关于本原射影 Reed-Solomon 码的深洞

徐小凡, 洪绍方*, 许永超

四川大学数学学院, 成都 610064

E-mail: xxfscu@163.com, sfhong@scu.edu.cn, xyongchao@hotmail.com

收稿日期: 2017-04-07; 接受日期: 2018-03-19; 网络出版日期: 2018-07-11; * 通信作者

国家自然科学基金 (批准号: 11771304) 和四川省教育厅自然科学基金 (批准号: 2016ZB0342) 资助项目

摘要 本原射影 Reed-Solomon 码是数字通信领域中一类重要的极大距离可分码. 在本原射影 Reed-Solomon 码的译码过程中, 人们通常采用极大似然译码算法. 对于一个收到的向量 $\mathbf{u} \in \mathbb{F}_q^n$, 极大似然译码算法关键在于确定向量 $\mathbf{u}$ 关于码 C 的错误距离 $d(\mathbf{u}, C)$. 熟知 $d(\mathbf{u}, C) \leq \rho(C)$, 其中 $\rho(C)$ 为码 C 的覆盖半径. 若 $d(\mathbf{u}, C) = \rho(C)$, 则称 $\mathbf{u}$ 为码 C 的深洞. 本文得到了本原射影 Reed-Solomon 码 $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的一类深洞. 实际上, 利用有限域 $\mathbb{F}_q$ 上极大距离可分码的生成矩阵, 本文证明如下结果成立: 如果 $q \geq 4$, 整数 k 满足 $2 \leq k \leq q-2$, 收到的向量 $\mathbf{u}$ 的前 $q-1$ 个分量的 Lagrange 插值多项式为 $u(x) = \lambda x^{q-2} + f_{\leq k-2}(x)$, 其中 $\lambda \in \mathbb{F}_q^*$, $f_{\leq k-2}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-2$ 的多项式, 并且 $\mathbf{u}$ 的第 q 个分量为 0, 那么 $\mathbf{u}$ 是本原射影 Reed-Solomon 码 $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的一个深洞.

关键词 本原射影 Reed-Solomon 码 MDS (maximum distance separable) 码 深洞

MSC (2010) 主题分类 94B35, 11C08

1 引言

在 1960 年, 作为 MIT (Massachusetts Institute of Technology) 林肯实验室成员的 Irving Stoy Reed 和 Gustave Solomon 提出了一种基于多项式的纠错编码, 即所谓的 Reed-Solomon 码 (以后均简记为 RS 码). 由于 RS 码为极大距离可分码, 即极小距离可达到 Singleton 界, 而且 RS 码是循环码的一种特殊情形, 它能够高效地进行编码, 尤其是针对本原 RS 码的软件实现非常方便, 且 RS 码能够很好地被译码, 因此, RS 码在数字通信领域中的实际应用十分广泛. 1977 年发射的“旅行者一号”和“旅行者二号”空间探测器就使用了 RS 码向地球传回了土星和天王星等天体的宝贵天文图片. 在 RS 码的研究中, 一个重要问题是, 在采用极大似然译码算法时, 对于收到的向量 $\mathbf{u}$, 确定其错误距离 $d(\mathbf{u}, C)$, 而错误距离问题主要在于确定其上下界, 达到上界即深洞问题^[1]. 在 2007 年, Cheng 和 Murry^[2] 猜想本原 RS 码的深洞只有向量 $\mathbf{u}$ 的 Lagrange 插值多项式 $u(x)$ 为 $ax^k + f_{\leq k-1}(x)$ 的情形. 在 2012 年, Wu 和 Hong^[3] 通过对 $\mathbb{F}_q$ 上的向量进行离散 Fourier 变换, 利用循环码的一些结论, 证明了当收到的向量 $\mathbf{u}$

英文引用格式: Xu X F, Hong S F, Xu Y C. On deep holes of primitive projective Reed-Solomon codes (in Chinese). Sci Sin Math, 2018, 48: 1087–1094, doi: 10.1360/N012017-00064

