F(X) = B(X) \cdot G(X).$$

证明。 如果 $k \geq q$，则结论显然成立，因此不妨设 $k < q$。

假设对于每个 $\ell < M$，我们都有：

$$F_{\langle \ell \rangle} = r \cdot U_\ell,$$
$$G_{\langle \ell \rangle} = r \cdot V_\ell,$$

其中 $U_\ell(X)$ $V_\ell(X) \in \mathbb{F}_q[X]$ 的次数至多为 h。

我们寻找形如以下形式的多项式 A， B：

$$A(X) = \sum_{i=0}^{M-c-1} A_i(X)\Lambda^i(X),$$

$$B(X) = \sum_{i=0}^{M-c-1} B_i(X)\Lambda^i(X),$$

其中 $\deg(A_i)$，$\deg(B_i) \leq k$。

未知数的数量严格大于 $2 \cdot (M-c) \cdot k$。

现在，我们对这些未知数施加齐次的 $\mathbb{F}_q$-线性约束。这些约束旨在表达以下等式：

$$(A \cdot F)_{\langle \ell \rangle} = (B \cdot G)_{\langle \ell \rangle},$$

对每个 $\ell < M$ 都成立。两边都可以用 A， B， F， G 的伪导数展开，其中后两个可以用 $r \cdot U_\ell$ 和 $r \cdot V_\ell$ 表示。

所有这些约束都可以简洁地写在环 $\mathbb{F}_q[X,T]$ 中，如下所示：

$$\left(\sum_{\ell_1<M} A_{\langle \ell_1 \rangle}(X) \cdot T^{\ell_1}\right) \cdot \left(\sum_{\ell_2<M} U_{\ell_2}(X) \cdot T^{\ell_2}\right) = \left(\sum_{\ell_3<M} B_{\langle \ell_3 \rangle}(X) \cdot T^{\ell_3}\right) \cdot \left(\sum_{\ell_4<M} V_{\ell_4}(X) \cdot T^{\ell_4}\right) \mod T^M$$

这里有 M 个次数至多为 $h+k$ 的关于 $\mathbb{F}_q[X]$ 的多项式等式，每个等式的系数都是由 A_i 和 B_i的系数组成的齐次线性组合。因此，线性约束总数为 $(h+k+1) \cdot M$ $\mathbb{F}_q$。

根据 k 的选取，我们有：

$$(h+k+1) \cdot M < 2k \cdot (M-c),$$

因此，这个方程组有一个非零解。

最后，我们证明 $A \cdot F = B \cdot G$。根据 A 和 B的设计，对每个 $\ell < M$，我们有：

$$(A \cdot F - B \cdot G)_{\langle \ell \rangle} = 0.$$

因此，对每个 $\alpha \in \mathbb{F}_q$，$\mathrm{mult}(A \cdot F - B \cdot G,\ \alpha) \geq M$。另一方面，

$$\deg(A \cdot F - B \cdot G) < cq + (M-c)q < Mq.$$

这意味着 $A \cdot F = B \cdot G$，正如所期望的那样。

□

• 下一个引理表明，如果我们有许多 r-扭曲的（h， M）-伪多项式，其次数至多为cq ，且 c， h 很小，那么它们之间存在非平凡关系。对 c 的小量要求较弱，但由此得到的关系也较弱。

引理 5.6。 设 m、 c、 h、 M 为参数，且 $c < \frac{m-1}{m} M$。设 r： $\mathbb{F}_q \to \mathbb{F}_q$。

假设 F_1（X）...、 F_m（X） $\in \mathbb{F}_q[X]$，其中 deg（F_i） $< cq$ 均为 r-扭曲的 （h， M）-伪多项式。假设

$$k > \frac{M}{(m-1)M - mc} \cdot (h+1).$$

那么存在 k-伪多项式 A_1（X）...、 A_m（X），其中 deg（A_i） $< Mq$，且不全为零，使得：

$$\sum_i A_i(X) F_i(X) = 0.$$

证明与引理 5.5 的证明完全相同，后者是 $m = 2$ 情形。

• 完全相同的论证同样可以给出稳健版本。

L引理 5.7。 设 c、 h、 γ、 M 为参数，且 $c <$ （$1 - 2\gamma$） $M/2$。设 r_1、 r_2： $\mathbb{F}_q \to \mathbb{F}_q$，满足：

$$\Delta(r_1, r_2) \leq \gamma q.$$

假设 $F(X)$ $G(X)$ $\in \mathbb{F}_q[X]$ 的次数(F)和次数(G) $< cq$分别为 r_1-扭曲和 r_2-扭曲的(h, M)-伪多项式。

假设

$$k > \frac{M}{(1-2\gamma)M - 2c} \cdot (h+1).$$

*Then th*存在非零的 k-伪多项式 $A(X)$ $B(X)$，其次数(A)和次数(B) $< Mq$满足：

$$A(X) \cdot F(X) = B(X) \cdot G(X).$$

证明中唯一的变化是，现在我们要寻找次数小于 $((1-\gamma)M - c)q$ 的 $A(X)$ 和 $B(X)$，这样即使给定的相符项更少，仍可转化为一个多项式恒等式。

Lemma 5.8. 令 m、 c、 h、 γ、 M 为参数，其中 $c < \frac{(m-1) - m\gamma}{m} M$。令 $r_1, \ldots, r_m$： $\mathbb{F}_q \to \mathbb{F}_q$，其中 ：

$$|\{\alpha \in \mathbb{F}_q \mid r_i(\alpha) \neq r_j(\alpha) \text{ for some } i, j\}| \leq \gamma q.$$

