Science in China Series A: Mathematics
www.scichina.com math.scichina.com
www.springerlink.com

© 2008 SCIENCE IN CHINA PRESS
Springer

On error distance of Reed-Solomon codes

LI YuJuan[1†] & WAN DaQing[2]

[1] Institute of Mathematics, Chinese Academy of Sciences, Beijing 100080, China
[2] Department of Mathematics, University of California, Irvine, CA 92697-3875, USA
(email: liyj@amss.ac.cn, dwan@math.uci.edu)

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, we show that the error distance can be determined precisely when the degree of the received word is small. As an application of our method, we give a significant improvement of the recent bound of Cheng-Murray on non-existence of deep holes (words with maximal error distance).

Keywords: Reed-Solomon code, error distance, deep hole, character sum

MSC(2000): 30P12, 32C12

1 Introduction

1.1 Generalized Reed-Solomon codes

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Fix a subset $\mathcal{D} = \{x_1, \ldots, x_n\} \subseteq \mathbb{F}_q$, 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

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

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 $d(\cdot, \cdot)$ denotes 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 $\rho(\mathcal{C}) = \max_{u \in \mathbb{F}_q^n} d(u, \mathcal{C})$. 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 maximum likelihood decoding (MLD): given a word $u \in \mathbb{F}_q^n$, find a codeword $v \in \mathcal{C}$

Received September 26, 2007; accepted January 16, 2008
DOI: 10.1007/s11425-008-0066-3

† Corresponding author

This work was supported by the Research Foundation for Doctor Programme (Grant No. ———) and the National Natural Science Foundation of China (Grant No. ——)

such that $d(u,v)=d(u,\mathcal{C})$. The decision version of this problem is essentially to compute the error distance $d(u,\mathcal{C})$ for a received word u. This is well known to be NP-complete.

In this section, we only consider the generalized Reed-Solomon code $\mathcal{C}=\mathcal{C}_q(\mathcal{D},k)$. Given a received word $u\in\mathbb{F}_q^n$, if the error distance is small, say, $d(u,\mathcal{C})\leqslant n-\sqrt{nk}$, then the list decoding algorithm of Sudan[1] and Guruswami-Sudan[2] 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[3].

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

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

that is, $u(x)$ is the unique polynomial of degree at most $n-1$ such that $u(x_i)=u_i$ for $1\leqslant i\leqslant n$. 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 $\deg(u)\leqslant k-1$. Without loss of generality, we can then assume that $\deg(u)\geqslant k$ and $u(x)$ is monic. The following simple bounds can be easily proved.

Lemma 1.1[4]**.** *For $k\leqslant\deg(u)\leqslant n-1$, we have the inequality*

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

Definition 1.2. *Let $u\in\mathbb{F}_q^n$ be a word with $k\leqslant\deg(u)\leqslant n-1$. 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 $d(u,\mathcal{C})=n-\deg(u)$.*

If $\deg(u)=k$, then the upper bound coincides with the lower bound. In this case, $d(u,\mathcal{C})=n-k$ and u is a deep hole. This immediately gives $(q-1)q^k$ deep holes. It would be interesting to determine all deep holes. We shall return to this problem shortly.

If $\deg(u)=k+1$, we can assume $u(x)$ is monic of the form $u(x)=x^{k+1}+bx^k+\cdots$. Then it is not hard to prove that u is not a deep hole if and only if there is a k-subset $\{x_{i_1},\dots,x_{i_k}\}$ of $\mathcal{D}$ such that $x_{i_1}+\cdots+x_{i_k}=b$. But this k-subset sum problem over finite fields for general $\mathcal{D}$ is well known to be NP-complete, even for each fixed odd prime p. This implies that decoding the generalized Reed-Solomon code is NP-complete[5].

For the standard Reed-Solomon code, the complexity of decoding is unknown and much more subtle. It was shown in [6] to be at least as hard as the discrete logarithm in some cases. In this paper, we apply the method of Cheng-Wan to studying the error distance $d(u,\mathcal{C})$ for the standard Reed-Solomon codes.

1.2 Standard Reed-Solomon codes

We shall now assume that $\mathcal{C}=\mathcal{C}(\mathbb{F}_q,k)$ is the standard Reed-Solomon code. If $\deg(u)=k$, then u is a deep hole. Based on numerical calculations, Cheng and Murray[5] 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

Theorem 1.3.[5] *Let $u \in \mathbb{F}_q^q$ such that $1 \leqslant d := \deg(u) - k \leqslant q-1-k$. Assume that $q \geqslant \max(k^{7+\epsilon}, d^{\frac{13}{3}+\epsilon})$, for some constant $\epsilon > 0$. Then $d(u, \mathcal{C}) < q-k$, that is, u is not a deep hole.*

The method of Cheng-Murray is to reduce the problem to the existence of a rational point on a hypersurface over $\mathbb{F}_q$. They showed that the resulting hypersurface is absolutely irreducible and then applied an explicit version of the Lang-Weil theorem. In this paper, we use Weil's character sum estimate and the approach of Cheng-Wan[6] to prove the following result.

