arXiv:2601.03982v1 [cs.IT] 7 Jan 2026

Uni关于超导数 Reed-Solomon 码的译码*

Haojie Gu†，Jun Zhang‡

摘要

纠错码是组合对象，旨在解决如何通过噪声信道可靠传输信息的问题。编码理论与实践中的一个基本问题，是如何高效地对含有错误的接收字进行译码，以获得传输码字。本文研究相对于 NRT 度量的超导数 Reed-Solomon（HRS）码的译码问题。具体而言，我们提出了一种用于 NRT HRS 码唯一译码的 Welch-Berlekamp 算法。

K关键词：HRS 码、MDS 码、NRT 度量、Welch-Berlekamp 算法

1 引言

设 $\mathbb{F}_q$ 是一个大小为 q、特征为 p 的有限域。设 $\mathbb{F}_q^n$ 是有限域 $\mathbb{F}_q$ 上的 n 维向量空间。纠错码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的一个子集。为了纠正传输过程中发生的错误，需要根据信道的错误类型，为空间 $\mathbb{F}_q^n$ 配备相应的度量。编码理论中的两个基本问题是：如何构造在基本参数界限意义下的最优码，以及如何高效地对含噪接收字进行译码。有时，可以将一个字写成 $\mathrm{Mat}_{r\times s}(\mathbb{F}_q)$ 中的矩阵形式；于是，文献中广泛研究了汉明度量、秩度量、 P度量等。

对于任意向量 $\boldsymbol{x}=(x_1,\ x_2,\ \cdots,\ x_n)\in\mathbb{F}_q^n$，其汉明重量 $\omega_H(\boldsymbol{x})$ 定义为 $\boldsymbol{x}$ 的非零坐标个数，即 $\omega_H(\boldsymbol{x})=|\{i\,|\,1\leqslant i\leqslant n,\, x_i\neq 0\}|$.

$[n,k,d]$-线性码 $\mathcal{C}\subseteq\mathbb{F}_q^n$ 是 $\mathbb{F}_q^n$ 的一个 k维线性子空间，其最小距离$d=d_H(\mathcal{C})$定义为

$$d_H(\mathcal{C})=\min\{\omega_H(c):c\in\mathcal{C}\backslash\{0\}\}.$$

对于任意向量 $\boldsymbol{u}\in\mathbb{F}_q^n$，从 $\boldsymbol{u}$ 到 $\mathcal{C}$ 的错误距离定义为

$$d_H(\boldsymbol{u},\mathcal{C})=\min\{d_H(\boldsymbol{u},\boldsymbol{v})\,|\,\boldsymbol{v}\in C\},$$

其中，$d_H(\boldsymbol{u},\ \boldsymbol{v})=|\{i\,|\,u_i\neq v_i,\,1\leq i\leq n\}|$ 表示向量 $\boldsymbol{u}$ 与 $\boldsymbol{v}$之间的汉明距离。众所周知的 Singleton 界指出，对于任意 $[n,k,d]$ 线性码 $\mathcal{C}$，$d\leq n-k+1$。如果 $d=n-k+1$，则 $\mathcal{C}$ 称为汉明度量下的最大距离可分（MDS）码。

定义 1.1. 令 $\mathcal{A}=\{\alpha_1,\cdots,\alpha_n\}\subseteq\mathbb{F}_q$ 为求值集，则长度为 n、维数为 k 的 ***Reed-Solomon*** 码$RS_k(\mathcal{A})$ 定义为

$$RS_k(\mathcal{A})=\{(f(\alpha_1),\cdots,f(\alpha_n)):f(x)\in\mathbb{F}_q[x],\deg(f)\leq k-1\}.$$

*本研究得到国家自然科学基金项目（批准号：12222113 和 12441105）的资助。

†Haojie Gu 就职于中国北京首都师范大学数学科学学院，邮编 100048。电子邮箱：2200502051@cnu.edu.cn。

‡Jun Zhang 任职于中国北京 100048 首都师范大学数学科学学院。电子邮箱：junz@cnu.edu.cn。

关于 Reed-Solomon 码，最基本的问题之一是其可译码性。具体而言，考虑这样一种协议：发送方选取 $\boldsymbol{c} \in RS_k(\mathcal{A})$，并通过信道发送 $\boldsymbol{c}$，接收方收到的是错误消息 $\boldsymbol{y} \in \mathbb{F}_q^n$。我们希望了解在什么情况下可以从 $\boldsymbol{y}$中恢复出 $\boldsymbol{c}$。例如，如果 $\boldsymbol{c}$与 $\boldsymbol{y}$ 之间的汉明距离不超过唯一译码半径 $\lfloor (d-1)/2 \rfloor$，Welch-Berlekamp译码器 [26]便可以高效地恢复 $\boldsymbol{c}$。