假设 $F_1(X) \ldots, F_m(X) \in \mathbb{F}_q[X]$ 的次数$(F_i) < cq$是 r_i-扭曲的(h, M)-伪多项式。假设

$$k > \frac{M}{(m - 1 - m\gamma)M - mc} \cdot (h+1).$$

那么存在 k-伪多项式 $A_1(X) \ldots, A_m(X)$，满足 deg$(A_i) < Mq$，且不全为零，使得：

$$\sum_i A_i(X) F_i(X) = 0.$$

5.5 Weil 界

- 现在我们可以证明二次剩余特征的 Weil 界。

  设 $f(X)$ $g(X) \in \mathbb{F}_q[X]$ 是次数至多为 $d \le O(\epsilon\sqrt{q})$ 的互不相同的首一无平方因子多项式。我们将证明

  $$\Delta(\chi \circ f, \chi \circ g) \ge \left(\frac{1}{2} - \epsilon\right) q.$$

  令 $M = \frac{2}{\epsilon}d$, $c = d$。设 $F(X) = f(X)^{(q-1)/2+M}$, $G(X) = g(X)^{(q-1)/2+M}$。

  那么 F 和 G 分别是 $(\chi \circ f)$-扭曲的和 $(\chi \circ g)$-扭曲的 (dM, M)-伪多项式 .

  现在令 $h = dM$ 和 $\gamma = \frac{1}{2} - \epsilon$。若 $\Delta(\chi \circ f, \chi \circ g) \le \gamma q$，则引理 5.7 告诉我们：

  $$k = \frac{1}{\epsilon} \cdot (h+1) \le O(\frac{d^2}{\epsilon^2}) < \frac{q}{4},$$

  t此处存在非零的 k-伪多项式 $A(X)$ $B(X)$，满足 $\deg(A), \deg(B) < Mq$，使得：

  $$A(X) \cdot F(X) = B(X) \cdot G(X),$$

  设 $H(X)$ 是一个多项式，它整除 $f(X)$ 和 $g(X)$ 中的一个，但不整除另一个。

  将引理 3.3 应用于 $H(X)$，再结合上述恒等式，便会得到矛盾。

- 接下来，我们证明 m 次幂剩余特征标 χ_m 的 Weil 界，其中 m 为素数。

  设 $f, g \in \mathbb{F}_q[X]$ 的次数至多为 $d \le O_m(\epsilon\sqrt{q})$，且彼此不同、均为首一多项式，并且每个不可约因子的重数为 $\in \{1, 2, \ldots, m-1\}$。当 $m = 2$ 时，最后这个条件推广了无平方因子性。我们将证明

  $$\Delta(\chi_m \circ f, \chi_m \circ g) \ge \left(1 - \frac{1}{m} - \epsilon\right) q.$$

  设 $M = O_m(\frac{d}{\epsilon})$、$c = O_m(d)$。设 $F(X) = f^{(q-1)/m+M}(X)$，$G(X) = g^{(q-1)/m+M}(X)$。

  设 $r_1, \ldots, r_m$： $\mathbb{F}_q \to \mathbb{F}_q$ 由下式给出：

  $$r_i(\alpha) = (\chi_m^{i-1} \circ f(\alpha)) \cdot (\chi_m^{m-i} \circ g(\alpha)).$$

  令 $F_1(X) \ldots, F_m(X)$ 定义为：

  $$F_i(X) = F^{i-1}(X) \cdot G^{m-i}(X).$$

  则 F_i 是一个 r_i-扭曲的（$O_m(dM)$ M）伪多项式。

  现在设 $h = O_m(dM)$ 和 $\gamma = 1 - \frac{1}{m} - \epsilon$。若 $\Delta(\chi_m \circ f, \chi_m \circ g) \le \gamma q$，则

  $$|\{\alpha \in \mathbb{F}_q \mid r_i(\alpha) \ne r_j(\alpha) \text{ for some } i, j\}| \le \gamma q,$$

  那么引理 5.8 告诉我们，对于：

  $$k = \frac{1}{\epsilon} \cdot (h+1) \le O(\frac{d^2}{\epsilon^2}) < \frac{q}{2m},$$

  存在 k-伪多项式 $A_i(X)$，其 $\deg(A_i) < Mq$，且并非全为零，使得：

  $$\sum_{i=1}^{m} A_i(X) \cdot F^{i-1}(X) \cdot G^{m-i}(X) = 0.$$

设 $H(X)$ 是一个不可约多项式，它在 $f(X)$ 和 $g(X)$ 中出现时具有不同的因子重数。那么，引理 3.3 告诉我们，上述和中的所有非零项在 $H(X)$ 中的因子重数各不相同（因为它们模 q 时彼此不同），因此该和不可能为 0，这就产生了矛盾。

- 对于小特征域上的加性特征和的 Weil 界，也可以给出类似的论证。这里仅作简要概述。

  设 q 的特征为 p。令 $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_q$ 和 $\mathbf{TR}(X) \in \mathbb{F}_q[X]$ 分别为域迹映射和迹多项式。

  设 $r\colon \mathbb{F}_q \to \mathbb{F}_q$是一个函数。若多项式 $F(X)$ 满足以下条件，我们称其为 r-引导的（h, M）伪多项式：对于所有 $\ell < M$，都存在 $U_\ell(X) \in \mathbb{F}_q[X]$，使得 $\deg(U_\ell) \le h$；并且只要 $\alpha \in \mathbb{F}_q$ 满足 $r(\alpha) = 0$，就有：

  $$F_{\langle \ell \rangle}(\alpha) = U_\ell(\alpha).$$

  设 $f(X) \in \mathbb{F}_q[X]$ 的次数为 $d \le O_p(\epsilon\sqrt{q})$，且其所有单项式的次数都与 p互素。我们将证明，满足 $\mathrm{Tr} \circ f(\alpha) = 0$的 $\alpha \in \mathbb{F}_q$至多有 $\left(\frac{1}{p} + \epsilon\right) q$个值。（由线性性可知，这给出了任意两个不同的此类 $\mathrm{Tr} \circ f$和 $\mathrm{Tr} \circ g$之间距离的下界 $\left(1 - \frac{1}{p} - \epsilon\right) q$。）