Theorem 1.4. *Let $u \in \mathbb{F}_q^q$ such that $1 \leqslant d := \deg(u) - k \leqslant q-1-k$. Assume that*

$$q > \max((k+1)^2, d^{2+\epsilon}), \quad k > \left(\frac{2}{\epsilon}+1\right)d + \frac{8}{\epsilon} + 2,$$

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

Obviously, under the condition of $k > (\frac{2}{\epsilon}+1)d + \frac{8}{\epsilon} + 2$, Theorem 1.4 has greatly improved the result of Theorem 1.3.

In fact, our proof shows that under a similar condition, we can actually determine the error distance $d(u, \mathcal{C})$ precisely.

Theorem 1.5. *Let $u \in \mathbb{F}_q^q$ such that $1 \leqslant d := \deg(u) - k \leqslant q-1-k$. Assume that*

$$q > \max((k+d)^2,\ (d-1)^{2+\epsilon}), \quad k > \left(\frac{4}{\epsilon}+1\right)d + \frac{4}{\epsilon} + 2,$$

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

It may be worthwhile to point out that the second inequality $k > (\frac{2}{\epsilon}+1)d + \frac{8}{\epsilon} + 2$ in Theorem 1.4 is weaker than the second inequality $k > (\frac{4}{\epsilon}+1)d + \frac{4}{\epsilon} + 2$ in Theorem 1.5. The coefficient of d is $\frac{2}{\epsilon}+1$ instead of $\frac{4}{\epsilon}+1$. This shows that Theorem 1.4 is not a corollary of Theorem 1.5. That is why we will prove the two theorems in Section 2 separately. Otherwise, the same proof of Theorem 1.5 gives a more general result which includes Theorem 1.5 and a weaker version of Theorem 1.4 as special cases.

2 Proof of main theorems

We first review the theory of character sums in the form we need and give a lemma for convenience of the proofs below. Let $\mathbb{F}_q[x]$ be the polynomial ring in one variable over $\mathbb{F}_q$. Let $\chi : (\mathbb{F}_q[x]/(x^{d+1}))^* \to \mathbb{C}^*$ be a character from the invertible elements of the residue class ring to the non-zero complex numbers. For $g \in \mathbb{F}_q[x]$, define

$$\chi(g) = \begin{cases} \chi\left(g \bmod x^{d+1}\right), & \text{if } \gcd\left(g, x^{d+1}\right) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

This defines a multiplicative function of the polynomial ring $\mathbb{F}_q[x]$. By the Weil bound as given in [7], if $\chi \neq 1$, we have

$$\left| \sum_{\substack{g \text{ monic} \\ \deg(g)=d-1}} \chi(g) \right| \leqslant dq^{\frac{d-1}{2}}.$$

If $g(0)=0$, we have $\chi(g)=0$. Thus, if $\chi\neq 1$ and $\chi(\mathbb{F}_q^*)=1$, we have

$$\left|\sum_{\substack{g\in\mathbb{F}_q[x],g(0)=1\\ \deg(g)=d-1}}\chi(g)\right|\leqslant dq^{\frac{d-1}{2}}. \tag{1}$$

Lemma 2.1. *Let $u\in\mathbb{F}_q^n$ be a word with $\deg(u)=k+d$, where $k+1\leqslant k+d\leqslant n-1$. Then, the error distance $d(u,\mathcal{C})\leqslant n-k-r$ $(1\leqslant r\leqslant d)$ if and only if there exists a subset $\{x_1,\dots,x_{k+r}\}\subseteq\mathcal{D}$ and a monic polynomial $g(x)\in\mathbb{F}_q[x]$ of degree $d-r$ such that*

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

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

Proof. Since for $u,v\in\mathbb{F}_q^n$,

$$d(u,v)=n-\sharp\{\text{distinct roots in }\mathcal{D}\text{ of }u(x)-v(x)=0\}.$$

Thus, $d(u,\mathcal{C})\leqslant n-k-r$ if and only if there exists a subset $\{x_1,\dots,x_{k+r}\}\subseteq\mathcal{D}$ and a monic polynomial $g(x)\in\mathbb{F}_q[x]$ of degree $d-r$ such that $u(x)-v(x)=(x-x_1)\cdots(x-x_{k+r})g(x)$ for some $v(x)\in\mathbb{F}_q[x]$ and $\deg v\leqslant k-1$.