秩度量码由 Delsarte 于 1978 [4] 引入，是有限域 $\mathbb{F}_q$上由 $m \times n$ 个矩阵组成的集合。设 $\mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ 是由元素来自 $\mathbb{F}_q$的 $m \times n$ 个矩阵构成的 $\mathbb{F}_q$-向量空间。对于任意矩阵 $A \in \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$，矩阵 A 的秩重量 $\omega_R(A)$ 是矩阵 A的秩，即$\omega_R(A) = \mathrm{rank}(A)$。因此，我们可以将 $\mathbb{F}_q$上两个矩阵 A 和 B 之间的秩距离定义为 $d_R(A, B) = \omega_R(A - B)$。码 $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ 的最小秩距离为

$$d_R(\mathcal{C}) = \min\{d_R(A, B) : A \neq B \in \mathcal{C}\}.$$

对于最小秩距离为 $d_R(\mathcal{C}) \geq d$的码 $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$，秩度量中的 Singleton 界指出， $\mathcal{C}$ 中的码字数量至多为 $q^{m(n-d+1)}$，参见 [10]。达到此界的码称为最大秩距离（MRD）码。

Gabidulin码 [4, 10, 22], 是一类重要的MRD码，可以视为Reed–Solomon码的线性化版本。它们通过对线性化多项式求值来定义。从这一视角来看，Gabidulin码堪称秩度量情形下Reed-Solomon码的完美类比。

定义 1.2. 对于整数 $m \geq n \geq k$ 以及在 $\mathbb{F}_q$上线性无关的元素 α_1、 $\cdots$、 $\alpha_n \in \mathbb{F}_{q^m}$，相应的 $\mathbb{F}_{q^m}$ 上的*Gabidulin*码定义为 $[n, k]_{\mathbb{F}_{q^m}}$-线性码

$$\mathcal{G}_{n,k}(\alpha_1, \cdots, \alpha_n) = \left\{ (f(\alpha_1), \cdots, f(\alpha_n)) : f(X) = \sum_{i=1}^{k} c_i X^{q^{i-1}}, c_1, c_2, \cdots, c_k \in \mathbb{F}_{q^m} \right\} \subseteq \mathbb{F}_{q^m}^n.$$

与里德-所罗门码类似，通过推广Berlekamp-Welch算法 [13]，可以为Gabidulin码设计高效的编码和唯一译码算法。

本文讨论的Niederreiter-Rosenbloom-Tsfasman（NRT）码同样定义在矩阵空间中。NRT度量下码的研究有着悠久的平行发展历史。一个早期来源是Niederreiter的一系列论文 [15, 16, 17]。1997年，Rosenbloom和Tsfasman出于信息论方面的动机，在由 $r \times s$ 矩阵构成的 $\mathbb{F}_q$-向量空间中引入了一种新度量 [21]。此后，围绕该度量的编码理论问题得到了研究，包括MDS码 [5, 7, 23], 、MacWilliams对偶性 [6, 18], 、线性码的结构与译码 [19, 20, 25], 、覆盖 [3]等。对这些度量空间的研究也受到单位立方体中点分布问题的推动（例如参见 [1, 5, 23]）。后来人们发现，这种矩阵度量对应于一种 P-度量，其中 P 是 s长度的 r 条链的并集。

引入 NRT 度量后，编码理论中的一个基本问题是：固定维数 k 和长度 n 时，如何在 NRT 度量下使最小距离最大化。在 [21],Rosenbloom 和 Tsfasman 得到了 NRT 度量下的 Singleton 界。有趣的是，作为 RS 码的一种扩展，超导数 Reed-Solomon（HRS）码能够达到 NRT 度量下的 Singleton 界，后文将介绍这一点。令人惊讶的是，HRS 码无法达到汉明度量下的 Singleton 界。与汉明度量下的 RS 码类似，我们自然会关注 NRT 度量下 HRS 码的译码问题。本文特别介绍 Welch-Berlekamp 算法，这是一种针对 NRT 度量下 HRS 码的唯一译码算法。

本文结构如下。第 2 节介绍基本对象，包括超导数和 NRT 度量。第 3 节针对 NRT HRS码的唯一译码，将 RS 码在汉明度量下使用的 Welch-Berlekamp 算法扩展到 NRT 度量下。

2 预备知识与符号

2.1 超导数

令 $\mathcal{P}(t-1)$ 表示次数至多为 $t-1$ 的多项式 $f(X) \in \mathbb{F}_q[X]$ 所构成的空间。以下定义有时也称为 Hasse 导数；不过，我们将严格称其为超导数，这一术语由 Skriganov 在 [23]中使用，并且也见于 Niederreiter 和 Lidl 的教材 [14]。

定义 2.1. 设 t 为正整数。给定 $f(x) \in \mathcal{P}(t-1)$，其形式为 $f(x) = f_0 + f_1 x + \cdots + f_{t-1}x^{t-1}$。设 $j < p$，则 $f(x)$ 的 j 阶超导数定义为下列多项式：

$$\partial^{(j)} f(x) = \binom{0}{j} f_0 x^{-j} + \binom{1}{j} f_1 x^{1-j} + \cdots + \binom{t-1}{j} f_{t-1} x^{t-1-j}, \tag{1}$$

