DOI: 10.13718/j.cnki.xdzk.2017.03.010

关于标准 Reed-Solomon 码的错误距离的注记①

徐小凡[1,2]，　许　霞[1]

1. 四川旅游学院，成都 610100；2. 四川大学 数学学院，成都 610064

摘要：Reed-Solomon 码是数字通信领域中的一类重要的极大距离可分码. Reed-Solomon 码的译码过程，通常采用最大似然译码算法. 对于收到的一个码字 $\boldsymbol{u}\in\mathbb{F}_q^n$，最大似然译码算法关键在于确定码字 $\boldsymbol{u}$ 对于码 C 的错误距离 $d(\boldsymbol{u},C)$. 熟知 $d(\boldsymbol{u},C)\leqslant n-k$，其中 n,k 分别为码 C 的码长和维数. 若 $d(\boldsymbol{u},C)=n-k$，则称 $\boldsymbol{u}$ 为码 C 的深洞. 借助有限域 $\mathbb{F}_q$ 上极大距离可分码的生成矩阵部分证明了标准 Reed-Solomon 码的深洞猜想.

关　键　词：Reed-Solomon 码；MDS 码；生成矩阵；错误距离

中图分类号：O236.2　　**文献标志码**：A　　**文章编号**：1673-9868(2017)03-0062-07

1960 年作为 MIT 林肯实验室成员的 Irving S Reed 和 Gustave Solomon 提出了一种基于多项式的纠错编码即 Reed-Solomon 码. 由于 Reed-Solomon 码为极大距离可分码即最小距离可达到 Singleton 界，而且 Reed-Solomon 码作为循环码的一种特殊情形，能够高效地进行编码，尤其是针对标准 Reed-Solomon 码的软件实现非常方便；并且 Reed-Solomon 码能够很好地被译码，因此 Reed-Solomon 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”、“旅行者二号”空间探测器就使用了 Reed-Solomon 码向地球传回了土星、天王星等天体的宝贵天文图片. 在 Reed-Solomon 码的研究中，其中一个重要方面是在采用 MLD 算法时对于收到的码字 $\boldsymbol{u}$ 如何确定其错误距离 $d(\boldsymbol{u},C)$，而错误距离问题主要在于确定其界，达到上界即深洞[1] 问题，达到下界即平凡码字[2] 问题. 文献[3]猜想标准 Reed-Solomon 码的深洞只有码字 $\boldsymbol{u}$ 的拉格朗日插值多项式 $u(x)$ 为 $ax^k+f_{\leqslant k-1}(x)$ 的情形. 文献[4]通过对 Reed-Solomon 码进行离散傅立叶变换，得到当收到的码字 $\boldsymbol{u}$ 的拉格朗日插值多项式 $u(x)$ 为 $ax^{q-2}+f_{\leqslant k-1}(x)$ 时，$\boldsymbol{u}$ 是标准 Reed-Solomon 码的深洞，并由此推翻了 Cheng-Murry 猜想，进一步 Wu 和 Hong 猜想码字 $\boldsymbol{u}$ 为标准 Reed-Solomon 码的深洞当且仅当其拉格朗日插值多项式 $u(x)$ 为 $ax^k+f_{\leqslant k-1}(x)$ 或 $ax^{q-2}+f_{\leqslant k-1}(x)$，其中 $a\in\mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式. 文献[5]通过对有限域上特定方程的求解证明当 $\mathbb{F}_q$ 为特征为 2 的有限域时，$ax^{q-3}+f_{\leqslant k-1}(x)$ 为 Reed-Solomon 码的深洞，其中 $a\in\mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式.

在本文中，当 $\lambda\in\mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式时，我们证明了 $\lambda x^{q-3}+f_{\leqslant k-1}(x)$ 和 $\lambda x^{k+1}+f_{\leqslant k-1}(x)$ 不是奇特征的有限域 $\mathbb{F}_q$ 上的 Reed-Solomon 码的深洞.

