Chin. Ann. Math.
32B(1), 2011, 89–98
DOI: 10.1007/s11401-010-0622-3

Chinese Annals of Mathematics, Series B

On Reed-Solomon Codes*

Qunying LIAO[1]

Abstract The complexity of decoding the standard Reed-Solomon code is a well-known open problem in coding theory. The main problem is to compute the error distance of a received word. Using the Weil bound for character sum estimate, Li and Wan showed that the error distance can be determined when the degree of the received word as a polynomial is small. In the first part, the result of Li and Wan is improved. On the other hand, one of the important parameters of an error-correcting code is the dimension. In most cases, one can only get bounds for the dimension. In the second part, a formula for the dimension of the generalized trace Reed-Solomon codes in some cases is obtained.

Keywords Reed-Solomon code, Weil bound, Error distance, Rational function, Trace Reed-Solomon code, Trace map
2000 MR Subject Classification 30P12, 32C12

1 On Improved Bounds for Error Distance of Standard Reed-Solomon Codes

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Fix a subset $\mathcal{D} = \{x_1, \cdots, x_n\} \subseteq \mathbb{F}_q$, which is called the evaluation set. The generalized Reed-Solomon code $\mathcal{C}_q(\mathcal{D}, k)$ of length n and dimension k over $\mathbb{F}_q$ is

$$\mathcal{C}_q(\mathcal{D}, k) = \{(f(x_1), \cdots, f(x_n)) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x],\ \deg f(x) \leq k-1\}.$$

Its elements are called codewords. The most widely used cases are $\mathcal{D} = \mathbb{F}_q$ or $\mathbb{F}_q^*$. These two cases are essentially equivalent. We call the case $\mathcal{D} = \mathbb{F}_q$ the standard Reed-Solomon code. Note that in other literature, the case $\mathcal{D} = \mathbb{F}_q^*$ is called standard.

For a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ and a word $u \in \mathbb{F}_q^n$, we define the error distance of u to the code $\mathcal{C}$ to be

$$d(u, \mathcal{C}) = \min_{v \in \mathcal{C}} d(u, v),$$

where $d(\ ,\ )$ denote the Hamming distance. It is clear that $d(u, \mathcal{C}) = 0$ if and only if u is a codeword. The covering radius of $\mathcal{C}$ is defined to be

$$\rho(\mathcal{C}) = \max_{u \in \mathbb{F}_q^n} d(u, \mathcal{C}).$$

Manuscript received July 26, 2009. Revised July 6, 2010. Published online December 28, 2010.
[1]Institution of Mathematics and Software Science, Sichuan Normal University, Chengdu 610066, China. E-mail: liao_ qunying@yahoo.com.cn
*Project supported by the National Natural Science Foundation of China (No. 10990011), the Doctoral Program Foundation of Ministry of Education of China (No. 20095134120001) and the Sichuan Province Foundation of China (No. 09ZA087).

The minimal distance of $\mathcal{C}$ is defined to be

$$d(\mathcal{C}) = \min_{u \neq v \in \mathcal{C}} d(u, v) = \min_{0 \neq v \in \mathcal{C}} d(0, v).$$

It is easy to see that the minimal distance of the generalized Reed-Solomon code $\mathcal{C}_q(\mathcal{D}, k)$ is $n-k+1$, and its covering radius ρ is $n-k$. The most important algorithmic problem in coding theory is the maximal likelihood decoding (MLD): given a word $u \in \mathbb{F}_q^n$, find a codeword $v \in \mathcal{C}$ such that $d(u, v) = d(u, \mathcal{C})$. The decision version of this problem is essentially computing the error distance $d(u, \mathcal{C})$ for a received word u. This is well-known to be NP-complete.

Given a received word $u \in \mathbb{F}_q^n$, if the error distance is small, say, $d(u, \mathcal{C}) \leq n - \sqrt{nk}$, then the list decoding algorithm of Sudan [11] and Guruswami-Sudan [5] provides a polynomial time algorithm for the decoding of u. When the error distance increases, the decoding becomes more complicated, in fact, NP-complete for generalized Reed-Solomon codes (see [7]).

For $u = (u_1, \cdots, u_n) \in \mathbb{F}_q^n$, let

$$u(x) = \sum_{i=1}^{n} u_i \frac{\prod\limits_{j \neq i} (x - x_j)}{\prod\limits_{j \neq i} (x_i - x_j)} \in \mathbb{F}_q[x],$$

that is, $u(x)$ is the unique polynomial of degree at most $n-1$ such that $u(x_i) = u_i$ for $1 \leq i \leq n$. For $u \in \mathbb{F}_q^n$, we define $\deg u := \deg u(x)$, called the degree of u. As mentioned above, the fundamental decoding problem is to compute the error distance $d(u, \mathcal{C})$ for received word $u \in \mathbb{F}_q^n$. It is clear that $d(u, \mathcal{C}) = 0$ if and only if $\deg u \leq k-1$. Without loss of generality, we can assume that $k \leq \deg u \leq n-1$.