  令 $F(X) = \text{迹} \circ f(X)$。
  那么对于所有 $i \in [1, p-1]$，$F^i(X)$ 都是一个由 (迹 $\circ f$) 引导的 $(dM,\ M)$-伪多项式。此外，$\deg(F^i) = {}^{i\cdot\text{次数为}}{}_{p}\cdot q < dq$，因此 F^i对应 $i \in [1, p-1]$的次数模 q两两至少相差 $\frac{q}{p}$。

  假设对于超过 $(\frac{1}{p} + \epsilon)q$ 个 $\alpha \in \mathbb{F}_q$ 值，$\mathrm{Tr} \circ f(\alpha) = 0$。
  现在令 $A_0(X) \ldots,\ A_{p-1}(X)$ 为未知多项式，且 $\deg(A_i) < \left(\left(\frac{1}{p} + \frac{\epsilon}{2}\right) M - d\right) q$，$\mathrm{pdeg}(A_i) < O(\frac{dM}{\epsilon})$ $< \frac{q}{4p}$。通过计算约束，我们可以确保该多项式：

  $$B(X) = \sum_{i=0}^{p-1} A_i(X) \cdot F^i(X),$$

  其次数至多为 $\left(\frac{1}{p} + \frac{\epsilon}{2}\right) Mq$，在所有满足 $(\mathrm{Tr} \circ f)(\alpha) = 0$ 的 $\alpha \in \mathbb{F}_q$ 处都以重数 M 消失。（这里我们使用了 F^i 的 $(\mathrm{Tr} \circ f)$ 引导性质。）这意味着多项式 $B(X)$ 等于 0。

  最终的矛盾源于这样一个事实：$B(X)$ 中不同项的次数模 q 互不相同，因此它们的和不可能为 0。

5.6 算法 A 的另一种分析

现在，我们用刚刚介绍的一些术语，对算法 A 进行一种略有不同（也可能更具概念性）的分析。对于零错误的情况，这或许是最简单的正确性证明。

这种分析可以处理数量较少（但仍为 $\Omega(q)$）的错误。为简洁起见，我们假设 $g(X)$ 没有任何一次不可约因子，因此 $\chi \circ g$ 仅取 $\{\pm 1\}$ 值。我们还假设 r 仅取 $\{\pm 1\}$ 值。

我们沿用定理 3.1 证明中的记号，并从证明步骤 2 的开头继续。算法找到的 $F(X)$ 是一个 r-扭曲的 $(h,\ M)$-伪多项式。我们知道 $G(X)$ 是一个 $(\chi \circ g)$-扭曲的 $(O(dM)\ M)$-伪多项式。

那么 $(F \cdot G)(X)$ 是一个 $(r \cdot (\chi \circ g))$-扭曲的 $(h + O(dM)\ M)$-伪多项式。

现在观察到，函数 $r \cdot (\chi \circ g) : \mathbb{F}_q \to \mathbb{F}_q$ 与常值函数 1 很接近。它在 $\alpha \in \mathbb{F}_q$ 的至少 $q - e$ 个值上取值为 1。如果它处处取值为 1，那么 $(F \cdot G)$ 就会是一个真正的伪多项式。

我们可以像证明中的步骤 1 那样，使用高重数错误定位伪多项式来修正它。设 c', h' 由 $c' = M/4, h' = 4e$ 给出。那么，由于 $c' \cdot (h'+1) > eM$，我们可以得到一个多项式 $E'(X)$，满足 $\deg(E') < c'q$ 且 $\mathrm{pdeg}(E') \le h'$，并且它在 S 的所有点处都以重数 M 消失。

于是 $(E' \cdot F \cdot G)(X)$ 具有如下性质：对所有 $\ell < M$：

$$\deg((E' \cdot F \cdot G)_{\langle \ell \rangle}(X)) \le h' + h + O(dM).$$

此外，$\deg(E' \cdot F \cdot G) < c'q + cq + 2d \cdot ((q-1)/2 + M) < Mq$。

根据第 5.1 节中的事实，这意味着 $(E \cdot F \cdot G)(X)$ 是一个真正的 $(h + h' + O(dM))$-伪多项式。因此我们得到方程：

$$E'(X) \cdot F(X) \cdot G(X) = B(X),$$

其中 $E'(X)$ 是一个 $(h' + O(dM))$-伪多项式，$B(X)$ 是一个 $(h + h' + O(dM))$-伪多项式，并且 $\deg(E')$, $\deg(B) < Mq$。

将引理 3.3 应用于 $E'(X)$ 和 $B(X)$ 以分析因子重数，可得 $(F \cdot G)(X)$ 的所有不可约因子的因子重数都近似为 q 的倍数，正如所需。

5.7 定理 5.4 的证明

回顾定理 5.4 的陈述。

定理 5.4。设 q 为素数。

设 $A(X) \in \mathbb{F}_q[X]$ 是一个次数为$\deg(A) < cq$ 且 $\mathrm{pdeg}(A) < k$的非零多项式。设 M 满足$c < M < q$。

那么：

$$|\{\alpha \in \mathbb{F}_q \mid \mathsf{mult}(A, \alpha) \ge M\}| \le \min\left(\frac{c}{M - c + 1} \cdot k + c, \quad k\right).$$

证明。 首先证明较容易的界：

$$|\{\alpha \in \mathbb{F}_q \mid \mathsf{mult}(A, \alpha) \ge M\}| \le k.$$

由于 A 是一个次数至多为 $< Mq$的非零多项式，因此存在某个 $\ell < M$ 和某个 α_0，使得 $A_{\langle \ell \rangle}(\alpha_0) = A^{[\ell]}(\alpha_0) \neq 0$。对于这个 ℓ，我们有 $A_{\langle \ell \rangle}(X)$是一个次数至多为 k的非零多项式，因此至多有 k个 α 的取值使得 $A^{[\ell]}(\alpha) = A_{\langle \ell \rangle}(\alpha) = 0$。因此，对于至多 k 个 $\alpha \in \mathbb{F}_q$的取值，$\mathrm{mult}(A, \alpha) > \ell$，如所需。

现在证明另一个界。写作 $A(X) = \sum_{i=0}^{c-1} A_i(X) X^{iq}$，其中 $\deg(A_i) \le k + M$.