1　预备知识

在本节中，我们给出一些定义和引理.

① 收稿日期：2016-05-19
基金项目：四川省教育厅自然科学基金项目(2016ZB0342)；四川省科技厅软科学项目(2016ZR0112).
作者简介：徐小凡(1987-)，男，湖北麻城人，博士研究生，主要从事数论与编码理论研究.
通信作者：许　霞，教授.

定义 1[3] 设 $\mathbb{F}_q$ 为特征为 p 的有限域，令集合 $\mathbb{F}_q^* = \{a_1, a_2, a_3, \cdots, a_{q-1}\}$，有限域 $\mathbb{F}_q$ 上长度为 n，维数为 k 的标准 Reed-Solomon 码定义为

$$RS_q(\mathbb{F}_q^*, k) := \{(f(a_1), f(a_2), f(a_3), \cdots, f(a_{q-1})) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \leqslant k-1\}$$

其中 $n = q-1$，$RS_q(\mathbb{F}_q^*, k)$ 中的元素称为码字.

定义 2[4] 设 $\boldsymbol{u} = (u_1, u_2, u_3, \cdots, u_n) \in \mathbb{F}_q^n$，$\boldsymbol{v} = (v_1, v_2, v_3, \cdots, v_n) \in \mathbb{F}_q^n$，定义 $d(\boldsymbol{u}, \boldsymbol{v}) = \#\{i \mid u_i \neq v_i, u_i \in \mathbb{F}_q, v_i \in \mathbb{F}_q\}$ 为码字 $\boldsymbol{u}, \boldsymbol{v}$ 的汉明距离.

定义 3[4] 有限域 $\mathbb{F}_q$ 上的 $[n, k]_q$ 线性码 C，对于接受到的码字 $\boldsymbol{u} \in \mathbb{F}_q^n$，定义 $d(\boldsymbol{u}, C) = \min\{d(\boldsymbol{u}, \boldsymbol{v}) \mid \boldsymbol{v} \in C, \boldsymbol{v} \neq \boldsymbol{0}\}$ 为码字 $\boldsymbol{u}$ 对于码 C 的错误距离. 显然 $d(\boldsymbol{u}, C) = 0 \Leftrightarrow \boldsymbol{u} \in C$.

定义 4[4] 有限域 $\mathbb{F}_q$ 上的 $[n, k]_q$ 线性码 C，定义 $\rho(C) = \max\{d(\boldsymbol{u}, C) \mid \boldsymbol{u} \in \mathbb{F}_q^n\}$ 为码 C 的覆盖半径. 特别地，对于 Reed-Solomon 码有 $\rho(C) = n-k$.

对于标准 Reed-Solomon 码，设收到的码字 $\boldsymbol{u} = (u_1, u_2, u_3, \cdots, u_n) \in \mathbb{F}_q^n$，$\mathbb{F}_q$ 上的拉格朗日插值多项式定义为

$$u(x) := \sum_{i=1}^{n} u_i \prod_{i=1, j\neq i}^{n} \frac{x - x_j}{x_i - x_j}$$

其中 $u(x_i) = u_i$. 由拉格朗日插值多项式的性质知

$$\deg u(x) \leqslant n-1$$

又

$$\boldsymbol{u} \in C \Leftrightarrow \deg u(x) \leqslant k-1 \Leftrightarrow d(\boldsymbol{u}, C) = 0$$

故文中我们只讨论 $k \leqslant \deg u(x) \leqslant n-1 = q-2$ 的情形.