Lemma 1.1 (see [8]) *For $k \leq \deg u \leq n-1$, we have the inequality*

$$n - \deg u \leq d(u, \mathcal{C}) \leq n - k = \rho.$$

In particular, the word u is called a deep hole if the above upper bound is an equality, i.e., if $d(u, \mathcal{C}) = n - k$. The word u is called ordinary if the above lower bound is an equality, i.e., if $d(u, \mathcal{C}) = n - \deg u$.

By definition, we have the following result.

Lemma 1.2 (see [8]) *Let $u \in \mathbb{F}_q^n$ be a word with $\deg u = k+d$, where $k+1 \leq k+d \leq n-1$. Then the error distance $d(u, \mathcal{C}) \leq n - k - r$ $(1 \leq r \leq d)$ if and only if there exists a subset $\{x_1, \cdots, x_{k+r}\} \subseteq \mathcal{D}$ and a monic polynomial $w(x) \in \mathbb{F}_q[x]$ of degree $d - r$ such that*

$$u(x) - v(x) = (x - x_1) \cdots (x - x_{k+r}) w(x)$$

for some $v(x) \in \mathbb{F}_q[x]$ with $\deg v(x) \leq k-1$.

From now on, we assume that $\mathcal{C}$ is the standard Reed-Solomon code $\mathcal{C}_q(\mathbb{F}_q, k)$. For the standard Reed-Solomon code $\mathcal{C}$, the complexity of decoding is unknown and much more subtle. It was shown in [2, 4] to be at least as hard as the discrete logarithm in a large extension $\mathbb{F}_{q^h}$, where h can be as large as $\sqrt{q}$. If $\deg u(x) = k$, then u is a deep hole. Based on numerical calculations, Cheng and Murray [1] conjectured that there are no other deep holes for standard

Reed-Solomon codes. As a theoretical evidence, they proved that their conjecture is true if $d := \deg u - k$ is small and q is sufficiently large compared to $d+k$. More precisely, they showed

Proposition 1.1 *Let $u \in \mathbb{F}_q^q$ such that $1 \le d := \deg u(x) - k \le q-k-1$. Assume that*

$$q \ge \max(k^{7+\varepsilon}, d^{\frac{13}{3}+\varepsilon})$$

for some constant $\epsilon > 0$. Then $d(u, \mathcal{C}) < q-k$, that is, u is not a deep hole.

For the words with small degree represented by a polynomial in $\mathbb{F}_q[x]$, Li and Wan [9] applied the method of Cheng and Wan [2] to study the error distance $d(u, \mathcal{C})$ for the standard Reed-Solomon code. They proved the following two results.

Proposition 1.2 (see [9, Theorem 1.4]) *Let $u \in \mathbb{F}_q^q$ be such that $1 \le d := \deg u(x) - k \le q-k-1$. Assume that*

$$q > \max((k+1)^2, d^{2+\varepsilon}), \quad k > \Big(\frac{2}{\varepsilon}+1\Big)d + \frac{8}{\varepsilon} + 2$$

for some constant $\epsilon > 0$. Then $d(u, \mathcal{C}) < q-k$, that is, u is not a deep hole.

More precisely, the error distance can be determined with a similar hypothesis.

Proposition 1.3 (see [9, Theorem 1.5]) *Let $u \in \mathbb{F}_q^q$ be such that $1 \le d := \deg u(x) - k \le q-k-1$. Assume that*

$$q > \max((k+1)^2, d^{2+\varepsilon}), \quad k > \Big(\frac{4}{\varepsilon}+1\Big)d + \frac{4}{\varepsilon} + 2$$

for some constant $\epsilon > 0$. Then $d(u, \mathcal{C}) = q-(k+d)$, that is, u is ordinary.

This result can be used to determine the error distance $d(u, \mathcal{C})$ only for the received word $u \in \mathbb{F}_q^q$ with small degree.

In this part, for the standard Reed-Solomon code $\mathcal{C} = \mathcal{C}_q(\mathbb{F}_q, k)$, we generalize the above results. In fact, we prove the following result.

Theorem 1.1 *Let $r \ge 1$ be an integer. For any received word $u \in \mathbb{F}_q^q$ with $u(x)$ as its interpolation polynomial of degree m, if $m \ge k+r$,*

$$q > \max\left\{2\binom{k+r}{2} + (m-k),\ (m-k)^{2+\varepsilon}\right\}$$

and

$$k > \frac{1}{1+\varepsilon}\Big(r + (2+\varepsilon)\Big(\frac{m}{2}+1\Big)\Big)$$

for some constant $\epsilon > 0$, then we have $d(u, \mathcal{C}) \le q-k-r$. So u is not a deep hole.