Proof of Theorem 1.4. Let $A=(\mathbb{F}_q[x]/(x^{d+1}))^*$ and $\hat{A}$ denotes the set of all characters of A. Let $\hat{B}=\{\chi\in\hat{A}\mid\chi(\mathbb{F}_q^*)=1\}$, an abelian subgroup of order q^d. For $u\in\mathbb{F}_q^q$, $\deg(u)=k+d$, where $k+1\leqslant k+d\leqslant q-1$, we may assume that

$$u(x)=x^{k+d}+u_1x^{k+d-1}+\cdots+u_dx^k+v(x),\quad \deg v\leqslant k-1.$$

Then by Lemma 2.1, we know that $d(u,\mathcal{C})\leqslant q-k-1$ if and only if there exists a subset $\{x_1,\dots,x_{k+1}\}\subseteq\mathbb{F}_q$ and a monic polynomial $h(x)\in\mathbb{F}_q[x]$ of degree $d-1$ such that

$$u(x)-v'(x)=(x-x_1)\cdots(x-x_{k+1})h(x)$$

for some $v'(x)\in\mathbb{F}_q[x]$, $\deg v'(x)\leqslant k-1$. It is enough to show that there exists a subset $\{x_1,\dots,x_{k+1}\}\subseteq\mathbb{F}_q$ and a polynomial $g(x)\in\mathbb{F}_q[x]$ of degree $d-1$ and $g(0)=1$ such that

$$1+u_1x+\cdots+u_dx^d+\gamma_{d+1}x^{d+1}+\cdots+\gamma_{d+k}x^{d+k}=(1-x_1x)\cdots(1-x_{k+1}x)g(x)$$

for some $\gamma_j\in\mathbb{F}_q$, $d+1\leqslant j\leqslant k+d$.

Let $f(x)=1+u_1x+\cdots+u_dx^d\in A$, and

$$\begin{aligned}N_f=\sharp\{(x_1,\dots,&x_{k+1},g(x))\mid f(x)\equiv(1-x_1x)\cdots(1-x_{k+1}x)g(x)(\bmod x^{d+1}),\\ &x_i\in\mathbb{F}_q,\ \text{distinct},\deg g(x)=d-1,g(0)=1\}.\end{aligned}$$

Using character sums, we have

$$N_f=\frac{1}{q^d}\sum_{\substack{x_i\in\mathbb{F}_q,\text{distinct}\\ 1\leqslant i\leqslant k+1}}\ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}}\ \sum_{\chi\in\hat{B}}\chi\left(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}\right).$$

Since the third summand is always non-negative, applying the Principle of Inclusion and Exclusion, we deduce

$$\begin{aligned} N_f \geqslant \frac{1}{q^d}\Bigg\{ & \sum_{\substack{x_i\in\mathbb{F}_q\\ 1\leqslant i\leqslant k+1}} \ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}} \ \sum_{\chi\in\hat{B}} \chi\bigg(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}\bigg) \\ & - \sum_{\substack{x_i=x_j\\ 1\leqslant i<j\leqslant k+1}} \ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}} \ \sum_{\chi\in\hat{B}} \chi\bigg(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}\bigg)\Bigg\}. \end{aligned}$$

Separating the trivial character, we obtain

$$\begin{aligned} N_f \geqslant \frac{1}{q^d}\Bigg\{ & q^{k+d} - \binom{k+1}{2} q^{k+d-1} \\ & + \sum_{\substack{\chi\in\hat{B}\\ \chi\neq 1}} \ \sum_{\substack{x_i\in\mathbb{F}_q\\ 1\leqslant i\leqslant k+1}} \ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}} \chi(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}) \\ & - \sum_{\substack{\chi\in\hat{B}\\ \chi\neq 1}} \ \sum_{\substack{x_i=x_j\\ 1\leqslant i<j\leqslant k+1}} \ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}} \chi\bigg(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}\bigg)\Bigg\}. \end{aligned}$$

If χ is non-trivial and $\chi(\mathbb{F}_q^*)=1$, Weil's estimate[7] gives

$$\bigg|\sum_{x_i\in\mathbb{F}_q}\chi(1-x_ix)\bigg| = \bigg|1+\sum_{a\in\mathbb{F}_q}\chi(x-a)\bigg| \leqslant (d-1)q^{\frac{1}{2}}. \tag{2}$$