的 Lagrange 插值多项式 $u(x)$ 为 $ax^{q-2} + f_{\leq k-1}(x)$ 时, $\mathbf{u}$ 是本原 RS 码的深洞. 进一步地, Wu 和 Hong 猜想收到的向量 $\mathbf{u}$ 为本原 RS 码的深洞当且仅当其 Lagrange 插值多项式 $u(x)$ 为 $ax^k + f_{\leq k-1}(x)$ 或 $ax^{q-2} + f_{\leq k-1}(x)$, 其中 $a \in \mathbb{F}_q^*$, $f_{\leq k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式. 紧接着, 在 2016 年, Hong 和 Wu^[4] 证明了, 当 $a_j \in \mathbb{F}_q \setminus \{a_1, \dots, a_l\}$ 时, $a(x - a_j)^{q-2} + f_{\leq k-1}(x)$ 为广义 RS 码的深洞. 同时, Zhang 和 Wan^[5] 通过对有限域上子集合问题的求解, 证明了 $ax^k + f_{\leq k-1}(x)$ 为射影 RS 码的深洞, 其中 $a \in \mathbb{F}_q^*$, $f_{\leq k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式. 关于编码方面的一些基础知识, 读者可参见万哲先先生的专著《代数和编码》^[6].

本文研究本原射影 RS 码的深洞. 实际上, 当 $\lambda \in \mathbb{F}_q^*$, $f_{\leq k-2}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-2$ 的多项式时, 我们证明了由 $\lambda x^{q-2} + f_{\leq k-2}(x)$ 所生成的向量是有限域 $\mathbb{F}_q$ 上的本原射影 RS 码的一类深洞, 即有如下的主要结果.

定理 1.1 设 $q \geq 4$, 整数 k 满足 $2 \leq k \leq q-2$, 收到的向量 $\mathbf{u} \in \mathbb{F}_q^q$ 的前 $q-1$ 个分量的 Lagrange 插值多项式为 $u(x)$. 如果 $u(x) = \lambda x^{q-2} + f_{\leq k-2}(x)$, 其中 $\lambda \in \mathbb{F}_q^*$, $f_{\leq k-2}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-2$ 的多项式, 并且 $\mathbf{u}$ 的第 q 个分量为 0, 那么 $\mathbf{u}$ 是本原射影 RS 码 $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的一个深洞.

本文余下的内容安排如下: 首先, 第 2 节给出一些基本的定义和预备引理. 紧接着, 第 3 节利用第 2 节中的引理及 Vandermonde 行列式, 给出定理 1.1 的证明.

2 预备知识

本节给出一些基本的定义和一些引理.

定义 2.1^[5] 设 $\mathbb{F}_q$ 是特征为 p 的有限域. 令 $\mathbb{F}_q^* = \{\alpha_1, \dots, \alpha_{q-1}\}$, 则有限域 $\mathbb{F}_q$ 上长度为 n 、维数为 k 的本原射影 Reed-Solomon 码 (简称为本原射影 RS 码) 表为 $\text{PPRS}_q(\mathbb{F}_q^*, k)$, 定义为

$$\text{PPRS}_q(\mathbb{F}_q^*, k) := \{(f(\alpha_1), \dots, f(\alpha_{q-1}), c_{k-1}(f)) \in \mathbb{F}_q^q \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \leq k-1\},$$

其中 $c_{k-1}(f)$ 为 $f(x)$ 中 x^{k-1} 的系数. 称 $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 中的元素为码字.

定义 2.2^[6] 设 $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{F}_q^n$, $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$. 称 $d(\mathbf{u}, \mathbf{v}) := \#\{i \mid u_i \neq v_i, u_i \in \mathbb{F}_q, v_i \in \mathbb{F}_q\}$ 为向量 $\mathbf{u}$ 与 $\mathbf{v}$ 的 Hamming 距离.

定义 2.3^[6] 设 C 是参数为 $[n, k]$ 的线性码. 称 $d(C) := \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$ 为码 C 的极小距离.

定义 2.4^[6] 设 C 是参数为 $[n, k]$ 的线性码, $\mathbf{u} \in \mathbb{F}_q^n$. 称 $d(\mathbf{u}, C) := \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{v} \in C, \mathbf{v} \neq \mathbf{0}\}$ 为向量 $\mathbf{u}$ 到码 C 的错误距离.

显然, $d(\mathbf{u}, C) = 0 \Leftrightarrow \mathbf{u} \in C$.