引理 1[6] 设 $\boldsymbol{u} \in \mathbb{F}_q^n$，$k \leqslant \deg u(x) \leqslant n-1$，$C$ 为 $\mathbb{F}_q$ 上的长度为 n，维数为 k 的 Reed-Solomon 码，则

$$n - \deg(u(x)) \leqslant d(\boldsymbol{u}, C) \leqslant n-k$$

定义 5[7] 设 C 为 $\mathbb{F}_q$ 上的长度为 n，维数为 k 的 Reed-Solomon 码，若 $d(\boldsymbol{u}, C) = n-k$，称码字 $\boldsymbol{u}$ 为 Reed-Solomon 码的深洞，其中 $u(x)$ 为 $\boldsymbol{u}$ 的拉格朗日插值多项式.

引理 2[8] 设 C 为 $\mathbb{F}_q$ 上的维数为 k 的 Reed-Solomon 码，$\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$，若 $u(x) = \lambda v(x) + f_{\leqslant k-1}(x)$，其中 $\lambda \in \mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式，$u(x), v(x)$ 分别为码字 $\boldsymbol{u}, \boldsymbol{v}$ 的拉格朗日插值多项式，则 $d(\boldsymbol{u}, C) = d(\boldsymbol{v}, C)$，即 $\boldsymbol{u}$ 为码 C 的深洞当且仅当 $\boldsymbol{v}$ 为码 C 的深洞.

引理 3[9] 设 $\mathbb{F}_q$ 为特征为 p 的有限域，C 为 $\mathbb{F}_q$ 上的 $[n, k]$MDS码且其覆盖半径 $\rho = n-k$，则码字 $\boldsymbol{u} \in \mathbb{F}_q^n$ 为码 C 的深洞当且仅当

$$\boldsymbol{G}^u = \begin{pmatrix} \boldsymbol{G} \\ \boldsymbol{u} \end{pmatrix}$$

为 MDS 码的生成矩阵，即 $\boldsymbol{G}^u$ 的任意 $k+1$ 列线性无关，其中 $\boldsymbol{G}$ 为码 C 的生成矩阵.

引理 4 设 $\mathbb{F}_q$ 为特征 $p \geqslant 7$ 的有限域，若 $2 \leqslant k \leqslant q-5$，则方程 $x_1 + x_2 + \cdots + x_{k+1} = 0$ 在 $\mathbb{F}_q^*$ 中有解，其中 $\{x_1, x_2, \cdots, x_{k+1}\} \subset \mathbb{F}_q^*$.

证 因为 $\mathbb{F}_q$ 为特征 $p \geqslant 7$ 的奇特征域，所以对于任意的 $\alpha \in \mathbb{F}_q^*$，有

$$\{\alpha, -\alpha\} \subset \mathbb{F}_q^*$$

从而

$$\mathbb{F}_q = \{0, \alpha_1, -\alpha_1, \alpha_2, -\alpha_2, \cdots, \alpha_{\frac{q-1}{2}}, -\alpha_{\frac{q-1}{2}}\}$$

(i) 当 $2 \mid k+1$ 时，令

$$\{x_1, x_2, \cdots, x_{k+1}\} = \{\alpha_1, -\alpha_1, \alpha_2, -\alpha_2, \cdots, \alpha_{\frac{k+1}{2}}, -\alpha_{\frac{k+1}{2}}\} \subset \mathbb{F}_q^*$$

则

$$\sum_{i=1}^{k+1} x_i = \alpha_1 + (-\alpha_1) + \alpha_2 + (-\alpha_2) + \cdots + \alpha_{\frac{k+1}{2}} + (-\alpha_{\frac{k+1}{2}}) = 0$$

(ⅱ) 当 $2 \nmid k+1$ 时，因为 $\mathbb{F}_q$ 为特征 $p \geqslant 7$ 的有限域，所以 $\{1, 2, p-3\} \subset \mathbb{F}_p{}^* \subset \mathbb{F}_q^*$. 又 $2 \leqslant k \leqslant q-5$，从而存在

$$\{\gamma_1, -\gamma_1, \cdots, \gamma_{\frac{k-2}{2}}, -\gamma_{\frac{k-2}{2}}\} \subset \mathbb{F}_q^* \setminus \{1, 2, p-3\}$$