Taking $h = 0$ in the following proof and $r = 1$ or $m-k$ in Theorem 1.1, we get Propositions 1.2 and 1.3 respectively.

Proof Let $h(x)$ be a fixed monic polynomial in $\mathbb{F}_q[x]$ of degree $0 \le h \le \min\{m-k+1, k-1\}$ with no zero in $\mathbb{F}_q$. Let $\overline{h}(x) = x^{m-k+1}h(\frac{1}{x}) \in \mathbb{F}_q[x]$, $A = (\mathbb{F}_q[x]/(\overline{h}(x)))^*$ and $\widehat{A}$ denotes the set of all characters of A. Then $|\widehat{A}| = \Phi(\overline{h}(x)) \le q^{\deg \overline{h}(x)} - 1 = q^{m-k+1} - 1$, where $\Phi(\overline{h}(x))$ is

the Euler function of the polynomial $\overline{h}(x)$, i.e., $\Phi(\overline{h}(x))$ is equal to the number of units in A. Then $\widehat{B} = \{\chi \in \widehat{A} \mid \chi(\mathbb{F}_q^*) = 1\}$ is an abelian group of order $\leq q^{m-k}$.

For $g(x) \in \mathbb{F}_q[x]$, define

$$\chi(g(x)) = \begin{cases} \chi(g(x) (\mathrm{mod}\ \overline{h}(x))), & \text{if } \gcd(g(x), \overline{h}(x)) = 1, \\ 0, & \text{othserwise.} \end{cases}$$

This defines a multiplicative function of the polynomial ring $\mathbb{F}_q[x]$. By the Weil bound as given in [14], if $\chi \neq 1$ and $\chi(\mathbb{F}_q^*) = 1$, we have

$$\Big| \sum_{\substack{g(0)=1 \\ \deg g(x) = m-(k+r)}} \Lambda(g(x))\chi(g(x)) \Big| \leq (m-k) q^{\frac{m-(k+r)}{2}}, \tag{1.1}$$

where $\Lambda(g(x))$ is the Von-Mangoldt function on $\mathbb{F}_q[x]$, i.e., $\Lambda(g(x))$ is equal to $\deg P$ if g is a power of an irreducible polynomial P and is otherwise equal to zero.

For a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree at most $k - 1 - \deg h(x)$ (thus $f(x)$ represents a codeword), the sum

$$\frac{u(x)}{h(x)} + f(x) = \frac{u(x) + f(x)h(x)}{h(x)}$$

has at most $\deg u(x) = m$ roots in $\mathbb{F}_q$ since

$$\deg u(x) = m \geq k + h - 1 \geq \deg f(x)h(x).$$

Then by Lemma 1.2, we know that

$$d(u, \mathcal{C}) \leq q - k - r$$

if there exists a subset $\{x_1, \cdots, x_{k+r}\} \subseteq \mathbb{F}_q$ and a monic polynomial $v(x) \in \mathbb{F}_q[x]$ of degree $m - (k + r)$ such that $v(0) \neq 0$ and

$$(x - x_1) \cdots (x - x_{k+r}) v(x) = u(x) + f(x)h(x)$$

for some $f(x) \in \mathbb{F}_q[x],\ \deg f(x) \leq k - 1 - \deg h(x)$. This is equivalent to the equation

$$(1 - xx_1) \cdots (1 - xx_{k+r}) x^{m-(k+r)} v\Big(\frac{1}{x}\Big) = x^m u\Big(\frac{1}{x}\Big) + x^m f\Big(\frac{1}{x}\Big) h\Big(\frac{1}{x}\Big).$$

If we denote $\widetilde{u}(x) = x^m u\left(\frac{1}{x}\right)$, $\widetilde{h}(x) = x^h h\left(\frac{1}{x}\right)$, $\widetilde{f}(x) = x^{k-1-\deg h(x)} f\left(\frac{1}{x}\right)$, $\widetilde{v}(x) = x^{m-(k+r)} v\left(\frac{1}{x}\right)$, then

$$\begin{aligned} &\deg \widetilde{u}(x) = \deg u(x) = m, \quad && \deg \widetilde{h}(x) = \deg h(x) = h, \\ &\deg \widetilde{v}(x) = m - (k + r), && \deg \widetilde{f}(x) \leq k - 1 - \deg h(x). \end{aligned}$$

That is

$$(1 - xx_1) \cdots (1 - xx_{k+r}) \widetilde{v}(x) = \widetilde{u}(x) + x^{m-(k+h-1)} \widetilde{f}(x) \widetilde{h}(x). \tag{1.2}$$