定义 2.5^[6] 设 C 是参数为 $[n, k]$ 的线性码. 称 $\rho(C) := \max\{d(\mathbf{u}, C) \mid \mathbf{u} \in \mathbb{F}_q^n\}$ 为码 C 的覆盖半径.

定义 2.6^[7] 设 C 是参数为 $[n, k]$ 的线性码. 若向量 $\mathbf{u}$ 满足 $d(\mathbf{u}, C) = \rho(C)$, 则称 $\mathbf{u}$ 为码 C 的一个深洞.

定义 2.7^[6] 设 C 是参数为 $[n, k]$ 的线性码, G 是一个 $k \times n$ 的矩阵. 如果 G 的行向量正好构成 C 的一组基底, 那么称 G 是 C 的生成矩阵.

定义 2.8^[6] 设 C 是一个 $[n, k, d]$ 线性码. 若 $d = n - k + 1$, 则称 C 为极大距离可分码, 简称为 MDS (maximum distance separable) 码.

引理 2.9^[6] 设 C 是参数为 $[n, k]$ 的线性码, G 是 C 的生成矩阵, 则 C 为 MDS 码当且仅当 G 的任意 k 个不同的列向量均在 $\mathbb{F}_q$ 上是线性无关的.

引理 2.10^[8] 我们有

$$\rho(\text{PPRS}_q(\mathbb{F}_q^*, k)) = d(\text{PPRS}_q(\mathbb{F}_q^*, k)) - 1.$$

引理 2.11^[9] 设 C 为有限域 $\mathbb{F}_q$ 上的长度为 n 、维数为 k 的 MDS 码. 若码 C 的覆盖半径 $\rho(C) = n - k$, 则向量 $\mathbf{u} \in \mathbb{F}_q^n$ 为码 C 的一个深洞当且仅当如下的 $(k+1) \times n$ 矩阵:

$$\mathbf{G}^{\mathbf{u}} := \begin{pmatrix} \mathbf{G} \\ \mathbf{u} \end{pmatrix}$$

为某个 MDS 码的生成矩阵, 即当且仅当 $\mathbf{G}^{\mathbf{u}}$ 的任意 $k+1$ 列是线性无关的, 其中 $\mathbf{G}$ 为码 C 的生成矩阵.

对于本原射影 RS 码 $\text{PPRS}_q(\mathbb{F}_q^*, k)$, 定义收到的向量 $\mathbf{u} = (u_1, \dots, u_{q-1}, u_q) \in \mathbb{F}_q^q$ 的前 $q-1$ 个分量 $u_1, \dots, u_{q-1}$ 的 Lagrange 插值多项式 $u(x)$ 为

$$u(x) := \sum_{i=1}^{q-1} u_i \prod_{\substack{j=1 \\ j \neq i}}^{q-1} \frac{x - \alpha_j}{\alpha_i - \alpha_j}.$$

显然, $\deg u(x) \leq q-2$, $u(\alpha_i) = u_i$ ($1 \leq i \leq q-1$). 进而,

$$\mathbf{u} \in \text{PPRS}_q(\mathbb{F}_q^*, k) \Leftrightarrow \deg u(x) \leq k-1, \quad c_{k-1}(u(x)) = u_q.$$

故只需考虑情形 $k \leq \deg u(x) \leq q-2$ 或 $c_{k-1}(u(x)) \neq u_q$.

引理 2.12 设 $u(x)$ 和 $v(x)$ 分别为向量 $\mathbf{u} = (u_1, \dots, u_{q-1}, u_q) \in \mathbb{F}_q^q$ 和 $\mathbf{v} = (v_1, \dots, v_{q-1}, v_q) \in \mathbb{F}_q^q$ 的前 $q-1$ 个分量的 Lagrange 插值多项式. 若

$$u(x) = \lambda v(x) + f_{\leq k-2}(x), \quad u_q = \lambda v_q,$$

其中 $\lambda \in \mathbb{F}_q^*$, $f_{\leq k-2}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-2$ 的多项式, 则

$$d(\mathbf{u}, \text{PPRS}_q(\mathbb{F}_q^*, k)) = d(\mathbf{v}, \text{PPRS}_q(\mathbb{F}_q^*, k)).$$