Thus,

$$\bigg|\prod_{i=1}^{k+1}\sum_{x_i\in\mathbb{F}_q}\chi(1-x_ix)\bigg| \leqslant (d-1)^{k+1}q^{\frac{k+1}{2}};$$

if $\chi^2\neq 1$,

$$\bigg|\sum_{\substack{x_i=x_j\\ 1\leqslant i<j\leqslant k+1}}\chi((1-x_1x)\cdots(1-x_{k+1}x))\bigg| \leqslant (d-1)^k q^{\frac{k}{2}}\binom{k+1}{2};$$

if $\chi^2=1$,

$$\bigg|\sum_{\substack{x_i=x_j\\ 1\leqslant i<j\leqslant k+1}}\chi((1-x_1x)\cdots(1-x_{k+1}x))\bigg| \leqslant (d-1)^{k-1} q^{\frac{k+1}{2}}\binom{k+1}{2}.$$

By (2.0.1), we have known that for $\chi\neq 1$ and $\chi(\mathbb{F}_q^*)=1$,

$$\bigg|\sum_{\substack{g\in\mathbb{F}_q[x],g(0)=1\\ \deg g=d-1}}\chi(g)\bigg| \leqslant dq^{\frac{d-1}{2}}.$$

Thus,

$$\begin{aligned} \bigg| & \sum_{\substack{x_i\in\mathbb{F}_q\\ 1\leqslant i\leqslant k+1}} \ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}} \chi\bigg(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}\bigg) \\ & - \sum_{\substack{x_i=x_j\\ 1\leqslant i<j\leqslant k+1}} \ \sum_{\substack{g(x)\in\mathbb{F}_q[x],g(0)=1\\ \deg g(x)=d-1}} \chi\bigg(\frac{(1-x_1x)\cdots(1-x_{k+1}x)g(x)}{f(x)}\bigg)\bigg| \end{aligned}$$

$$\leqslant d^{k+2}q^{\frac{k+d}{2}}\left(\binom{k+1}{2}+1\right).$$

Then,

$$N_f \geqslant \frac{1}{q^d}\left(q^{k+d}-\binom{k+1}{2}q^{k+d-1}-q^d d^{k+2}q^{\frac{k+d}{2}}\left(\binom{k+1}{2}+1\right)\right).$$

Since $q>\max((k+1)^2,d^{2+\epsilon})$, $k>(\frac{2}{\epsilon}+1)d+\frac{8}{\epsilon}+2$, for some constant $\epsilon>0$, we deduce that $N_f>0$, i.e., u is not a deep hole.

Proof of Theorem 1.5. The proof is similar. Let $A=(\mathbb{F}_q[x]/(x^{d+1}))^*$ and $\hat{A}$ denotes the set of all characters of A and $\hat{B}=\{\chi\in\hat{A}\mid\chi(\mathbb{F}_q^*)=1\}$. For $u\in\mathbb{F}_q^q$, $\deg(u)=k+d$, where $k+1\leqslant k+d\leqslant q-1$, we may assume that

$$u(x)=x^{k+d}+u_1x^{k+d-1}+\cdots+u_dx^k+v(x),\ \deg v\leqslant k-1.$$

Then by Lemma 2.1, we know that $d(u,\mathcal{C})\leqslant q-k-d$ if and only if there exists a subset $\{x_1,\ldots,x_{k+d}\}\subseteq\mathbb{F}_q$ such that $u(x)-v'(x)=(x-x_1)\cdots(x-x_{k+d})$ for some $v'(x)\in\mathbb{F}_q[x]$, $\deg v'(x)\leqslant k-1$. It is enough to show that there exists a subset $\{x_1,\ldots,x_{k+d}\}\subseteq\mathbb{F}_q$ such that

$$1+u_1x+\cdots+u_dx^d+\gamma_{d+1}x^{d+1}+\cdots+\gamma_{d+k}x^{d+k}=(1-x_1x)\cdots(1-x_{k+d}x)$$

for some $\gamma_j\in\mathbb{F}_q$, $d+1\leqslant j\leqslant k+d$.