By definition

$$\overline{h}(x) = x^{m-k+1} h\Big(\frac{1}{x}\Big) = x^{m-k-h+1} \widetilde{h}(x),$$

we have

$$x^{m-(k+h-1)}\widetilde{f}(x)\widetilde{h}(x) \equiv 0 \pmod{\overline{h}(x)}.$$

Thus the equation (1.2) is equivalent to the congruence

$$(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x) \equiv \widetilde{u}(x) \pmod{\overline{h}(x)}. \tag{1.3}$$

Since $(u(x), h(x)) = 1$ and $h(x)$ has no zero, $\deg u(x) = m$ and $\widetilde{u}(0) \neq 0$, we know that $(\overline{h}(x), \widetilde{u}(x)) = 1$. Thus (1.3) is equivalent to the congruence

$$(1-xx_1)\cdots(1-xx_{k+r})\frac{\widetilde{v}(x)}{\widetilde{u}(x)} \equiv 1 \pmod{\overline{h}(x)}.$$

The number of solutions of this congruence in x_i's is

$$N_u = \sharp\left\{(x_1,\cdots,x_{k+r},\widetilde{v}(x)) \;\middle|\; \begin{array}{l}(1-xx_1)\cdots(1-xx_{k+r})\dfrac{\widetilde{v}(x)}{\widetilde{u}(x)} \equiv 1 (\mathrm{mod}\ \overline{h}(x)),\ x_i \in \mathbb{F}_q,\\ \text{distinct},\ 1 \le i \le\ k+r,\ \widetilde{v}(0)=1,\ \deg\widetilde{v}(x) = m-(k+r)\end{array}\right\}.$$

Denote

$$N = \frac{1}{|\widehat{B}|}\sum_{\substack{x_i\in\mathbb{F}_q,\text{distinct}\\ 1\le i\le k+r}}\ \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\sum_{\chi\in\widehat{B}}\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big).$$

One can easily check that if $N > 0$, then $N_u > 0$. So, in order to show that $N_u > 0$, it is enough to show that $N > 0$. Since the second summand of the above formula is always non-negative, applying inclusion and exclusion principle, we deduce

$$\begin{aligned}N \ge \frac{1}{|\widehat{B}|}\Big\{&\sum_{\substack{x_i\in\mathbb{F}_q\\ 1\le i\le k+r}}\ \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\sum_{\chi\in\widehat{B}}\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big)\\ &-\sum_{1\le i<j\le k+r}\ \sum_{x_i=x_j\in\mathbb{F}_q}\ \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\sum_{\chi\in\widehat{B}}\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big)\Big\}.\end{aligned}$$

Separating the trivial character, we obtain

$$\begin{aligned}N \ge \frac{1}{|\widehat{B}|}\Big\{&q^m - \binom{k+r}{2}q^{m-1}\\ &+\sum_{\substack{\chi\in\widehat{B}\\ \chi\neq 1}}\ \sum_{\substack{x_i\in\mathbb{F}_q\\ 1\le i\le k+r}}\ \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big)\\ &-\sum_{\substack{\chi\in\widehat{B}\\ \chi\neq 1}}\ \sum_{1\le i<j\le k+r}\ \sum_{x_i=x_j\in\mathbb{F}_q}\ \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big)\Big\}.\end{aligned}$$

If χ is non-trivial and $\chi(\mathbb{F}_q^*) = 1$, Weil's estimate (see [14]) gives

$$\Big|\sum_{x_i\in\mathbb{F}_q}\chi(1-xx_i)\Big| = \Big|1+\sum_{a\in\mathbb{F}_q}\chi(x-a)\Big| \le (m-k)q^{\frac{1}{2}}.$$

Thus

$$\Big|\prod_{i=1}^{k+r}\sum_{x_i\in\mathbb{F}_q}\chi(1-x_ix)\Big| \le (m-k)^{k+r}q^{\frac{k+r}{2}}.$$

If $\chi^2 \neq 1$,

$$\Big| \sum_{1\le i<j\le k+r} \sum_{x_i=x_j\in\mathbb{F}_q} \chi((1-xx_1)\cdots(1-xx_{k+r}))\Big| \le (m-k)^{k+r-1} q^{\frac{k+r-1}{2}} \binom{k+r}{2}.$$

If $\chi \neq 1$ but $\chi^2 = 1$,

$$\Big| \sum_{1\le i<j\le k+r} \sum_{x_i=x_j\in\mathbb{F}_q} \chi((1-xx_1)\cdots(1-xx_{k+r}))\Big| \le (m-k)^{k+r-2} q^{\frac{k+r}{2}} \binom{k+r}{2}.$$