其中约定，若 $0 \le j \le i$; 0，则 $\binom{i}{j} = \begin{cases} \frac{i!}{(i-j)!\,j!}, & \text{；否则，} \end{cases}$

对于 $\alpha \in \mathbb{F}_q$，我们用 $\nu_f(\alpha)$ 表示 $f(x)$ 在 α 处的消失阶。这意味着，整除 $f(x)$ 的 $(x-\alpha)$ 的最高次幂为 $\nu_f(\alpha)$。换句话说，对于某个多项式 $g(x)$，我们有 $f(x) = (x-\alpha)^{\nu_f(\alpha)} g(x)$，且 $g(\alpha) \neq 0$。

我们指出这个展开的两个直接推论。
(1) 对所有 $m \in \mathbb{N}$，我们有

$$\nu_f(u) = m \iff \partial^{(j)} f(u) = 0 \text{ for all } j \in \{0, 1, \ldots, m-1\} \text{ but } \partial^{(m)} f(u) \neq 0.$$

(2) 对任意整数 $a > \deg(f(x))$，我们有

$$\partial^{(a)} f(x) = 0.$$

引理 2.2 ([8])。对于任意 $A(X)\ B(X) \in \mathbb{F}_q[X]$ 和 $\ell \ge 0$，我们有

$$\partial^{(\ell)}(A(X)B(X)) = \sum_{i=0}^{\ell} \partial^{(i)} A(X) \partial^{(\ell-i)} B(X).$$

给定 $\mathcal{A} = \{\alpha_1, \cdots, \alpha_r\} \subseteq \mathbb{F}_q$ 和 $\boldsymbol{y} = (y_{i,j})_{1 \le j \le r}^{1 \le i \le s} \in \mathrm{Mat}_{s \times r}(\mathbb{F}_q)$，我们将 Hermite 插值 $H(X; \mathcal{A}, \boldsymbol{y})$ 定义为满足以下条件的最低次数多项式 $H(X)$

$$\partial^{(i-1)} H(\alpha_j) = y_{i,j}$$

对于所有 $1 \le i \le s$，$1 \le j \le r$。注意，Hermite 插值是 Lagrange 插值的扩展。Von Zur Gathen 和 Gerhard [24] 提出了 Hermite 插值的一种快速实现。

记 $M(n)$ 为乘两个次数为 n 的多项式所需的最少算术运算次数。若基域支持快速傅里叶变换，则 $M(n) \le O(n \log n)$；否则 $M(n) \le O(n \log n \log\log n)$ [24, 定理 8.18，定理 8.22]。

定理 *2.3*（[24]）。设 r, s 为满足 $s \leq p$, $\mathcal{A} = \{\alpha_1, \cdots, \alpha_r\} \subseteq \mathbb{F}_q$ 和 $\boldsymbol{y} = (y_{i,j})_{1 \leq i \leq s}^{1 \leq j \leq r} \in Mat_{s \times r}(\mathbb{F}_q)$ 的正整数。存在唯一的多项式 $H(X) \in \mathcal{P}(rs-1)$，使得对所有 $1 \leq i \leq r, 1 \leq j \leq s$，均有 $\partial^{(j-1)} H(\alpha_i) = y_{j,i}$。此外，$H(X; \mathcal{A}, \boldsymbol{y})$ 可在时间 $O(M(sr)\log(sr))$ 内计算。

2.2 NRT 度量

从历史上看，Brualdi 等人在 [2]中引入了偏序集度量（P-度量）的概念。关于 P-度量的更多背景和发展，可参见 [9] 和 [23]。作为 P-度量的一种特殊情形，Niederreiter 首先在其 1987年论文 [15], 中引入了 NRT 度量，并在均匀分布的欧几里得空间点分布这一背景下对其进行了研究。随后，Rosenbloom 和 Tsfasman 在其工作 [21], 中独立地应用了这一度量，并称之为 m-度量，且正式将其引入编码理论。

设 r 和 s 为正整数。$Mat_{s \times r}(\mathbb{F}_q)$ 上的 NRT 度量定义如下。

设 $A := (a_{ij})_{i=1, \ldots, s, \ j=1 \ldots r} \in Mat_{s \times r}(\mathbb{F}_q)$。设 $A_1, \ldots, A_r$ 表示 A 的各列。列 A_j 的 NRT 权重记作 $\omega_N(A_j)$，定义为

$$\begin{cases} s - i + 1, & if \ A_j \neq \mathbf{0} \\ 0, & if \ A_j = \mathbf{0} \end{cases},$$

其中，i 是从上到下看时，A_j 中第一个非零项的索引。于是，矩阵 A的 NRT 权重记为 $\omega_N(A)$，定义为 A所有列的 NRT 权重之和。也就是说，

$$\omega_N(A) = \omega_N(A_1) + \cdots + \omega_N(A_r).$$

接下来，矩阵 A 和 B 之间的 NRT 距离定义为

$$d_N(A, B) = \omega_N(A - B).$$

在 [2], 中，Brualdi等人证明了 P-距离实际上是 $\mathbb{F}_q^n$上的一种度量。因此，容易验证，NRT 距离是 $Mat_{s \times r}(\mathbb{F}_q)$ 上的一种度量。