证明 若 $h(x) \in \mathbf{F}_q[x]$, $\mathbb{F}_q^* = \{\alpha_1, \dots, \alpha_{q-1}\}$, 则定义

$$h(\mathbb{F}_q^*) := \{h(\alpha_1), \dots, h(\alpha_{q-1})\}.$$

令

$$P_{k-1} := \{f(x) \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \leq k-1\}.$$

因为 $u(x) = \lambda v(x) + f_{\leq k-2}(x)$ 和 $u_q = \lambda v_q$, 所以, 由 Hamming 距离的线性性可知,

$$\begin{aligned} d(\mathbf{u}, \text{PPRS}_q(\mathbb{F}_q^*, k)) &= d((u(\mathbb{F}_q^*), u_q), \text{PPRS}_q(\mathbb{F}_q^*, k)) \\ &= \min_{g \in P_{k-1}} d((u(\mathbb{F}_q^*), u_q), (g(\mathbb{F}_q^*), c_{k-1}(g))) \end{aligned}$$

$$\begin{aligned}
&= \min_{g \in P_{k-1}} d((\lambda v(\mathbb{F}_q^*) + f_{\leq k-2}(\mathbb{F}_q^*), \lambda v_q), (g(\mathbb{F}_q^*), c_{k-1}(g))) \\
&= \min_{g \in P_{k-1}} d((\lambda v(\mathbb{F}_q^*) + f_{\leq k-2}(\mathbb{F}_q^*), \lambda v_q), (g(\mathbb{F}_q^*) + f_{\leq k-2}(\mathbb{F}_q^*), c_{k-1}(g))) \\
&= \min_{g \in P_{k-1}} d((\lambda v(\mathbb{F}_q^*), \lambda v_q), (g(\mathbb{F}_q^*), c_{k-1}(g))) \\
&= \min_{g \in P_{k-1}} d((\lambda v(\mathbb{F}_q^*), \lambda v_q), (\lambda g(\mathbb{F}_q^*), \lambda c_{k-1}(g))) \quad (\text{因为 } \lambda \in \mathbb{F}_q^*) \\
&= \min_{g \in P_{k-1}} d((v(\mathbb{F}_q^*), v_q), (g(\mathbb{F}_q^*), c_{k-1}(g))) \\
&= d((v(\mathbb{F}_q^*), v_q), \text{PPRS}_q(\mathbb{F}_q^*, k)) \\
&= d(v, \text{PPRS}_q(\mathbb{F}_q^*, k)).
\end{aligned}$$

从而引理证毕. □

3 定理 1.1 的证明

本节利用第 2 节中的引理, 给出定理 1.1 的证明.

定理 1.1 的证明 对于任意非空子集 $\{\gamma_1, \dots, \gamma_n\} \subset \mathbb{F}_q$, 定义它的 Vandermonde 行列式 $V(\gamma_1, \dots, \gamma_n)$ 如下:

$$V(\gamma_1, \dots, \gamma_n) := \begin{vmatrix} 1 & 1 & \dots & 1 \\ \gamma_1 & \gamma_2 & \dots & \gamma_n \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{n-1} & \gamma_2^{n-1} & \dots & \gamma_n^{n-1} \end{vmatrix}.$$

在有限域上的线性代数中, 我们熟知

$$V(\gamma_1, \dots, \gamma_n) = \prod_{1 \leq i < j \leq n} (\gamma_j - \gamma_i).$$

设 $\mathbb{F}_q^* = \{\alpha_1, \dots, \alpha_{q-1}\}$. 由定义 2.7 知, $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的生成矩阵为

$$G = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_{q-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_{q-1}^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_{q-1}^{k-1} & 1 \end{pmatrix}_{k \times q}.$$

设 G 的列分块为 $G = (G_1, G_2, \dots, G_q)$, 设 $i_1, i_2, \dots, i_k$ 为任意 k 个整数, 满足 $1 \leq i_1 < i_2 < \dots < i_k \leq q$. 断言: $\det(G_{i_1}, G_{i_2}, \dots, G_{i_k}) \neq 0$. 下面给出证明.