By (1.1), we know that for $\chi \neq 1$ and $\chi(\mathbb{F}_q^*) = 1$,

$$\Big| \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\chi(\widetilde{v}(x))\Big| \le (m-k) q^{\frac{m-(k+r)}{2}}.$$

Thus for $\chi \neq 1$ and $\chi(\mathbb{F}_q^*) = 1$,

$$\begin{aligned}
&\Big| \sum_{\substack{x_i\in\mathbb{F}_q\\ 1\le i\le k+r}} \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big)\\
&- \sum_{1\le i<j\le k+r} \sum_{x_i=x_j\in\mathbb{F}_q} \sum_{\substack{\widetilde{v}(x)\in\mathbb{F}_q[x],\widetilde{v}(0)=1\\ \deg\widetilde{v}(x)=m-(k+r)}} \Lambda(\widetilde{v}(x))\chi\Big(\frac{(1-xx_1)\cdots(1-xx_{k+r})\widetilde{v}(x)}{\widetilde{u}(x)}\Big)\Big|\\
&\le (m-k)^{k+r} q^{\frac{m}{2}} \Big(\binom{k+r}{2} + (m-k)\Big).
\end{aligned}$$

Since $|\widehat{B}| \le q^{m-k}$, we have

$$N \ge \frac{1}{|\widehat{B}|}\Big(\Big(q - \binom{k+r}{2}\Big)q^{m-1} - q^{m-k}(m-k)^{k+r} q^{\frac{m}{2}}\Big(\binom{k+r}{2} + (m-k)\Big)\Big).$$

By our assumption, $q > 2\binom{k+r}{2} + (m-k)$. To prove $N > 0$, it suffices to show that

$$q^{m-1} > q^{m-k}(m-k)^{k+r} q^{\frac{m}{2}}.$$

Now since $q > (m-k)^{2+\varepsilon}$ and $k > \frac{1}{1+\varepsilon}\big(r + (2+\varepsilon)(\frac{m}{2}+1)\big)$ for some constant $\varepsilon > 0$, we deduce that $N > 0$. Thus $N_u > 0$. The proof is completed.

2 A Formula for the Dimension of Trace Reed-Solomon Codes

One of the important parameters of an error-correcting code is the dimension. In most cases, we only have bounds for the dimension (see [10, Chapter 7, 12]). It is interesting to try to improve these bounds, or better, to determine the true dimension. This part is a contribution to the solution of the dimension problem for generalized Reed-Solomon codes in some cases.

For $1 \le k \le n \le q^m$, and the generalized Reed-Solomon code $\mathcal{C}_{q^m}[\mathcal{D}, k]$, the following code over $\mathbb{F}_q$

$$\mathrm{Tr}_{q^m}[\mathcal{D}, k] = \{(\mathrm{Tr}(f(x_1)), \cdots, \mathrm{Tr}(f(x_n))) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_{q^m}[x],\ \deg(f(x)) \le k-1\}$$

is called the trace Reed-Solomon code of $\mathcal{C}_{q^m}[\mathcal{D}, k]$, where Tr is the Trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

By the general bound for the dimension of the trace code given in [6], we have the following result.

Proposition 2.1 (Trivial Bound) (see [6, Lemma VIII. 1.3]) *For $1 \leq k \leq n \leq q^m - 1$, we have*

$$k \leq \dim_{\mathbb{F}_q} (\mathrm{Tr}_{q^m}[\mathcal{D}, k]) \leq mk.$$

In 1991, Marcel van der Vluge [12, 13] improved the above upper bound for the dimension of Reed-Solomon codes in some special cases. In this section, we obtain an explicit formula for the dimension of trace Reed-Solomon codes in some cases.

Theorem 2.1 *Let $n-1$ be a positive divisor of $q^m - 1$, $\mathcal{D} = \{x_1, \cdots, x_{n-1}\} \cup \{0\}$ and $\{x_1, \cdots, x_{n-1}\}$ be the subgroup of order $n-1$ of the multiplicative group $\mathbb{F}_{q^m}^*$. Suppose that $S = \{1, \cdots, n-1\} \cup \{0\}$ and q acts on S as follows:*

$$q : S \to S, \quad 0 \mapsto 0, \quad u \mapsto \langle qu \rangle, \quad \forall\, u \in S \setminus \{0\},$$

where $\langle qu \rangle$ denotes the least nonnegative residue of qu modulo $n-1$. For any $u \in S$, denote the q-orbit of u by

$$\Omega_u = \{u, \langle qu \rangle, \cdots, \langle q^{h_u - 1} u \rangle\},$$

where $h_u \in \mathbb{Z}^+$ is the least positive integer such that $q^{h_u} \cdot u \equiv u \pmod{n-1}$ and u is the smallest integer of Ω_u. Then

$$\dim_{\mathbb{F}_q} \mathrm{Tr}_{q^m}[\mathcal{D}, k] = mk - (m-1) \cdot \Big(1 + \sum_{\substack{u \in S/\sim \\ u \in [1, k-1]}} h_u\Big),$$

where " $\sim$ " is the equivalence relation on $S \times S$ given by the q-action on S.