使用 NRT 度量（而非汉明度量）的码称为 NRT 码。在 NRT 度量下，最小距离也有相应的定义。设 $\mathcal{C}$ 是 $Mat_{s \times r}(\mathbb{F}_q)$ 的一个子集。用 $d_N(\mathcal{C})$表示 $\omega_N(V - W)$的最小非零权重，其中 $V \neq W \in \mathcal{C}$。NRT 度量下也有类似的 Singleton 界 [12] ，如下所示:

$$|\mathcal{C}| \leq q^{n - d_N(\mathcal{C}) + 1}.$$

特别地，如果 $\mathcal{C}$ 是线性 $[rs, t]$ NRT 码，则有

$$d_N(\mathcal{C}) \leq rs - t + 1.$$

我们将线性 NRT 码称为 $[rs, t, d_N]$ 码。如果 $d_N = rs - t + 1$，则称此码为 MDS NRT 度量码。

2.3 超导数 Reed-Solomon 码

设正整数 r、s 和 t 满足 $s \leq p$、$r \leq q$ 以及 $t \leq rs$。该构造基于一个 r元组 $\mathcal{A} = (\alpha_1$、$\cdots$、$\alpha_r)$，称为求值点；以及一个 $s \times r$ 矩阵 $V = (v_{ij})_{i=1, \cdots, j=1 \cdots \ r, \ s,}$

其元素属于 $\mathbb{F}_q^*$，称为乘子矩阵。超导数 Reed-Solomon（HRS）码记作 $HRS(\mathcal{A}、V、t-1)$，定义为下列求值映射的像：

$$EV_{\mathcal{A},V}:\mathcal{P}(t-1)\to \mathrm{Mat}_{s\times r}(\mathbb{F}_q)$$
$$f(z)\mapsto \begin{pmatrix} v_{1,1}\partial^{(0)}f(\alpha_1) & v_{1,2}\partial^{(0)}f(\alpha_2) & \cdots & v_{1,r}\partial^{(0)}f(\alpha_r)\\ v_{2,1}\partial^{(1)}f(\alpha_1) & v_{2,2}\partial^{(1)}f(\alpha_2) & \cdots & v_{2,r}\partial^{(1)}f(\alpha_r)\\ \vdots & \vdots & \vdots & \vdots\\ v_{s,1}\partial^{(s-1)}f(\alpha_1) & v_{s,2}\partial^{(s-1)}f(\alpha_2) & \cdots & v_{s,r}\partial^{(s-1)}f(\alpha_r)\end{pmatrix},$$

其中 $\partial^{(i)}f$ 表示 f 的第 i 阶超导数。

当乘子矩阵 V 为全 1 矩阵时，该定义最早由 Rosenbloom 和 Tsfasman 在其开创性论文 [21] 中提出。

接下来，我们给出任意 $s\le p$ 下码字 $EV_{\mathcal{A},V}(f)\in \mathrm{Mat}_{s\times r}(\mathbb{F}_q)$ 的 NRT 权重公式。

引理 2.4 ([23])。设 A 表示矩阵 $EV_{\mathcal{A},V}(f)$，其中 $f\in\mathcal{P}(t-1)$。设 A_j 表示 A 的第 j 列，则 A_j 的 *NRT* 权重为

$$\omega_N(A_j)=s-\nu_f(\alpha_j).$$

因此，矩阵 A 的 *NRT* 权重为

$$\omega_N(EV_{\mathcal{A},V}(f))=\sum_{j=1}^{r}(s-\nu_f(\alpha_j))=sr-\sum_{j=1}^{r}\nu_f(\alpha_j).$$

已有结果表明，HRS 码在 NRT 度量下是 MDS 码。

定理 2.5 ([23])。设 $\mathcal{A}=\{\alpha_1,\cdots,\alpha_r\}\subseteq\mathbb{F}_q$ 是 $\mathbb{F}_q$ 中的一个由 r 个互不相同元素组成的集合，且 $V\in(\mathbb{F}_q^*)^{s\times r}$。则 *HRS* 码 $HRS(\mathcal{A},V,t-1)$ 是一个 t 维 *MDS NRT* 度量码。