若 $i_k < q$, 则 k 阶子阵 $(G_{i_1}, G_{i_2}, \dots, G_{i_k})$ 的行列式为以 $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}$ 为参数的 k 阶 Vandermonde 行列式. 于是,

$$\det(G_{i_1}, G_{i_2}, \dots, G_{i_k}) = V(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}) = \prod_{1 \leq t < s \leq k} (\alpha_{i_s} - \alpha_{i_t}) \neq 0.$$

若 $i_k = q$, 则按最后一列展开, 有

$$\det(G_{i_1}, G_{i_2}, \dots, G_{i_k}) = V(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_{k-1}}) = \prod_{1 \leq t < s \leq k-1} (\alpha_{i_s} - \alpha_{i_t}) \neq 0.$$

这样就推得

$$\det(G_{i_1}, G_{i_2}, \dots, G_{i_k}) \neq 0.$$

即断言得证.

于是, 由断言立即可知 $G_{i_1}, G_{i_2}, \dots, G_{i_k}$ 是线性无关的, 即 $\mathbf{G}$ 的任意 k 列是线性无关的. 又据引理 2.9 可知, $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 为 MDS 码. 从而, 由定义 2.8 得

$$d(\text{PPRS}_q(\mathbb{F}_q^*, k)) = q - k + 1.$$

又 $\mathbb{F}_q^* \cup \{\infty\} \subset \mathbb{F}_q \cup \{\infty\}$, 故由引理 2.10 可知, $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的覆盖半径为

$$\rho(\text{PPRS}_q(\mathbb{F}_q^*, k)) = d - 1 = q - k.$$

现设 $u_q(x) = x^{q-2}$. 考虑 $u_q(x)$ 定义的向量 $\mathbf{u}_q = (\alpha_1^{q-2}, \alpha_2^{q-2}, \dots, \alpha_{q-1}^{q-2}, 0)$. 从而有

$$\mathbf{G}^{\mathbf{u}_q} := \begin{pmatrix} \mathbf{G} \\ \mathbf{u}_q \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_{q-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_{q-1}^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_{q-1}^{k-1} & 1 \\ \alpha_1^{q-2} & \alpha_2^{q-2} & \alpha_3^{q-2} & \dots & \alpha_{q-1}^{q-2} & 0 \end{pmatrix}.$$

下面证明 $\mathbf{G}^{\mathbf{u}_q}$ 的任意 $k+1$ 列是线性无关的. 设 $\mathbf{G}^{\mathbf{u}_q}$ 的列分块为

$$\mathbf{G}^{\mathbf{u}_q} = (\bar{G}_1, \bar{G}_2, \dots, \bar{G}_q).$$

设 $\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}$ 为 $\mathbf{G}^{\mathbf{u}_q}$ 的任意 $k+1$ 列, 其中 $j_1, j_2, \dots, j_{k+1}$ 为任意 $k+1$ 个整数且满足 $1 \leq j_1 < j_2 < \dots < j_{k+1} \leq q$, 则 $(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}})$ 为一个 $k+1$ 阶矩阵.

下证 $\det(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) \neq 0$. 为此, 考虑如下情形:

情形 1 $j_{k+1} < q$, 则有

$$(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_{k+1}} \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_{k+1}}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{j_1}^{k-1} & \alpha_{j_2}^{k-1} & \alpha_{j_3}^{k-1} & \dots & \alpha_{j_{k+1}}^{k-1} \\ \alpha_{j_1}^{q-2} & \alpha_{j_2}^{q-2} & \alpha_{j_3}^{q-2} & \dots & \alpha_{j_{k+1}}^{q-2} \end{pmatrix}.$$

由于对于 $1 \leq i \leq k+1$, 有 $\alpha_{j_i}^{q-2} = \alpha_{j_i}^{-1}$, 因此, 由 Vandermonde 行列式可推得

$$\begin{aligned}
\det(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) &= \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_{k+1}} \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_{k+1}}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{j_1}^{k-1} & \alpha_{j_2}^{k-1} & \alpha_{j_3}^{k-1} & \dots & \alpha_{j_{k+1}}^{k-1} \\ \alpha_{j_1}^{-1} & \alpha_{j_2}^{-1} & \alpha_{j_3}^{-1} & \dots & \alpha_{j_{k+1}}^{-1} \end{pmatrix} \\
&= \left(\prod_{i=1}^{k+1} \alpha_{j_i}^{-1} \right) \det \begin{pmatrix} \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_{k+1}} \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_{k+1}}^2 \\ \alpha_{j_1}^3 & \alpha_{j_2}^3 & \alpha_{j_3}^3 & \dots & \alpha_{j_{k+1}}^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{j_1}^k & \alpha_{j_2}^k & \alpha_{j_3}^k & \dots & \alpha_{j_{k+1}}^k \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix} \\
&= (-1)^k \left(\prod_{i=1}^{k+1} \alpha_{j_i}^{-1} \right) V(\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{k+1}}) \\
&= (-1)^k \left(\prod_{i=1}^{k+1} \alpha_{j_i}^{-1} \right) \prod_{1 \leq s < t \leq k+1} (\alpha_{j_t} - \alpha_{j_s}). \tag{3.1}
\end{aligned}$$