那么对于 $\ell < M$,

$$A^{[\ell]}(X) = \sum_{i=0}^{c-1} A_i^{[\ell]}(X) X^{iq}.$$

对于 $\alpha \in \mathbb{F}_q$，这让我们可以得到 $\mathrm{mult}(A, \alpha) \ge M$ 成立的一个简单判据：即，如果对所有 $\ell < M$,

$$\sum_{i=0}^{c-1} A_i^{[\ell]}(\alpha) \alpha^i = 0.$$

令 $R(X)$ 为该矩阵，其行由 $\ell \in \{0,1,\ldots,M-1\}$ 索引，列由 $i \in \{0,1,\ldots,c-1\}$ 索引，且其 (ℓ, i) 项为 $A_i^{[\ell]}(X)$。

令 $v(X)$ 为向量 $(1,\ X,\ X^2,\ \ldots\ldots,\ X^{c-1})$。

那么，$\mathrm{mult}(A,\ \alpha) \geq M$ 当且仅当：

$$R(\alpha) \cdot v(\alpha) = 0,$$

即，如果：

$$v(\alpha) \in \ker(R(\alpha)).$$

现在我们来界定此类 α 的数量。令 $W \subseteq \mathbb{F}_q^c$ 为所有满足 $\sum_i w_i A_i(X) = 0$ 的向量 $(w_0,\ \ldots\ldots,\ w_{c-1}) \in \mathbb{F}_q$ 的集合。那么对于每个 $w \in W$，

$$R(X) \cdot w = 0.$$

因此，对于每个 $\alpha \in \mathbb{F}_q$，

$$W \subseteq \ker(R(\alpha)).$$

对于满足 $v(\alpha) \in \ker(R(\alpha))$ 的 $\alpha \in \mathbb{F}_q$ 数量的界，随即由以下两个断言得到。

命题 5.9。满足 $\ker(R(\alpha)) \neq W$ 的 $\alpha \in \mathbb{F}_q$ 数量至多为 $\binom{c}{M-c+1} \cdot k$。 ———

命题 5.10。满足 $v(\alpha) \in W$ 的 $\alpha \in \mathbb{F}_q$ 数量至多为 c。

后一个命题直接由以下事实推出：$\dim(W) < c$，并且 $\mathbb{F}_q^c$ 中的矩曲线与任意真子空间的交集至多包含 c 个点。

下面证明第一个命题。

令 $I \subseteq \{0,1,\ldots,c-1\}$ 为使 $(A_i(X))_{i \in I}$ 在 $\mathbb{F}_q$ 上线性无关的极大子集。则 $|I| + \dim(W) = c$，且 $|I| \geq 1$。

令 $S(X)$表示 $R(X)$ 的子矩阵，该子矩阵由索引属于 I 的那些列组成。

现在假设 α 满足 $S(\alpha)$ 的列线性无关。于是我们得到 $\mathrm{rank}(R(\alpha)) = \mathrm{rank}(S(\alpha)) = |I|$，因此 $\dim(\ker(R(\alpha))) = c - |I| = \dim(W)$。这意味着 $\ker(R(\alpha)) = W$。

为了完成证明，我们证明使 $S(\alpha)$ 的列线性相关的 α 值至多有 $\binom{c}{M-c+1} \cdot k$ 个。这是定理 17（见 [GK16]，另见 [BCDZ25]）中论证的一个简单情形。

现在我们利用 q 的素性。根据线性无关的朗斯基判别准则（见 [BD10]），$S(X)$ 的顶端 $|I| \times |I|$ 子矩阵的行列式 $H(X)$ 非零。若 α 满足 $S(\alpha)$ 的列线性相关，则 α 是 $H(X)$ 的一个重数至少为 $M-c+1$ 的根。这是因为对于每个 $\ell < M-c+1$，$H^{[\ell]}(\alpha)$ 都是 $|I| \times |I|$ (α) 的若干 S 子矩阵的行列式[6] 的线性组合，而这些行列式全都为 0。但 $H(X)$ 是一个次数至多为 ck 的非零多项式。因此这样的 α 至多有 $\binom{c}{M-c+1} \cdot k$ 个。

至此，第一个断言的证明完成，定理也随之得证。 □

[6]这里我们使用 Hasse 导数的乘积法则、行列式的多重线性性，以及迭代 Hasse 导数的公式：$(F^{[i]})^{[j]}(X) = \binom{i+j}{j} F^{[i+j]}(X)$。 sse