令

$$\{x_1, x_2, \cdots, x_{k+1}\} = \{1, 2, p-3\} \cup \{\gamma_1, -\gamma_1, \cdots, \gamma_{\frac{k-2}{2}}, -\gamma_{\frac{k-2}{2}}\}$$

则

$$\sum_{i=1}^{k+1} x_i = 1 + 2 + p - 3 + \gamma_1 + (-\gamma_1) + \cdots + \gamma_{\frac{k-2}{2}} + (-\gamma_{\frac{k-2}{2}}) = 0$$

由 (ⅰ),(ⅱ) 知，存在 $\mathbb{F}_q^*$ 中 $k+1$ 个不同元满足

$$\sum_{i=1}^{k+1} x_i = 0$$

引理 4 证毕.

2　主要结果

定理 1　设 $\mathbb{F}_q$ 为特征 $p \geqslant 7$ 的有限域，若

$$u(x) = \lambda x^{q-3} + f_{\leqslant k-1}(x),\ 2 \leqslant k \leqslant q-5$$

其中 $\lambda \in \mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式，$u(x)$ 为码字 $\boldsymbol{u}$ 的拉格朗日插值多项式，则码字 $\boldsymbol{u}$ 不是 $RS_q(\mathbb{F}_q^*, k)$ 的深洞.

证　设 $\mathbb{F}_q^* = \{\alpha_1, \alpha_2, \cdots, \alpha_{q-1}\}$，则 $RS_q(\mathbb{F}_q^*, k)$ 的生成矩阵为

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_{q-1}^{k-1} \end{pmatrix}$$

不妨设 $u_k(x) = x^{q-3}$，则

$$\boldsymbol{u}_k = (\alpha_1^{q-3}, \alpha_2^{q-3}, \cdots, \alpha_{q-1}^{q-3})$$

从而有

$$\boldsymbol{G}^{\boldsymbol{u}_k} = \begin{pmatrix} \boldsymbol{G} \\ \boldsymbol{u}_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_{q-1}^{k-1} \\ \alpha_1^{q-3} & \alpha_2^{q-3} & \alpha_3^{q-3} & \cdots & \alpha_{q-1}^{q-3} \end{pmatrix}$$

取 $\{\beta_1, \beta_2, \beta_3, \cdots, \beta_{k+1}\} \subseteq \mathbb{F}_q^*$，下面考虑 $\boldsymbol{G}^{\boldsymbol{u}_k}$ 的 $k+1$ 阶子方阵

$$\boldsymbol{G}_{k+1}^{\boldsymbol{u}_k} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{k+1} \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \cdots & \beta_{k+1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \beta_3^{k-1} & \cdots & \beta_{k+1}^{k-1} \\ \beta_1^{q-3} & \beta_2^{q-3} & \beta_3^{q-3} & \cdots & \beta_{k+1}^{q-3} \end{pmatrix}$$

则

$$\det(\boldsymbol{G}_{k+1}^{\boldsymbol{u}_k})=\begin{vmatrix}1&1&1&\cdots&1\\ \beta_1&\beta_2&\beta_3&\cdots&\beta_{k+1}\\ \beta_1^2&\beta_2^2&\beta_3^2&\cdots&\beta_{k+1}^2\\ \vdots&\vdots&\vdots&\vdots&\vdots\\ \beta_1^{k-1}&\beta_2^{k-1}&\beta_3^{k-1}&\cdots&\beta_{k+1}^{k-1}\\ \beta_1^{q-3}&\beta_2^{q-3}&\beta_3^{q-3}&\cdots&\beta_{k+1}^{q-3}\end{vmatrix}=$$