3 NRT HRS 码的 Welch-Berlekamp 算法

考虑具有求值点 $\mathcal{A}=\{\alpha_1,\cdots,\alpha_r\}$ 和 $s\times r$ 矩阵 $V=\mathbf{1}_{s\times r}$ 的 $[sr,t,d=sr-t+1]_q$ NRT HRS 码。设 $EV_{\mathcal{A},\mathbf{1}}(P(X))$ 为传输码字，$\boldsymbol{y}=(y_{i,j})_{1\le j\le r}^{1\le i\le s}\in \mathrm{Mat}_{s\times r}(\mathbb{F}_q)$ 为接收字，其中 $P(X)\in\mathcal{P}(t-1)$。基本问题是如何恢复与接收向量 $\boldsymbol{y}$ 最接近的正确码字 $EV_{\mathcal{A},\mathbf{1}}(P(X))$，或一个码字 $EV_{\mathcal{A},\mathbf{1}}(Q(X))$。本文的主要结果是给出一种译码算法（算法1），该算法将 RS 码在汉明度量下的 Welch-Berlekamp 算法扩展到 NRT 度量下的 HRS 码，并能在多项式时间内纠正最多 $e<\frac{rs-t+1}{2}$ 个错误。我们将算法1称为 NRT HRS 码的 Welch-Berlekamp 算法。需要指出的是，当 $s=1$ 时，我们的算法退化为原始的 RS 码 Welch-Berlekamp 算法。

在验证 NRT HRS 码的 Welch-Berlekamp 算法的正确性之前，我们先举一个例子来说明该算法。

例 3.1. 令 $r=4$、$s=2$、$t=4$、$e\le\lfloor\frac{rs-t}{2}\rfloor=2$。令 $q=7$、$\mathcal{A}=\{1,2,3,4\}\subseteq\mathbb{F}_7$。选择一个多项式 $P(X)=X^3+3X^2+2X+5\in\mathcal{P}(3)$，它给出码字

$$EV_{\mathcal{A},\mathbf{1}}(P(X))=\begin{pmatrix}P(1)&P(2)&P(3)&P(4)\\ \partial^{(1)}P(1)&\partial^{(1)}P(2)&\partial^{(1)}P(3)&\partial^{(1)}P(4)\end{pmatrix}=\begin{pmatrix}4&1&2&6\\4&5&5&4\end{pmatrix}.$$

算法1： NRT HRS 码的 Welch-Berlekamp 算法

输入： r，$s \geq 1$，$1 \leq t \leq rs$，$0 < e < \frac{rs-t+1}{2}$，r 子集 $\mathcal{A} = \{\alpha_1, \cdots, \alpha_r\}$，$\boldsymbol{y} = (y_{i,\ j}) \in \mathrm{Mat}_{s \times r}(\mathbb{F}_q)$**输出：** 次数至多为 $t-1$ 的多项式 $P(X)$，否则失败

1 计算一个次数恰为 e 的非零多项式 $E(X)$，以及一个次数至多为 $e+t-1$ 的多项式 $N(X)$，使得对于所有 $1 \leq i \leq r$，都有

$$\begin{cases} N(\alpha_i) = & y_{1,i}E(\alpha_i) \\ \partial^{(1)}N(\alpha_i) = & \sum_{j=1}^{2} y_{j,i}\partial^{(2-j)}E(\alpha_i) \\ & \vdots \\ \partial^{(s-1)}N(\alpha_i) = & \sum_{j=1}^{s} y_{j,i}\partial^{(s-j)}E(\alpha_i) \end{cases} \tag{2}$$

2 如果上述 E(X) 和 N(X) 不存在，或者 E(X) 不能整除 N(X)，则 3 返回失败 4 结束5 $P(X) \leftarrow N(X)/E(X)$ **6 如果** $\omega_N(EV_{\mathcal{A}}, \mathbf{1}(P(X)) - \boldsymbol{y}) > e$ **则 7 返回失败 8 结束 9 否则，如果** $\omega_N(EV_{\mathcal{A}}, \mathbf{1}(P(X)) - \boldsymbol{y}) \leq e$ **则 10 返回** $P(X)$ **11 结束**

假设发生了以下 *NRT* 权重为2 的错误

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

因此，接收字为

$$\boldsymbol{y} = \begin{pmatrix} 4 & 1 & 2 & 6 \\ 5 & 5 & 6 & 4 \end{pmatrix}.$$

令 $N(X) = a_0 + a_1X + a_2X^2 + a_3X^2 + a_4X^4 + a_5X^5$ 和 $E(X) = b_0 + b_1X + X^2$。根据算法*1*的公式*(2)*，我们有

$$\begin{cases} \sum_{j=0}^{5} a_j\alpha_i^j - y_{1,i}b_0 - y_{1,i}\alpha_i b_1 = y_{1,i}\alpha_i^2, & i = 1,2,3,4 \\ \sum_{j=1}^{5} j a_j\alpha_i^{j-1} - y_{2,i}b_0 - (y_{1,i} + y_{2,i}\alpha_i)b_1 = 2y_{1,i}\alpha_i + y_{2,i}\alpha_i^2, & i = 1,2,3,4 \end{cases}.$$

换句话说，我们有以下线性方程组：

$$M\boldsymbol{x} = A,$$

其中 $\boldsymbol{x} = (a_0, a_1, \cdots, a_5, b_0, b_1)^T, A = (4、4、4、5、6、3、3、0)^T$以及