参考文献

[AGHP92] Noga Alon、Oded Goldreich、Johan H˚astad 和 Ren´e Peralta。《几乎两两独立随机变量的简单构造》。随机结构与算法，3(3):289–304，1992年。[AHS25] Vikrant Ashvinkumar、Mursalin Habib 和 Shashank Srivastava。《折叠 Reed-Solomon 码列表译码的算法改进》。CoRR，abs/2508.12548，2025年。[ALT01] Alexei Ashikhmin、Simon Litsyn 和 Michael A Tsfasman。《渐近良好的量子码》。Physical Review A，63(3):032311，2001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，并应用于局部性质和拟阵》。arXiv 预印本 arXiv:2510.13777，2025年。[BD10] Alin Bostan 和 Philippe Dumas。《朗斯基行列式与线性无关》。The American Mathematical Monthly，117(8):722–727，2010年。[Ber70] Elwyn R. Berlekamp。《大有限域上的多项式因式分解》。Mathematics of Computation，24(111):713–735，1970年。[BGKS12] Jean Bourgain、Moubariz Z Garaev、Sergei V Konyagin 和 Igor E Shparlinski。《关于隐藏移位幂问题》。SIAM Journal on Computing，41(6):1524–1557，2012年。[BHKS23] Siddharth Bhandari、Prahladh Harsha、Mrinal Kumar 和 Ashutosh Shankar。《将重数 Schwartz-Zippel 引理算法化》。载于 Nikhil Bansal 和 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年。[BHKS24] Siddharth Bhandari、Prahladh Harsha、Mrinal Kumar 和 Madhu Sudan。《乘积集上多变量重数码的译码》。IEEE 信息论汇刊，70(1):154–169，2024年。[Bom73] Enrico Bombieri。《有限域上曲线的点计数》。S´eminaire Bourbaki，1972/73(430):234–241，1973年。[BRC60] Raj C. Bose 和 Dwijendra K. Ray-Chaudhuri。《一类纠错二元群码》。Information and Control，3(1):68–79，1960年。[BW86] Elwyn R. Berlekamp 和 Lloyd R. Welch。《代数分组码的纠错》。技术报告，美国专利 4,633,470，1986年。于1983年提交。[CDGM25] Gil Cohen、Dean Doron、Noam Goldgraber 和 Tomer Manket。《追踪代数几何码：迈向达到 Gilbert–Varshamov 界》。计算复杂性电子研讨会（ECCC），32:174，2025年。[CGS16] Arkadev Chattopadhyay、Frederic Green 和 Howard Straubing。《奇特征域中幂运算的电路复杂度》。Chic. J. Theor. Comput. Sci.，2016，2016年。[CVDDM92] Zo´e Chatzidakis、Lou Van Den Dries 和 Angus Macintyre。《有限域上的可定义集》。J. reine angew. Math，427:107–135，1992年。[CZ25] Yeyuan Chen 和 Zihan Zhang。《显式折叠 Reed–Solomon 码和重数码达到宽松广义 Singleton 界》。载于《第57届 ACM 计算理论年会论文集》（STOC）。ACM，2025年。[DKSS13] Zeev Dvir、Swastik Kopparty、Shubhangi Saraf 和 Madhu Sudan。《重数方法的扩展及其在 Kakeya 集和合并器中的应用》。SIAM Journal on Computing，42(6):2305–2328，2013年。

[GHK+25] Abhibhav Garg、Prahladh Harsha、Mrinal Kumar、Ramprasad Saptharishi 和 Ashutosh Shankar。折叠 Reed–Solomon 码近期列表大小界综述。CoRR，abs/2502.14358，2025年。[GHKS24] Rohan Goyal、Prahladh Harsha、Mrinal Kumar 和 Ashutosh Shankar。单变量重数码与折叠 Reed–Solomon 码的快速列表解码。载于第65届 IEEE 计算机科学基础研讨会（FOCS）论文集，第328–343页。IEEE 计算机学会，2024年。[GK16] Venkatesan Guruswami 和 Swastik Kopparty。显式子空间设计。Combinatorica，36(2):161–185，2016年。[GR08] Ariel Gabizon 和 Ran Raz。大域上仿射源的确定性提取器。Combinatorica，28(4):415–440，2008年。[GS71] Ronald L. Graham 和 Joel H. Spencer。锦标赛问题的一个构造性解。Canadian Mathematical Bulletin，14(1):45–48，1971年。[GS99] Venkatesan Guruswami 和 Madhu Sudan。Reed-Solomon 码和代数几何码的改进解码。IEEE 信息论汇刊，45(6):1757–1767，1999年。[GW13] Venkatesan Guruswami 和 Carol Wang。Reed–Solomon 码的线性代数列表解码。IEEE 信息论汇刊，59(10):6415–6427，2013年。[HKT08] James W. P. Hirschfeld、G´abor Korchm´aros 和 Fernando Torres。有限域上的代数曲线。普林斯顿大学出版社，普林斯顿，新泽西州，2008年。[Hoc59] Alexis Hocquenghem。纠错码。Chiffres，2:147–156，1959年。[IKS+18] G´abor Ivanyos、Marek Karpinski、Miklos Santha、Nitin Saxena 和 Igor E Shparlinski。利用有限域上的高次幂进行多项式插值与恒等性测试。Algorithmica，80(2):560–575，2018年。[KL05] Tali Kaufman 和 Simon Litsyn。近乎正交的线性码具有局部可测试性。载于第46届 IEEE 计算机科学基础年会（FOCS）论文集，第317–326页。IEEE 计算机学会，2005年。[KL11] Tali Kaufman 和 Shachar Lovett。Weil 界的一个新扩展及其在特征和编码中的应用。载于Rafail Ostrovsky编，IEEE第52届计算机科学基础年会（FOCS 2011），美国加利福尼亚州棕榈泉，2011年10月22日至25日，第788–796页。IEEE 计算机学会，2011年。[Kop10] Swastik Kopparty。随机性与伪随机性中的代数方法。博士论文，麻省理工学院，剑桥，马萨诸塞州，2010年。导师：Madhu Sudan。[Kop11] Swastik Kopparty。有限域中幂运算的复杂性。载于Lance Fortnow和Salil P. Vadhan编，第43届 ACM 计算理论研讨会论文集（STOC 2011），美国加利福尼亚州圣何塞，2011年6月6日至8日，第489–498页。ACM，2011年。[Kop14] Swastik Kopparty。关于重数码的一些评论。载于《离散几何与代数组合学》，第625卷《Contemporary Mathematics》，第155–174页。美国数学会，2014年。[Kop15] Swastik Kopparty。重数码的列表解码。Theory of Computing，11(1):149–182，2015年。[KRZSW23] Swastik Kopparty、Noga Ron-Zewi、Shubhangi Saraf 和 Mary Wootters。折叠 Reed–Solomon 码与重数码的改进列表解码。SIAM Journal on Computing，52(2):515–549，2023年。