Proof For the generalized Reed-solomon code

$$\mathcal{C}_{q^m}[\mathcal{D}, k] = \{(f(x_1), \cdots, f(x_n)) \,|\, f(x) \in \mathbb{F}_{q^m}[x],\ \deg f(x) \leq k-1\},$$

the trace code is defined to be

$$\mathrm{Tr}_{q^m}[\mathcal{D}, k] = \{(\mathrm{Tr}(f(x_1)), \cdots, \mathrm{Tr}(f(x_n))) \,|\, f(x) \in \mathbb{F}_{q^m}[x],\ \deg f(x) \leq k-1\},$$

where $\mathrm{Tr}(\alpha)$ is the trace map of $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Suppose that K_k is the kernel of the trace map TR which is defined to be

$$\begin{aligned} &\mathrm{TR} : \mathbb{F}_{q^m}[x]_{\leq k-1} \to \mathrm{Tr}_q[\mathcal{D}, k], \\ &f(x) \mapsto (\mathrm{Tr}(f(x_1)), \cdots, \mathrm{Tr}(f(x_n))), \end{aligned}$$

where $\mathbb{F}_{q^m}[x]_{\leq k-1}$ is the set of polynomials in $\mathbb{F}_{q^m}[x]$ with degree $\leq k-1$. Then

$$\dim_{\mathbb{F}_q} \mathrm{Tr}_{q^m}[\mathcal{D}, k] = \dim_{\mathbb{F}_q} \mathcal{C}_{q^m}[\mathcal{D}, k] - \dim_{\mathbb{F}_q} K_k = mk - \dim_{\mathbb{F}_q} K_k. \tag{2.1}$$

For any $u \in S$, set $f_u(x) = cx^u - c^q x^{\langle qu \rangle} \in \mathbb{F}_{q^m}[x]$. Then $\deg f_u(x) \leq q^m - 1$. Note that $qu \equiv \langle qu \rangle \pmod{n-1}$, thus $\forall\, \alpha \in \mathcal{D},\ \alpha^{\langle qu \rangle} = \alpha^{qu}$. This means that

$$\mathrm{Tr}(f_u(\alpha)) = \mathrm{Tr}(c\alpha^u) - \mathrm{Tr}(c^q \alpha^{\langle qu \rangle}) = \mathrm{Tr}(c\alpha^u) - \mathrm{Tr}(c^q \alpha^{qu}) = 0.$$

And so

$$\{cx^u - c^q x^{\langle qu\rangle} \,|\, u \in S,\ c \in \mathbb{F}_{q^m}\} \cap \{f(x) \in \mathbb{F}_{q^m}[x] \,|\, \deg f(x) \le k-1\} \subseteq K_k.$$

For a fixed $i = 1, \cdots, h_u$, set $A_i = \{cx^u - c^{q^i} x^{\langle q^i u\rangle} \,|\, c \in \mathbb{F}_{q^m}\}$. Take $\alpha \in \mathbb{F}_q$ and $f(x) = cx^u - c^{q^i} x^{\langle q^i u\rangle} \in A_i,\ g(x) = dx^u - d^{q^i} x^{\langle q^i u\rangle} \in A_i$. Then

$$f(x) - g(x) = (c-d)x^u - (c^{q^i} - d^{q^i})x^{\langle q^i u\rangle} = (c-d)x^u - (c-d)^{q^i} x^{\langle q^i u\rangle} \in A_i$$

and

$$\alpha f(x) = \alpha c x^u - \alpha c^{q^i} x^{\langle q^i u\rangle} = (\alpha c)x^u - (\alpha c)^{q^i} x^{\langle q^i u\rangle} \in A_i.$$

Hence, A_i is an $\mathbb{F}_q$-vector space. Furthermore, for any $f(x) \in A_i \cap A_j, 1 \le i \ne j \le h_u$, from

$$f(x) = cx^u - c^{q^i} x^{\langle q^i u\rangle} = dx^u - d^{q^j} x^{\langle q^j u\rangle},$$