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 3 & 3 \\ 1 & 2 & 4 & 1 & 2 & 4 & 6 & 5 \\ 1 & 3 & 2 & 6 & 4 & 5 & 5 & 1 \\ 1 & 4 & 2 & 1 & 4 & 2 & 1 & 4 \\ 0 & 1 & 2 & 3 & 4 & 5 & 2 & 5 \\ 0 & 1 & 4 & 5 & 4 & 3 & 2 & 3 \\ 0 & 1 & 6 & 6 & 3 & 6 & 1 & 1 \\ 0 & 1 & 1 & 6 & 4 & 6 & 3 & 6 \end{pmatrix}$$

通过求解 方程组，我们得到解 $\boldsymbol{x} = (1,\ 0,\ 6,\ 0,\ 6,\ 1,\ 3,\ 3)^T$。因此 ,

$$N(X) = X^5 + 6X^4 + 6X^2 + 1 \quad and \quad E(X) = X^2 + 3X + 3.$$

容易验证， $E(X) \mid N(X)$。因此，算法*1*返回

$$P(X) = \frac{N(X)}{E(X)} = X^3 + 3X^2 + 2X + 5.$$

最后，我们得到传输码字

$$EV_{\mathcal{A},\mathbf{1}}(P(X)) = \begin{pmatrix} P(1) & P(2) & P(3) & P(4) \\ \partial^{(1)}P(1) & \partial^{(1)}P(2) & \partial^{(1)}P(3) & \partial^{(1)}P(4) \end{pmatrix} = \begin{pmatrix} 4 & 1 & 2 & 6 \\ 4 & 5 & 5 & 4 \end{pmatrix}.$$

因此，算法*1*确实恢复出了正确码字。

接下来，我们证明所提出的 NRT HRS 码的 Welch-Berlekamp 算法的正确性。

引理 3.2. 存在一对多项式 $E_1(X)$ 和 $N_1(X)$ ，满足步骤 *1*，使得$N_1(X) = E_1(X)P(X)$。

证明。 根据定理 2.3，存在一个多项式 $H(X) \in \mathcal{P}(rs-1)$，使得 $H(X) = H(X; \mathcal{A}, \boldsymbol{y})$。令 $Q(X) = P(X) - H(X)$。记

$$E_1(X) = X^{e-\Delta} \prod_{1 \le i \le r} (x - \alpha_i)^{s - \nu_Q(\alpha_i)}, \tag{3}$$

其中 $\Delta = \omega_N(EV_{\mathcal{A},\mathbf{1}}(Q(X)))$。令 $N_1(X) = E_1(X)P(X)$，则 $\deg(E_1(X)) = e$且

$$\deg(N_1(X)) = \deg(E_1(X)) + \deg(P(X)) \le e + t - 1.$$

对于 $1 \le i \le r$，若 $1 \le j \le \nu_Q(\alpha_i)$，则 $(X - \alpha_i)^j | Q(X)$。因此

$$\partial^{(j-1)}(P(\alpha_i)) = \partial^{(j-1)}H(\alpha_i) = y_{j,i}.$$

若 $\nu_Q(\alpha_i) < j \le s$，则 $s - j < s - \nu_Q(\alpha_i)$。因此,

$$\partial^{(s-j)}E_1(\alpha_i) = 0.$$

总而言之，对于所有的 $1 \le i \le r, 1 \le j \le s$，我们有

$$(y_{j,i} - \partial^{(j-1)}P(\alpha_i)) \cdot \partial^{(s-j)}E_1(\alpha_i) = 0.$$

So

$$y_{j,i} \cdot \partial^{(s-j)} E_1(\alpha_i) = \partial^{(j-1)} P(\alpha_i) \cdot \partial^{(s-j)} E_1(\alpha_i)$$

and

$$\sum_{j=1}^{s} y_{j,i} \partial^{(s-j)} E_1(\alpha_i) = \sum_{j=1}^{s} \partial^{(j-1)} P(\alpha_i) \cdot \partial^{(s-j)} E_1(\alpha_i).$$

根据引理 2.2，我们有

$$\sum_{j=1}^{s} y_{j,i} \partial^{(s-j)} E_1(\alpha_i) = \partial^{(s-1)}(P(\alpha_i) \cdot E_1(\alpha_i)) = \partial^{(s-1)} N_1(\alpha_i).$$

类似地，对于所有 $1 \le \ell \le s-1$，$1 \le i \le r$，$1 \le j \le s-\ell$，我们有

$$(y_{j,i} - \partial^{(j-1)} P(\alpha_i)) \cdot \partial^{(s-\ell-j)} E_1(\alpha_i) = 0.$$

因此，

$$\sum_{j=1}^{s-\ell} y_{j,i} \partial^{(s-\ell-j)} E_1(\alpha_i) = \sum_{j=1}^{s-\ell} \partial^{(j-1)} P(\alpha_i) \cdot \partial^{(s-\ell-j)} E_1(\alpha_i) = \partial^{(s-\ell-1)} N_1(\alpha_i).$$

□

注意到，现在只需论证：对于满足步骤 1 的任意一对解 $(N_1(X)\ E_1(X))$ 和 $(N_2(X)\ E_2(X))$，$\frac{N_1(X)}{E_1(X)} = \frac{N_2(X)}{E_2(X)}$。然后根据引理 3.2，该比值必为 $P(X)$。