[KS07] Tali Kaufman 和 Madhu Sudan。稀疏随机线性码具有局部可解码性和局部可测试性。载于第48届 IEEE 计算机科学基础年会（ FOCS ）论文集，第 590–600 页。IEEE 计算机学会，2007 年。[KS10] Swastik Kopparty 和 Shubhangi Saraf。高错误率下随机线性码的局部列表解码与测试。载于第42届 ACM 计算理论年会（STOC）论文集，第511–520页。ACM，2010年。[KSS19] Swastik Kopparty、Ronen Shaltiel 和 Jad Silbak。适用于空间有界信道的准线性时间列表可解码码。载于第60届 IEEE 计算机科学基础年会（FOCS）论文集，第302–333页。IEEE，2019年。[KSY14] Swastik Kopparty、Shubhangi Saraf 和 Sergey Yekhanin。具有亚线性时间解码的高码率码。ACM学报（JACM），61(5):28:1–28:20，2014年。[KTSY24] Swastik Kopparty、Amnon Ta-Shma 和 Kedem Yakirevitch。迹厄米特码具有消失偏差。计算复杂性电子研讨会（ECCC），31:69，2024年。[LN97] Rudolf Lidl 和 Harald Niederreiter。有限域，第20卷《数学及其应用百科全书》。剑桥大学出版社，第2版，1997年。[Nie01] Rasmus Nielsen。代数几何码的列表解码。博士论文，丹麦技术大学，2001年。[RS04] Alexander Russell 和 Igor E Shparlinski。通过特征求值进行经典与量子函数重构。复杂性杂志，20(2-3):404–422，2004年。[RT97] Mikhail Yu. Rosenbloom 和 Michael A. Tsfasman。关于 m-度量的码。信息传输问题，33(1):45–52，1997年。[Sch76] Wolfgang M. Schmidt。有限域上的方程：初等方法，第536卷《数学讲义》。施普林格出版社，1976年。[Shp09] Amir Shpilka。低次数纠错 ε偏差生成器的构造。计算复杂性，18(4):495–525，2009年。[Sri25] Shashank Srivastava。折叠 Reed–Solomon 码的改进列表大小。载于2025年 ACM-SIAM 离散算法年会（SODA）论文集，第1560–1578页。SIAM，2025年。[Ste69] S. A. Stepanov。有限素域上超椭圆曲线的点数。《苏联数学文集》，3(5):1103–1114，1969年。将经典初等方法应用于有限域上的 Weil 界。[Ste70] S. A. Stepanov。素数模数同余理论中的初等方法。《算术学报》，17(3):231–247，1970年。对其初等方法的另一篇奠基性阐述。[Ste74] S. A. Stepanov。有限域上方程理论中的一种初等方法。载于国际数学家大会论文集，第1卷 ICM，第383–391页，1974年。会议报告总结了该技术。[Sud96] Madhu Sudan。超越纠错界的 Reed-Solomon 码解码。载于第37届 IEEE 计算机科学基础年会（FOCS）论文集，第164–172页。IEEE 计算机学会，1996年。[SV86] Karl-Otto St¨ohr 和 Jos´e Felipe Voloch。魏尔斯特拉斯点与有限域上的曲线。伦敦数学会会刊，3(1):1–19，1986年。[Tam24] Itzhak Tamo。折叠 Reed-Solomon 码和重数码的列表解码与恢复的更紧列表大小界。IEEE 信息论汇刊，70(12):8659–8668，2024年。

[Tao13] 特伦斯·陶。代数正则性引理的谱理论证明。
https://terrytao.wordpress.com/2013/10/29/a-spectral-theory-proof-of-the-algebraic-regularity-lemma/，2013年。博客文章。[Tao14] 特伦斯·陶。大特征有限域上的扩张多项式，以及可定义集的正则性引理。《数学论坛·Sigma》，2:e1，2014年。[VDHI06] Wim Van Dam、Sean Hallgren 和 Lawrence Ip。某些隐藏移位问题的量子算法。SIAM Journal on Computing，36(3):763–778，2006年。[Wei41] Andr´e Weil。函数域上的黎曼假设。《美国国家科学院院刊》，27(7):345–347，1941年。[Wei48] Andr´e Weil。关于某些指数和。《美国国家科学院院刊》，34(5):204–207，1948年。[Wei49] Andr´e Weil。有限域中方程的解的数量。《美国数学会通报》，55:497–508，1949年。

A 伪次数的代数刻画

现在我们证明伪次数的代数刻画。

引理 5.3. 设 $A(X) \in \mathbb{F}_q[X]$，并设

$$A(X) = \sum_{i \geq 0} A_i(X) \Lambda^i(X),$$

其中每个 次数$(A_i) < q$，是 $A(X)$ 的以 $\Lambda(X)$ 为底的展开。

Then

$$\mathsf{pdeg}(A) = \max_{i \geq 0} \mathsf{deg}(A_i).$$

证明。 利用 Hasse 导数的乘积法则：

$$\begin{aligned} A^{[\ell]}(X) &= \sum_{i \geq 0} \left(A_i \cdot \Lambda^i\right)^{[\ell]}(X) \\ &= \sum_{i \geq 0} \left(\sum_{\substack{\ell_0, \ell_1, \ldots, \ell_i \\ \sum \ell_j = \ell}} A_i^{[\ell_0]}(X) \cdot \prod_{j=1}^{i} \Lambda^{[\ell_j]}(X) \right) \end{aligned}$$

将这些项模 $\Lambda(X)$ 化简后，唯一保留下来的项都满足所有 ℓ_1、……、$\ell_i \in \{1, q\}$，因此 $\ell \geq i$ 和$\ell_0 \in [0, \ell - i]$。