we can get $g(x) = (c-d)x^u - c^{q^i} x^{\langle q^i u\rangle} + d^{q^j} x^{\langle q^j u\rangle} \equiv 0$. While $\deg g(x) \le q^m - 1$, thus $c = d$ and $c^{q^i} = d^{q^j} = 0$ or $c^{q^i} - d^{q^j} = 0$ according as $\langle q^i u\rangle = \langle q^j u\rangle$ or not. Fix a $u \in \{1, \cdots, n-1\}$ and $1 \le i \ne j \le h_u - 1$. By the definition of h_u, we have $\langle q^i u\rangle \ne \langle q^j u\rangle$. This means that $f(x) \equiv 0$, i.e., $A_i \cap A_j = \{0\},\ 1 \le i \ne j \le h_u - 1$. Therefore

$$V_u = \bigoplus_{i=1}^{h_u} \{cx^u - c^{q^i} x^{\langle q^i u\rangle} \,|\, c \in \mathbb{F}_{q^m}\}$$

is an $\mathbb{F}_q$-vector space of $\mathbb{F}_{q^m}[x]$, and $\dim_{\mathbb{F}_q} V_u = \sum_{i=1}^{h_u-1} \dim_{\mathbb{F}_q} A_i + \dim_{\mathbb{F}_q} A_{h_u}$.

Now from

$$A_{h_u} = \{cx^u - c^{q^{h_u}} x^{\langle q^{h_u} u\rangle} = cx^u - c^{q^{h_u}} x^u \,|\, c \in \mathbb{F}_{q^m}\}$$

and

$$A_i = \{cx^u - c^{q^i} x^{\langle q^i u\rangle} \,|\, c \in \mathbb{F}_{q^m}\}, \quad \forall\, i = 1, \cdots, h_u - 1,$$

we have

$$\dim_{\mathbb{F}_q} A_{h_u} = m - h_u, \quad \dim_{\mathbb{F}_q} A_i = m, \quad \forall\, i = 1, \cdots, h_u - 1.$$

Namely,

$$\dim_{\mathbb{F}_q} V_u = \sum_{i=1}^{h_u-1} m + (m - h_u) = h_u \cdot m - h_u.$$

And so

$$\dim_{\mathbb{F}_q} V = \sum_{u \in S/\sim} h_u(m-1) = n(m-1),$$

where $V = \bigoplus_{u \in S/\sim} V_u$, " $\sim$ " is the equivalence relation on $S \times S$ given by the q-action on S. Taking $f(x) \in V$ and $\alpha \in \mathcal{D}$, we have $\mathrm{Tr}(f(\alpha)) = 0$, which means that $V \subseteq \mathrm{Ker}\, T$, where the map T is defined to be

$$\begin{aligned} &T : \mathbb{F}_{q^m}[x]_{\le n-1} \to \mathbb{F}_q^m, \\ &f(x) \mapsto (\mathrm{Tr}(f(x_1)), \cdots, \mathrm{Tr}(f(x_n))). \end{aligned}$$

On the other hand, it is well-known that the trace map is surjective, hence $\dim_{\mathbb{F}_q} \operatorname{Ker} T = m \cdot n - n = n(m-1) = \dim_{\mathbb{F}_q} V$, and then $V = \operatorname{Ker} T$. Therefore

$$\begin{aligned} K_k &= \operatorname{Ker} T \cap \mathbb{F}_{q^m}[x]_{\le k-1} = V \cap \mathbb{F}_{q^m}[x]_{\le k-1} \\ &= \bigoplus_{\substack{u \in S/\sim \\ u \in [0,k-1]}} \bigoplus_{\langle q^i u \rangle \le k-1}^{h_u} \{c_i x^u - c_i^{q^i} x^{\langle q^i u \rangle} \mid c_i \in \mathbb{F}_{q^m}\}. \end{aligned}$$

Thus

$$\dim_{\mathbb{F}_q} K_k = m - 1 + (m-1) \cdot \sum_{\substack{u \in S/\sim \\ u \in [1,k-1]}} h_u.$$

Now from (2.1) we immediately have

$$\dim_{\mathbb{F}_q} \operatorname{Tr}_{q^m}[\mathcal{D}, k] = mk - (m-1) \cdot \Big(1 + \sum_{\substack{u \in S/\sim \\ u \in [1,k-1]}} h_u\Big).$$

Corollary 2.1 *With the assumptions as in Theorem* 2.1*, we have*

$$\begin{aligned} &mk - (m-1) \cdot \Big(1 + \sum_{u \in [1,k-1]/\sim} m\Big) \\ &\le \dim_{\mathbb{F}_q} Tr_{q^m}[\mathcal{D}, k] \le mk - (m-1) \cdot \Big(1 + \sum_{u \in [1,k-1]/\sim} 1\Big) < mk, \end{aligned}$$

where $\sim$ is the equivalent relation given by the q-action on S.