引理 3.3。步骤 *1* 中的任意两个不同解 $(E_1(X)\ N_1(X) \neq (E_2(X)\ N_2(X))$ 满足 $\frac{N_1(X)}{E_1(X)} = \frac{N_2(X)}{E_2(X)}$。

证明。根据定理 2.3，存在一个多项式 $H(X) \in \mathcal{P}(rs-1)$，使得 $H(X) = H(X; \mathcal{A}, \boldsymbol{y})$。由于 $(N_1(X)\ E_1(X)$ 和 $(N_2(X)\ E_2(X))$ 满足步骤 1，我们有

$$\partial^{(\ell-1)} N_k(\alpha_i) = \sum_{j=1}^{\ell} y_{j,i} \partial^{(\ell-j)} E_k(\alpha_i)$$

对所有 $1 \le \ell \le s, 1 \le i \le r$ 和 $k = 1,2$。

设 $F(X) = N_1(X)E_2(X) - N_2(X)E_1(X)$。对于 $1 \le i \le r$ 和 $1 \le j \le s$，我们有

$$\begin{aligned}
\partial^{(j-1)} F(\alpha_i) &= \partial^{(j-1)}(N_1(\alpha_i)E_2(\alpha_i) - N_2(\alpha_i)E_1(\alpha_i)) \\
&= \sum_{\ell=1}^{j} \partial^{(\ell-1)} N_1(\alpha_i) \partial^{(j-\ell)} E_2(\alpha_i) - \sum_{\ell=1}^{j} \partial^{(\ell-1)} N_2(\alpha_i) \partial^{(j-\ell)} E_1(\alpha_i) \\
&= \sum_{\ell=1}^{j} \sum_{k=1}^{\ell} y_{k,i} \partial^{(\ell-k)} E_1(\alpha_i) \partial^{(j-\ell)} E_2(\alpha_i) - \sum_{\ell=1}^{j} \sum_{k=1}^{\ell} y_{k,i} \partial^{(\ell-k)} E_2(\alpha_i) \partial^{(j-\ell)} E_1(\alpha_i) \\
&= \sum_{k=1}^{j} y_{k,i} \sum_{\ell=k}^{j} \partial^{(\ell-k)} E_1(\alpha_i) \partial^{(j-\ell)} E_2(\alpha_i) - \sum_{k=1}^{j} y_{k,i} \sum_{\ell=k}^{j} \partial^{(\ell-k)} E_2(\alpha_i) \partial^{(j-\ell)} E_1(\alpha_i) \\
&= \sum_{k=1}^{j} y_{k,i} \partial^{(j-k)} \left(E_1(\alpha_i) E_2(\alpha_i)\right) - \sum_{k=1}^{j} y_{k,i} \partial^{(j-k)} \left(E_1(\alpha_i) E_2(\alpha_i)\right) = 0.
\end{aligned}$$

So

$$\prod_{1\le i\le r}(X-\alpha_i)^s \mid F(X).$$

但是， $F(X)$ 的次数满足 $\deg(F(X)) \le e+e+t-1 < rs$。因此， $F(X) = 0$ 是零多项式。于是，

$$\frac{N_1(X)}{E_1(X)} = \frac{N_2(X)}{E_2(X)}.$$

□

根据引理 3.2 和引理 3.3，我们知道，如果算法1没有输出“失败”，那么该算法就会给出正确的输出。

现在，我们分析算法1的运行时间。在步骤 1 中， $N(X)$ 有 $e+t$ 个未知数，而 $E(X)$ 有 $e+1$ 个未知数。对于每个 $1 \le i \le r$，式 (2) 中的约束是在这些未知数上含有 r 个方程的线性方程组。因此，我们得到一个含有 rs 个线性方程、$2e+t+1 < rs+2$ 个未知数的方程组。根据引理 3.2，该方程组有解。唯一的额外要求是，多项式 $E(X)$ 的次数恰好为 e。我们已经证明，式 (3) 中的 $E(X)$ 满足这一要求。因此，我们添加一个约束，要求 $E(X)$ 中 X^e 的系数为 1。于是，我们得到 $rs+1$ 个线性方程，至多含有 $rs+1$ 个变量，可以在 $O(r^3s^3)$ 时间内求解，例如使用高斯消元。最后请注意，步骤 5 可以通过“多项式长除法”在 $O(r^3s^3)$ 时间内实现。由此，我们得到以下主要定理。

定理 *3.4*。如果传输了 $EV_{\mathcal{A},1}(P(X)) \in Mat_{s\times r}(\mathbb{F}_q)$，且接收字 $\boldsymbol{y} \in Mat_{s\times r}(\mathbb{F}_q)$ 中至多出现 $e \le \frac{rs-t}{2}$ 个错误，即 $\omega_{C(s,r)}(\boldsymbol{y} - EV_{\mathcal{A},1}(P(X))) \le e$，其中 $P(X)$ 是次数至多为 $t-1$ 的多项式，则 *Welch-Berlekamp* 算法输出 $P(X)$。此外，*Welch-Berlekamp* 算法可在 $O(r^3s^3)$ 时间内完成。