但是 $\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{k+1}}$ 为 $\mathbb{F}_q^*$ 中 $k+1$ 个不同元素. 所以, 由 (3.1) 可知, $\det(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) \neq 0$.

情形 2 $j_{k+1} = q$, 那么有

$$(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 0 \\ \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_k} & 0 \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_k}^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{j_1}^{k-1} & \alpha_{j_2}^{k-1} & \alpha_{j_3}^{k-1} & \dots & \alpha_{j_k}^{k-1} & 1 \\ \alpha_{j_1}^{q-2} & \alpha_{j_2}^{q-2} & \alpha_{j_3}^{q-2} & \dots & \alpha_{j_k}^{q-2} & 0 \end{pmatrix}.$$

于是, 由 $\alpha_{j_i}^{q-2} = \alpha_{j_i}^{-1}$ ($1 \leq i \leq k$), 可推得

$$\det(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 0 \\ \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_k} & 0 \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_k}^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{j_1}^{k-1} & \alpha_{j_2}^{k-1} & \alpha_{j_3}^{k-1} & \dots & \alpha_{j_k}^{k-1} & 1 \\ \alpha_{j_1}^{-1} & \alpha_{j_2}^{-1} & \alpha_{j_3}^{-1} & \dots & \alpha_{j_k}^{-1} & 0 \end{pmatrix}$$

$$\begin{aligned}
&= (-1)^{2k+1} \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_k} \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_k}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{j_1}^{k-2} & \alpha_{j_2}^{k-2} & \alpha_{j_3}^{k-2} & \dots & \alpha_{j_k}^{k-2} \\ \alpha_{j_1}^{-1} & \alpha_{j_2}^{-1} & \alpha_{j_3}^{-1} & \dots & \alpha_{j_k}^{-1} \end{pmatrix} \\
&= (-1)^{2k+1} \left(\prod_{i=1}^k \alpha_{j_i}^{-1} \right) \det \begin{pmatrix} \alpha_{j_1} & \alpha_{j_2} & \alpha_{j_3} & \dots & \alpha_{j_k} \\ \alpha_{j_1}^2 & \alpha_{j_2}^2 & \alpha_{j_3}^2 & \dots & \alpha_{j_k}^2 \\ \alpha_{j_1}^3 & \alpha_{j_2}^3 & \alpha_{j_3}^3 & \dots & \alpha_{j_k}^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{j_1}^{k-1} & \alpha_{j_2}^{k-1} & \alpha_{j_3}^{k-1} & \dots & \alpha_{j_k}^{k-1} \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix} \\
&= (-1)^{2k+1} (-1)^{k-1} \left(\prod_{i=1}^k \alpha_{j_i}^{-1} \right) V(\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_k}) \\
&= (-1)^{3k} \left(\prod_{i=1}^k \alpha_{j_i}^{-1} \right) \prod_{1 \leq s < t \leq k} (\alpha_{j_t} - \alpha_{j_s}). \tag{3.2}
\end{aligned}$$

但是, $\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_k}$ 为 $\mathbb{F}_q^*$ 中 k 个不同元素. 所以, 由 (3.2) 立即推得 $\det(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) \neq 0$.