Proof Since $n-1$ is a positive divisor of $q^m - 1$, $q^m \equiv 1 \pmod{n-1}$. Note that $qu \equiv \langle qu \rangle \pmod{n-1}$ and $\Omega_u = \{u, \langle qu \rangle, \cdots, \langle q^{h_u - 1} u \rangle\}$ is the q-orbit of u. Therefore $h_u | m$, and so

$$\begin{aligned} &mk - (m-1) \cdot \Big(1 + \sum_{u \in [1,k-1]/\sim} m\Big) \\ &\le \dim_{\mathbb{F}_q} \operatorname{Tr}_{q^m}[\mathcal{D}, k] \le mk - (m-1) \cdot \Big(1 + \sum_{u \in [1,k-1]/\sim} 1\Big) < mk, \end{aligned}$$

Taking $\mathcal{D} = \mathbb{F}_{q^m}$ in Theorem 2.1, we get a formula for the dimension of the standard trace Reed-Solomon code.

Corollary 2.2 *Let $S = \{1, \cdots, q^m - 1\} \cup \{0\}$. Suppose that q acts on the set S as follows:*

$$\begin{aligned} q : S &\to S \\ 0 &\mapsto 0, \\ u &\mapsto \langle qu \rangle, \quad \forall\, u \in S \backslash \{0\}, \end{aligned}$$

where $\langle qu \rangle$ denotes the residue of qu modulo $q^m - 1$. $\forall u \in S$, denote the q-orbit of u to be

$$\Omega_u = \{u, \langle qu \rangle, \cdots, \langle q^{h_u - 1} u \rangle\},$$

where $h_u = |\Omega_u|$ and u is the smallest integer in Ω_u. Then

$$\dim_{\mathbb{F}_q} \operatorname{Tr}_{q^m}[\mathbb{F}_{q^m}, k] = mk - (m-1) \cdot \Big(1 + \sum_{\substack{u \in S/\sim \\ u \in [1,k-1]}} h_u\Big).$$

And so

$$mk-(m-1)\cdot\Big(1+\sum_{u\in[1,k-1]/\sim} m\Big)$$
$$\le \dim_{\mathbb{F}_q}\mathrm{Tr}_{q^m}[\mathbb{F}_{q^m},k]\le mk-(m-1)\cdot\Big(1+\sum_{u\in[1,k-1]/\sim}1\Big)<mk,$$

where $\sim$ is the equivalent relation given by the q-action on S.

Acknowledgement The author would like to thank Professor Daqing Wan for some helpful discussions.

References

[1] Cheng, Q. and Murray, E., On deciding deep holes of Reed-Solomon codes, Proceedings of TAMC 2007, Lecture Notes in Computer Science, **4484**, Springer-Verlag, Berlin, 2007, 296–305.

[2] Cheng, Q. and Wan, D. Q., On the list and bounded distance decodibility of the Reed-Solomon codes (extended abstract), Proc. 45th IEEE Symp. On Foundation of Comp. Sciences (FOCS), Rome, 2004, 335–341.

[3] Cheng, Q. and Wan, D. Q., On the list and bounded distance decodibility of Reed-Solomon codes, *SIAM J. Comput.*, **37**(1), 2007, 195–209.

[4] Cheng, Q. and Wan, D. Q., Complexity of decoding positive rate Reed-Solomon codes, 35-th International Colloquium on Automata, Languages and Programming (ICALP08), Lecture Notes in Computer Science, **5125**, Springer-Verlag, Berlin, 2008, 283–293.

[5] Guruswami, V. and Sudan, M., Improved decoding of Reed-Solomon and algebraic-geometry codes, *IEEE Transactions on Information Theorey*, **45**(6), 1999, 1757–1767.

[6] Henning, S., Algebraic Functions Fields and Codes, Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[7] Guruswami, V. and Vardy, A., Maximal-likelihood decoding of Reed-Solomon codes is NP-hard, *IEEE Transactions on Information Theory*, **51**(7), 2005, 2249–2256.

[8] Li, J. Y. and Wan, D. Q., On the subset sum problem over finite fields, *Finite Fields and Appl.*, **14**(4), 2008, 911–929.

[9] Li, Y. J. and Wan, D. Q., On error distance of Reed-Solomon codes, *Sci. China Ser. A*, **51**(11), 2008, 1982–1988.

[10] Macwilliams, F. J. and Sloane, N. J., The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.

[11] Sudan, M., Decoding of Reed-Solomon codes beyond the error-correction bound, *J. Complexity*, **13**, 1997, 180–193.

[12] van der Vlugt, M., On the dimension of trace codes, *IEEE Transactions on Information Theory*, **37**(1), 1991, 196–199.

[13] van der Vlugt, M., A new upper bound for the dimension of trace codes, *Bull. London Math. Soc.*, **23**, 1991, 395–400.

[14] Wan, D. Q., Generators and irreducible polynomials over finite fields, *Mathematics of Computation*, **66**, 1997, 1195–1212.