4 结论

本文研究了 NRT HRS码的译码问题。我们提出了一种用于 NRT HRS码唯一译码的 Welch-Berkamp 算法，该算法能够在多项式时间内纠正 NRT 度量下不超过唯一译码半径的错误。最后，我们指出，本文提出的 Welch-Berkamp 算法可以扩展为适用于 NRT HRS码的列表译码器 [11]。

参考文献

[1] Alexander Barg 和 Punarbasu Purkayastha。有序码与正交数组的界。载于*2007*年 *IEEE* 信息论国际研讨会，第 331–335 页。IEEE，2007年。[2] Richard A Brualdi、Janine Smolin Graves 和 K Mark Lawrence。具有偏序集度量的码。离散数学，147(1-3)：57–72，1995年。[3] Andr´e G Castoldi 和 Emerson L Monte Carmelo。罗森布鲁姆–茨法斯曼空间中的覆盖问题。电子组合学杂志，22(3)：P3.30，2015年。[4] Ph Delsarte。有限域上的双线性形式及其在编码理论中的应用。组合论杂志 *A*辑，25(3)：226–241，1978年。[5] Steven T Dougherty 和 Keisuke Shiromoto。具有非汉明度量和均匀分布的 $\mathrm{Mat}_{n,\,s}(z_k)$ 中的最大距离码。设计、编码与密码学，33：45–61，2004年。

[6]Steven T Dougherty 和 Maxim Mikhailovich Skriganov。MacWilliams对偶性与罗森布鲁姆–茨法斯曼度量。莫斯科数学杂志，2(1)：81–97，2002年。[7] Steven T Dougherty 和 Maxim Mikhailovich Skriganov。任意字母表上的 ρ 度量中的最大距离可分码。代数组合学杂志，16：71–81，2002年。[8] 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*计算杂志，42(6)：2305–2328，2013年。[9] Marcelo Firer、Marcelo Muniz S Alves、Jerry Anderson Pinheiro 和 Luciano Panek。偏序集码：偏序、度量与编码理论。施普林格，2018年。[10] Ernest Mukhamedovich Gabidulin。最大秩距离码理论。信息传输问题，21(1)：3–16，1985年。[11] Haojie Gu 和 Jun Zhang。超导数 Reed-Solomon 码的列表译码。准备中。[12] Jong Yoon Hyun 和 Hyun Kwang Kim。最大距离可分偏序集码。设计、编码与密码学，48(3)：247–261，2008年。[13] Ralf Koetter 和 Frank R Kschischang。随机网络编码中的错误与擦除编码。*IEEE*信息论汇刊，54(8)：3579–3591，2008年。[14] Rudolf Lidl 和 Harald Niederreiter。有限域。第20卷。剑桥大学出版社，1997年。[15] Harald Niederreiter。差异度小的点集与序列。数学月刊¨，104：273–337，1987年。[16] Harald Niederreiter。有限域上向量空间的一个组合问题。离散数学，96(3)：221–228，1991年。[17] Harald Niederreiter。单位立方体中均匀点分布理论里的正交数组及其他组合方面。离散数学，106：361–367，1992年。[18] Mehmet Ozen、Minjia Shi 和 Vedat Siap。有限交换 Frobenius 环上的 m-spotty 罗森布鲁姆–茨法斯曼重量枚举式之间的一个恒等式。韩国数学会会刊，52(3)：809–823，2015年。[19] Mehmet Ozen 和 Irfan Siap。关于罗森布鲁姆–茨法斯曼度量的线性码。设计、编码与密码学，38(1)：17–29，2006年。[20] Luciano Panek、Marcelo Firer 和 Marcelo Muniz Silva Alves。Niederreiter–Rosenbloom–Tsfasman分组码的分类。*IEEE*信息论汇刊，56(10)：5207–5216，2010年。[21] M Yu Rosenbloom 和 Michael Anatol'evich Tsfasman。 m度量下的码。信息传输问题，33(1)：55–63，1997年。[22] Ron M Roth。最大秩阵码及其在交叉错误纠正中的应用。*IEEE*信息论汇刊，37(2)：328–336，2002年。

[23] Maxim Mikhailovich Skriganov。编码理论与均匀分布。代数与分析，13(2):191，2001年。[24] 约阿希姆·冯·楚尔·加滕和J¨urgen Gerhard。现代计算机代数。剑桥大学出版社，2003年。[25] 王欣然、李成举和衡子玲。罗森布鲁姆–茨法斯曼度量下线性矩阵码的新界与最优构造。*IEEE*信息论汇刊，2025年。[26] 劳埃德·R·韦尔奇和埃尔温·R·伯勒坎普。代数分组码的纠错。载于美国专利*4,633,470*。*1986*年*12*月*30*日。