Let $f(x)=1+u_1x+\cdots+u_dx^d\in A$, and

$$N_f=\sharp\{(x_1,\ldots,x_{k+d})\mid f(x)\equiv(1-x_1x)\cdots(1-x_{k+d}x)\pmod{x^{d+1}},x_i\in\mathbb{F}_q,\text{distinct}\}.$$

Then

$$\begin{aligned}N_f&=\frac{1}{q^d}\sum_{\substack{x_i\in\mathbb{F}_q\\ \text{distinct}}}\sum_{\chi\in\hat{B}}\chi\left(\frac{(1-x_1x)\cdots(1-x_{k+d}x)}{f(x)}\right)\\&\geqslant\frac{1}{q^d}\left(\sum_{\substack{x_i\in\mathbb{F}_q\\1\leqslant i\leqslant k+d}}-\sum_{\substack{x_i=x_j\\1\leqslant i<j\leqslant k+d}}\right)\sum_{\chi\in\hat{B}}\chi\left(\frac{(1-x_1x)\cdots(1-x_{k+d}x)}{f(x)}\right)\\&\geqslant\frac{1}{q^d}\left\{q^{k+d}-\binom{k+d}{2}q^{k+d-1}+\sum_{\substack{\chi\in\hat{B}\\ \chi\neq1}}\sum_{\substack{x_i\in\mathbb{F}_q\\1\leqslant i\leqslant k+d}}\chi\left(\frac{(1-x_1x)\cdots(1-x_{k+d}x)}{f(x)}\right)\right.\\&\quad\left.-\sum_{\substack{\chi\in\hat{B}\\ \chi\neq1}}\sum_{\substack{x_i=x_j\\1\leqslant i<j\leqslant k+d}}\chi\left(\frac{(1-x_1x)\cdots(1-x_{k+d}x)}{f(x)}\right)\right\}.\end{aligned}$$

From (2.0.2), for $\chi\in\hat{B}$, $\chi\neq1$, we have

$$\left|\prod_{i=1}^{k+d}\sum_{x_i\in\mathbb{F}_q}\chi(1-x_ix)\right|\leqslant(d-1)^{k+d}q^{\frac{k+d}{2}};$$

If $\chi^2\neq1$,

$$\left|\sum_{\substack{x_i=x_j\\1\leqslant i<j\leqslant k+d}}\chi((1-x_1x)\cdots(1-x_{k+d}x))\right|\leqslant(d-1)^{k+d-1}q^{\frac{k+d-1}{2}}\binom{k+d}{2};$$

If $\chi^2 = 1$,

$$\left| \sum_{\substack{x_i = x_j \\ 1 \leqslant i < j \leqslant k+d}} \chi((1 - x_1 x) \cdots (1 - x_{k+d} x)) \right| \leqslant (d-1)^{k+d-2} q^{\frac{k+d}{2}} \binom{k+d}{2}.$$

Thus,

$$\left| \left(\sum_{\substack{x_i \in \mathbb{F}_q \\ 1 \leqslant i \leqslant k+d}} - \sum_{\substack{x_i = x_j \\ 1 \leqslant i < j \leqslant k+d}} \right) \chi\left(\frac{(1 - x_1 x) \cdots (1 - x_{k+d} x)}{f(x)} \right) \right| \leqslant (d-1)^{k+d} q^{\frac{k+d}{2}} \left(1 + \binom{k+d}{2} \right).$$

It follows that

$$N_f \geqslant \frac{1}{q^d} \left\{ q^{k+d} - \binom{k+d}{2} q^{k+d-1} - q^d (d-1)^{k+d} q^{\frac{k+d}{2}} \left(\binom{k+d}{2} + 1 \right) \right\}.$$

Since $q > \max((k+d)^2, (d-1)^{2+\epsilon})$, $k > (\frac{4}{\epsilon} + 1)d + \frac{4}{\epsilon} + 2$, for some constant $\epsilon > 0$, we deduce $N_f > 0$, i.e., $d(u, \mathcal{C}) \leqslant q - (k+d)$. On the other hand, by Lemma 1.1, we have known that $d(u, \mathcal{C}) \geqslant q - (k+d)$. Thus, we deduce $d(u, \mathcal{C}) = q - (k+d)$.

References

1 Sudan M. Decoding of Reed-Solomon codes beyond the error-correction bound. *J Complexity*, **13**: 180–193 (1997)

2 Guruswami V, Sudan M. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans Inform Theory*, **45**(6): 1757–1767 (1999)

3 Guruswami V, Vardy A. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. *IEEE Trans Inform Theory*, **51**(7): 2249–2256 (2005)

4 Li J, Wan D. On the subset sum problem over finite fields, preprint, 2

5 Cheng Q, Murray E. On deciding deep holes of Reed-Solomon codes. In: Proceedings of TAMC 2007, LNCS 4484, 296–305

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

7 Wan D. Generators and irreducible polynomials over finite fields. *Math Comp*, **66**(219): 1195– (1997)

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