$$\prod_{i=1}^{k+1}\beta_i^{-2}\begin{vmatrix}\beta_1^2&\beta_2^2&\beta_3^2&\cdots&\beta_{k+1}^2\\ \beta_1^3&\beta_2^3&\beta_3^3&\cdots&\beta_{k+1}^3\\ \vdots&\vdots&\vdots&\vdots&\vdots\\ \beta_1^{k+1}&\beta_2^{k+1}&\beta_3^{k+1}&\cdots&\beta_{k+1}^{k+1}\\ 1&1&1&\cdots&1\end{vmatrix}=$$

$$(-1)^k\prod_{i=1}^{k+1}\beta_i^{-2}\begin{vmatrix}1&1&1&\cdots&1\\ \beta_1^2&\beta_2^2&\beta_3^2&\cdots&\beta_{k+1}^2\\ \beta_1^3&\beta_2^3&\beta_3^3&\cdots&\beta_{k+1}^3\\ \vdots&\vdots&\vdots&\vdots&\vdots\\ \beta_1^{k+1}&\beta_2^{k+1}&\beta_3^{k+1}&\cdots&\beta_{k+1}^{k+1}\end{vmatrix}$$

又因为

$$\begin{vmatrix}1&1&1&\cdots&1&1\\ \beta_1&\beta_2&\beta_3&\cdots&\beta_{k+1}&x\\ \beta_1^2&\beta_2^2&\beta_3^2&\cdots&\beta_{k+1}^2&x^2\\ \beta_1^3&\beta_2^3&\beta_3^3&\cdots&\beta_{k+1}^3&x^3\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\ \beta_1^{k+1}&\beta_2^{k+1}&\beta_3^{k+1}&\cdots&\beta_{k+1}^{k+1}&x^{k+1}\end{vmatrix}=$$

$$\prod_{i=1}^{k+1}(x-\beta_i)\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\triangleq$$

$$\sum_{i=0}^{k+1}a_ix^i$$

从而

$$\det(\boldsymbol{G}_{k+1}^{\boldsymbol{u}_k})=(-1)^k\prod_{i=1}^{k+1}\beta_i^{-2}(-1)^{k+4}a_1=$$

$$(-1)^{2k+4}\prod_{i=1}^{k+1}\beta_i^{-2}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\sum_{j=1}^{k+1}(-1)^k\prod_{i=1}^{k+1}\beta_i\beta_j^{-1}=$$

$$(-1)^{3k+4}\prod_{i=1}^{k+1}\beta_i^{-1}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\sum_{j=1}^{k+1}\beta_j^{-1}\triangleq$$

$$(-1)^{3k+4}\prod_{i=1}^{k+1}\beta_i^{-1}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\sum_{j=1}^{k+1}\gamma_j$$

故由引理4知，当 $p\geqslant 7$，$2\leqslant k\leqslant q-5$ 时，存在 $\{\gamma_1,\gamma_2,\cdots,\gamma_{k+1}\}\subset\mathbb{F}_q^*$ 使得

$$\sum_{j=1}^{k+1}\gamma_j=0$$

从而有

$$\det(\boldsymbol{G}_{k+1}^{\boldsymbol{u}_k})=0$$

即 $\boldsymbol{G}^{\boldsymbol{u}_k}$ 中存在 $k+1$ 列线性相关. 据引理 3 知，$\boldsymbol{u}_k$ 不是 $RS_q(\mathbb{F}_q^*, k)$ 的深洞. 又

$$u(x)=\lambda u_k(x)+f_{\leqslant k-1}(x)$$

从而对于 $1\leqslant i\leqslant q-1$ 有

$$u(\alpha_i)=\lambda u_k(\alpha_i)+f_{\leqslant k-1}(\alpha_i)$$

即

$$\boldsymbol{u}=\lambda\boldsymbol{u}_k+f_{\leqslant k-1}$$

由引理 2 知，$\boldsymbol{u}$ 不是 $RS_q(\mathbb{F}_q^*, k)$ 的深洞. 定理 1 证毕.