So

$$
\begin{aligned}
A^{[\ell]}(X) \mod \Lambda(X) &= \sum_{i=0}^{\ell} \left(\sum_{\substack{\ell_1,\ldots,\ell_i \in \{1,q\} \\ \ell_0 = \ell - (\ell_1 + \ldots + \ell_i)}} A_i^{[\ell_0]}(X) \cdot \prod_{j=1}^{i} \Lambda^{[\ell_j]}(X) \right) \\
&= \sum_{i=0}^{\ell} \sum_{\ell_0=0}^{\ell-i} A_i^{[\ell_0]}(X) \cdot \left(\sum_{\substack{\ell_1,\ldots,\ell_i \in \{1,q\} \\ (\ell_1 + \ldots + \ell_i) = \ell - \ell_0}} \prod_{j=1}^{i} \Lambda^{[\ell_j]}(X) \right) \\
&= \sum_{i=0}^{\ell} \sum_{\ell_0=0}^{\ell-i} A_i^{[\ell_0]}(X) \cdot C_{i,\ell,\ell_0,q} \quad \text{for some integer } C_{i,\ell_0,\ell,q} \\
&= (-1)^{\ell} A_{\ell}(X) + \sum_{i=0}^{\ell-1} \sum_{\ell_0=0}^{\ell-i} A_i^{[\ell_0]}(X) \cdot C_{i,\ell,\ell_0,q} \quad \text{isolating the } i = \ell, \ell_0 = 0 \text{ term} \qquad (22)
\end{aligned}
$$

因此，如果所有 这些 A_i 的次数至多为 k，由此可得 $A^{[\ell]}$ 模 $\Lambda(X) = A_{\langle \ell \rangle}(X)$ 的次数至多为 k .

反过来，上述公式使我们能够将 $A_\ell(X)$ 表示为 $\pm A_{\langle \ell \rangle}(X)+$ 的线性组合，其中包含 $A_i^{[j]}$，且 $i < \ell$。对 ℓ 进行归纳可得，$\deg(A_\ell)$ 的次数至多为 $\max_{i \le \ell} \deg(A_{\langle i \rangle})$。

□

B m 次幂剩余特征标

设 q 是一个素数幂。设 m 是一个整除 $(q-1)$ 的素数。设 Γ_m 是 $\mathbb{F}_q$ 中所有 m 次单位根构成的集合。设 χ_m：$\mathbb{F}_q \to \{0\} \cup \Gamma_m$ 是由下式给出的 ($\mathbb{F}_q$ 值) m 次幂剩余特征标：$\chi_m(\alpha) = \alpha^{(q-1)/m}$。
设 $g(X)$ 是次数至多为 $d \le O_m(\epsilon \sqrt{q})$ 的首一多项式，且每个不可约因子的重数为$\in \{1, 2, \ldots, m-1\}$。

以下算法可在给定 r 的情况下，高效地找到 $g(X)$：$\mathbb{F}_q \to \{0\} \cup \Gamma_m$，其中 $\Delta(\chi \circ g,\ r)$ 不超过 q 的一个足够小的常数比例。与 $m = 2$ 的情况一样，这个译码半径低于唯一译码半径，后者约为 $\frac{1}{2}\left(1 - \frac{1}{m}\right) q$。

算法 $\mathbf{A}_m$：
参数：次数 $d \le O(\sqrt[\epsilon]{m} q)$，误差界 $e \le \left(\frac{1}{12} - \epsilon\right) q$。输入 r：
$\mathbb{F}_q \to \{0\} \cup \Gamma_m$

1. 设置
   - $M = \frac{16}{\epsilon} dm$
   - $c = \frac{M}{2}$
   - $h = 2 \cdot e.$
   - $D = d \cdot \left((q-1) \cdot \frac{m-1}{m} + M\right) + cq = (1 + O(\epsilon)) \cdot \frac{1}{2} \cdot M \cdot q,$
   - $u = h + (m-1)dM = 2e + O(\frac{md^2}{\epsilon}).$
2. 对每个 $\nu \in \{1, 2, \ldots, m-1\}$：
   - 求解 $\mathbb{F}_q$ 线性方程组，以找出多项式 $F_\nu(X) U_{\nu,\ 0}(X) \ldots, U_{\nu,\ M-1}(X) \in \mathbb{F}_q[X]$，且不全为零，并满足：

- $\deg(F_\nu) \le D$,
- for each ℓ, $\deg(U_{\nu,\ell}) \le u$,
- For all $\alpha \in \mathbb{F}_q$, $0 \le \ell < M$:

$$F_\nu^{[\ell]}(\alpha) = r^\nu(\alpha) \cdot U_{\nu,\ell}(\alpha). \tag{23}$$

3. 将 $F_\nu(X)$因式分解为不可约因子：

$$F_\nu(X) = \lambda_\nu \prod_j H^{\mu_{\nu,j}}{}^{j} X(),$$

其中，$H_j(X) \in \mathbb{F}_q[X]$ 是互不相同的首一不可约多项式，且 $\lambda \in \mathbb{F}_q^*$。

4. 对于每个 j，定义 $\mu_j \in \{0, 1, \ldots, m-1\}$ 为唯一满足以下条件的数：对于所有 $\nu \in \{1, \ldots, m-1\}$，有：

$$\mu_{\nu,j} - \frac{\nu \cdot \mu_j}{m} \cdot (q-1) \in \left(-\left(\frac{1}{12} - \epsilon\right) q, \quad \left(\frac{3}{12} - \epsilon\right) q\right) \mod q.$$

5. 令

$$f(X) = \prod_j H_j^{\mu_j}(X).$$

6. 返回 $f(X)$。

该分析与第 3 节中的分析非常相似。

令 $G(X) = g^{(q-1)/m+M}(X)$，它是一个 $(\chi_m \circ g)$-扭曲的 $(O(dM)\ M)$-伪多项式。

为证明这些线性方程有解，我们首先插值出一个高重数错误定位伪多项式 $E(X)$，满足 $\deg(E) < cq$ 且 $\mathrm{pdeg}(E) < h$。然后我们证明，取 $F_\nu = E \cdot G^\nu$ 即可得到方程组 (23) 的一个解。