这样就完成了结论 $\det(\bar{G}_{j_1}, \bar{G}_{j_2}, \dots, \bar{G}_{j_{k+1}}) \neq 0$ 的证明. 由此立即可知 $\mathbf{G}^{\mathbf{u}_q}$ 中任意 $k+1$ 列是线性无关的. 从而, $\mathbf{G}^{\mathbf{u}_q}$ 必为某个 MDS 码的生成矩阵. 于是, 根据引理 2.11 立即可知 $\mathbf{u}_q$ 是码 $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的深洞, 即

$$d(\mathbf{u}_q, \text{PPRS}_q(\mathbb{F}_q^*, k)) = n - k = q - k.$$

又 $u(x) = \lambda u_q(x) + f_{\leq k-2}(x)$, 且 $\mathbf{u}$ 和 $\mathbf{u}_q$ 的第 q 个分量均为 0, 那么, 由引理 2.12 可知,

$$d(\mathbf{u}, \text{PPRS}_q(\mathbb{F}_q^*, k)) = d(\mathbf{u}_q, \text{PPRS}_q(\mathbb{F}_q^*, k)) = q - k.$$

故收到的向量 $\mathbf{u} = (u(\mathbb{F}_q^*), 0)$ 是 $\text{PPRS}_q(\mathbb{F}_q^*, k)$ 的深洞. 这样就完成了定理 1.1 的证明. $\square$

致谢 作者十分感谢两位审稿人对本论文所提出的宝贵修改意见.

参考文献

- 1 Li J Y, Wan D Q. On the subset sum problem over finite fields. *Finite Fields Appl*, 2008, 14: 911–929
- 2 Cheng Q, Murray E. On deciding deep holes of Reed-Solomon codes. In: *International Conference on Theory and Applications of Models of Computation*. Berlin-Heidelberg: Springer, 2007, 296–305
- 3 Wu R J, Hong S F. On deep holes of standard Reed-Solomon codes. *Sci China Math*, 2012, 55: 2447–2455
- 4 Hong S F, Wu R J. On deep holes of generalized Reed-Solomon codes. *AIMS Math*, 2016, 1: 96–101
- 5 Zhang J, Wan D Q. On deep holes of projective Reed-Solomon codes. In: *2016 IEEE International Symposium on Information Theory (ISIT)*. Barcelona: IEEE, 2016, 925–929
- 6 万哲先. 代数和编码 (第三版). 北京: 高等教育出版社, 2007
- 7 Dür A. On the covering radius of Reed-Solomon codes. *Discrete Math*, 1994, 126: 99–105

- 8 Dür A. The decoding of extended Reed-Solomon codes. *Discrete Math*, 1991, 90: 21–40
- 9 Zhuang J C, Cheng Q, Li J Y. On determining deep holes of generalized Reed-Solomon codes. *IEEE Trans Inform Theory*, 2016, 62: 199–207

On deep holes of primitive projective Reed-Solomon codes

Xiaofan Xu, Shaofang Hong & Yongchao Xu

Abstract Primitive projective Reed-Solomon code, which is an important class of maximum distance separable codes, is currently widely used in digital communication. We usually use the maximum likelihood decoding algorithm in the decoding process of Reed-Solomon codes. For the received word $\mathbf{u} \in \mathbb{F}_q^n$, the maximum likelihood decoding algorithm lies in determining its error distance $d(\mathbf{u}, C)$. It is well known that $d(\mathbf{u}, C) \leq \rho(C)$ with $\rho(C)$ being the covering radius of code C . If $d(\mathbf{u}, C) = \rho(C)$, then $\mathbf{u}$ is called a deep hole of C . In this paper, we obtain a class of deep holes of primitive projective Reed-Solomon codes $\text{PPRS}_q(\mathbb{F}_q^*, k)$. In fact, by using the generating matrix of maximal distance separable codes over the finite field $\mathbb{F}_q$ and Vandermonde determinant, we show that if $q \geq 4$, k is an integer with $2 \leq k \leq q-2$ and the Lagrange interpolating polynomial of the first $q-1$ components of the received word $\mathbf{u}$ is $\lambda x^{q-2} + f_{\leq k-2}(x)$, with $\lambda \in \mathbb{F}_q^*$ and $f_{\leq k-2}(x)$ being a polynomial of degree no more than $k-2$ over $\mathbb{F}_q$, and the q -th component of $\mathbf{u}$ is 0, then $\mathbf{u}$ is a deep hole of the primitive projective Reed-Solomon code $\text{PPRS}_q(\mathbb{F}_q^*, k)$.

Keywords primitive projective Reed-Solomon code, MDS (maximum distance separable) code, deep hole

MSC(2010) 94B35, 11C08

doi: 10.1360/N012017-00064