定理 2　设 $\mathbb{F}_q$ 为特征 $p\geqslant 7$ 的有限域，若

$$v(x)=\lambda x^{k+1}+f_{\leqslant k-1}(x),\ 2\leqslant k\leqslant q-5$$

其中 $\lambda\in\mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式，$v(x)$ 为码字 $\boldsymbol{v}$ 的拉格朗日插值多项式，则码字 $\boldsymbol{v}$ 不是 $RS_q(\mathbb{F}_q^*, k)$ 的深洞.

证　设 $\mathbb{F}_q^*=\{\alpha_1, \alpha_2, \cdots, \alpha_{q-1}\}$，则 $RS_q(\mathbb{F}_q^*, k)$ 的生成矩阵为

$$\boldsymbol{G}=\begin{pmatrix}1 & 1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1}\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_{q-1}^{k-1}\end{pmatrix}$$

不妨设

$$v_k(x)=x^{k+1}$$

则

$$\boldsymbol{v}_k=(\alpha_1^{k+1}, \alpha_2^{k+1}, \cdots, \alpha_{q-1}^{k+1})$$

从而有

$$\boldsymbol{G}^{\boldsymbol{v}_k}=\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{v}_k\end{pmatrix}=\begin{pmatrix}1 & 1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1}\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_{q-1}^{k-1}\\ \alpha_1^{k+1} & \alpha_2^{k+1} & \alpha_3^{k+1} & \cdots & \alpha_{q-1}^{k+1}\end{pmatrix}$$

取 $\{\beta_1, \beta_2, \beta_3, \cdots, \beta_{k+1}\}\subseteq\mathbb{F}_q^*$，下面考虑 $\boldsymbol{G}^{\boldsymbol{v}_k}$ 的 $k+1$ 阶子方阵的行列式

$$\det(\boldsymbol{G}_{k+1}^{\boldsymbol{v}_k})=\begin{vmatrix}1 & 1 & 1 & \cdots & 1\\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{k+1}\\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \cdots & \beta_{k+1}^2\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \beta_1^{k-1} & \beta_2^{k-1} & \beta_3^{k-1} & \cdots & \beta_{k+1}^{k-1}\\ \beta_1^{k+1} & \beta_2^{k+1} & \beta_3^{k+1} & \cdots & \beta_{k+1}^{k+1}\end{vmatrix}$$

又因为

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{k+1} & x \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \cdots & \beta_{k+1}^2 & x^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \beta_3^{k-1} & \cdots & \beta_{k+1}^{k-1} & x^{k-1} \\ \beta_1^k & \beta_2^k & \beta_3^k & \cdots & \beta_{k+1}^k & x^k \\ \beta_1^{k+1} & \beta_2^{k+1} & \beta_3^{k+1} & \cdots & \beta_{k+1}^{k+1} & x^{k+1} \end{vmatrix} =$$

$$\prod_{i=1}^{k+1}(x-\beta_i)\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\triangleq$$

$$\sum_{i=0}^{k+1} b_i x^i$$

故

$$\det(\boldsymbol{G}_{k+1}^{\boldsymbol{v}_k}) = (-1)^{2k+3} b_k =$$

$$(-1)^{2k+3}(-1)\sum_{j=1}^{k+1}\beta_j\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i) =$$

$$\sum_{j=1}^{k+1}\beta_j\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)$$

故由引理4知，当 $p\geqslant 7$，$2\leqslant k\leqslant q-5$ 时，存在 $\{\beta_1,\beta_2,\cdots,\beta_{k+1}\}\subset\mathbb{F}_q^*$ 使得

$$\sum_{j=1}^{k+1}\beta_j = 0$$

从而有

$$\det(\boldsymbol{G}_{k+1}^{\boldsymbol{v}_k}) = 0$$

即 $\boldsymbol{G}^{\boldsymbol{v}_k}$ 中存在 $k+1$ 列线性相关. 据引理3知，$\boldsymbol{v}_k$ 不是 $RS_q(\mathbb{F}_q^*,k)$ 的深洞. 而