接下来，我们证明算法找到的任意 F_ν 都与 G有关。与第 3 节完全相同，我们找到多项式 $A_\nu(X)\ B_\nu(X)$，满足 $\deg(A_\nu) < \frac{3}{8}Mq$、$\deg(B_\nu) < \frac{7}{8}Mq$，以及 $\mathrm{pdeg}(A_\nu) \le e$、$\mathrm{pdeg}(B_\nu) \le 3e + O(dM)$，使得：

$$A_\nu(X) \cdot F_\nu(X) = B_\nu(X) \cdot G^\nu(X).$$

根据这些方程，我们将能够提取出 $g(X)$ 的所有不可约因子。设 $H(X)$ 是一个不可约多项式，并令 μ_{A_ν}，μ_{F_ν}，μ_{B_ν}，μ_G，μ_g 分别表示它在 A_ν，F_ν，B_ν，G，g 中的因子重数。那么上述恒等式给出：

$$\mu_{A_\nu} + \mu_{F_\nu} = \mu_{B_\nu} + \nu \cdot \mu_g \cdot \frac{q-1}{m}.$$

因此，对所有 ν：

$$\mu_{F_\nu} - \nu \cdot \mu_g \cdot \frac{q-1}{m} = \mu_{B_\nu} - \mu_{A_\nu} \in q \cdot \mathbb{Z} + [-e, 3e + O(dM)] \subseteq q \cdot \mathbb{Z} + \left(-\left(\frac{1}{12} - \epsilon\right) q, \left(\frac{3}{12} - \epsilon\right) q\right).$$

因此，μ_g 是算法步骤 4 中找到的一个解。为什么不存在其他解？假设 $\mu' \in \{0, 1, \ldots, m-1\}$ 与 μ_g 不同，且满足：

$$\mu_{F_\nu} - \nu \cdot \mu' \cdot \frac{q-1}{m} \in q \cdot \mathbb{Z} + \left(-\left(\frac{1}{12} - \epsilon\right) q, \left(\frac{3}{12} - \epsilon\right) q\right)$$

对所有 ν 均成立。然后，将两个方程相减并令 $\mu'' = \mu' - \mu_g$，可得对所有 $\nu \in \{1, \ldots, m-1\}$：

$$\nu \cdot \mu'' \cdot \frac{q-1}{m} \in q \cdot \mathbb{Z} + \left(-\left(\frac{1}{3} - 2\epsilon\right) q, \left(\frac{1}{3} - 2\epsilon\right) q\right).$$

这是不可能的可能：对于任意 $\mu'' \in \{1, \ldots, m-1\}$，都存在一个 $\nu \in \{1, \ldots, m-1\}$ 使得 $\frac{\mu'' \cdot \nu}{m} \in \mathbb{Z} + \left[\frac{1}{3}, \frac{2}{3}\right]$。

C　小特征域上的加性特征 p

我们只给出第 4 节中主要子程序算法 B 的对应版本。

设 $q = p^b$，其中 p 为素数。设 Tr：$\mathbb{F}_q \to \mathbb{F}_p$ 为域迹映射。

设 $g(X)$ 为一个次数至多为 $d \le O_m(\epsilon\sqrt{q})$ 的多项式，其中仅含与 m 互素的次数的单项式。

以下算法能够根据一个 r 高效地求出 $g(X)$ 的首项系数：$\mathbb{F}_q \to \mathbb{F}_p$，其中 $\Delta(\mathrm{Tr} \circ g, r)$ 至多为 $\frac{1}{p}q$ 的一个足够小的常数比例。对于 $p = O(1)$，这是 q 的一个常数比例；但对于不断增大的 p，这一结果远不能令人满意。底层码的距离约为 $(1 - \frac{1}{p})q$（实际上，它随 p 增大而增大），因此应该存在一种能够达到该距离一半的高效唯一译码算法。–

算法 B$_p$:
参数：次数为 $d \le O_p(\epsilon\sqrt{q})$ 的多项式（p 不整除该次数），误差界为 $e \le \left(\frac{1}{4p} - \epsilon\right)q$。输入

r：$\mathbb{F}_q \to \mathbb{F}_p$

1. 令

   - $M = \frac{16}{\epsilon}d$
   - $c = \frac{1}{2} \cdot M$
   - $h = 2 \cdot e$
   - $u = h + dM = 2e + O(\frac{d^2}{\epsilon})$。

2. 对每个 $h^* \in [0, h]$

   • 尝试求解一个 $\mathbb{F}_q$ 线性方程组，以求得多项式 $E(X)$、$F(X)$、$(U_\ell(X))_{\ell \in [0, M-1]}$，其中：– $F(X)$ 的次数恰好为 $(d/p + c)q + h^*$。– $E(X)$ 的次数恰好为 $cq + h^*$，且其形式为：

$$\sum_{i=0}^{c} E_i(X)\Lambda^i(X),$$

   其中 $\deg(E_i) \le h$。

   – 每个 $U_\ell(X)$ 的次数至多为 u。

   – 对于所有 $\alpha \in \mathbb{F}_q, 0 \le \ell < M$:

$$F^{[\ell]}(\alpha) = r(\alpha) \cdot E^{[\ell]}(\alpha) + U_\ell(\alpha), \tag{24}$$

3. 如果不存在这样的 h^*，则返回 $0 \cdot X^d$。4. 否则，取一个解 $E(X)$ $F(X)$，其次数分别为 D_E，D_F。5. 令 $a \cdot X^{D_F}, b \cdot X^{D_E}$ 分别为 $F(X)$ $E(X)$ 的首项单项式。设 $a_d = (a/b)^p$。6. 返回 $a_d X^d$。

正确性证明与第 4 节中定理 4.2 的证明基本相同，故略去。