$$v(x)=\lambda v_k(x)+f_{\leqslant k-1}(x)$$

从而对于 $1\leqslant i\leqslant q-1$ 有

$$v(\alpha_i)=\lambda v_k(\alpha_i)+f_{\leqslant k-1}(\alpha_i)$$

即

$$\boldsymbol{v}=\lambda\boldsymbol{v}_k+f_{\leqslant k-1}$$

由引理2知，$\boldsymbol{v}$ 不是 $RS_q(\mathbb{F}_q^*,k)$ 的深洞. 定理2证毕.

3 结束语

在本文中，对于奇特征的有限域 $\mathbb{F}_q$ 上的 $RS_q(\mathbb{F}_q^*,k)$，我们证明当 $u(x)=\lambda x^{q-3}+f_{\leqslant k-1}(x)$ 或 $u(x)=\lambda x^{k+1}+f_{\leqslant k-1}(x)$ 时，$\boldsymbol{u}$ 不是标准Reed-Solomon码的深洞，其中 $\lambda\in\mathbb{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式. 由此在一定条件下部分证明了标准Reed-Solomon码的深洞猜想.

参考文献：

[1] 徐小凡，林宗兵，许 霞. 关于标准Reed-Solomon码的深洞猜想的注记[J]. 四川大学学报(自然科学版)，2016，53(5)：963－966.

[2] 徐小凡，谭千蓉. 关于Reed-Solomon码的平凡码字的注记[J]. 四川大学学报(自然科学版)，2014，51(1)：7－9.

[3] CHENG Q，MURRAY E. On Deciding Deep Holes of Reed-Solomon Codes[J]. Mathematics，2007(4484)：296－305.

[4] WU R，HONG S. On Deep Holes of Standard Reed-Solomon Codes[J]. Science China Math，2012，55：2447－2455.

[5] 张　俊，符方伟，廖群英. 广义 Reed-Solomon 码的深洞 [J]. 中国科学：数学，2013，43(7)：727－740.
[6] LI J，WAN D. On the Subset Sum Problem Over Finite Fields [J]. Finite Fields Appls，2008，14：911－929.
[7] 郑涛，吴荣军. 关于 Reed-Solomon 码的深洞的注记 [J]. 四川大学学报(自然科学版)，2009，46(4)：9－16.
[8] HONG S，WU R. On Deep Holes of Generalized Reed-Solomon Codes [J]. AIMS Mathematics，2016(1)：96－101.
[9] ZHUANG J，CHENG Q，LI J. On Determing Deep Holes of Generalized Reed-Solomon Codes [J]. IEEE Transactions on Information Theory，2016，62(1)：199－207.

A Remark on Error Distance of Standard Reed-Solomon Codes

XU Xiao-fan[1,2]，　XU　Xia[1]

1. *Sichuan Tourism University*，*Chengdu 610100*，*China*；
2. *Mathematical College*，*Sichuan University*，*Chengdu 610064*，*China*

Abstract：Reed-Solomon codes are now widely used in digital communication，which are an important class of maximum distance separable codes. The maximum likelihood decoding algorithm is usually used in the decoding process of Reed-Solomon codes. For the received word $\boldsymbol{u}\in\mathbb{F}_q^n$，maximum likelihood decoding algorithm lies in determining its error distance $d(\boldsymbol{u}, C)$. We have known that $d(\boldsymbol{u}, C)\leqslant n-k$，where n，k are the length and dimension of code C. If $d(\boldsymbol{u}, C)=n-k$，$\boldsymbol{u}$ then is called a deep hole of C. In this paper，we have partially proved a conjecture of deep hole of standard Reed-Solomon codes by using the generator matrix of maximum distance separable code.

Key words：Reed-Solomon code；MDS code；generator matrix；error distance

责任编辑　张　枸