ON DEEP HOLES OF GENERALIZED REED-SOLOMON CODES

RONGJUN WU AND SHAOFANG HONG*

ABSTRACT. Determining deep holes is an important topic in decoding Reed-Solomon codes. In a previous paper [8], we showed that the received word is a deep hole of the standard Reed-Solomon codes \([q - 1, k]_q\) if its Lagrange interpolation polynomial is the sum of monomial of degree \(q - 2\) and a polynomial of degree at most \(k - 1\). In this paper, we extend this result by giving a new class of deep holes of the generalized Reed-Solomon codes.

1. Introduction and the statement of the main result

Let \(F_q\) be the finite field of \(q\) elements with characteristic \(p\). Let \(D = \{x_1, ..., x_n\}\) be a subset of \(F_q\), which is called the evaluation set. The generalized Reed-Solomon code \(C_q(D, k)\) of length \(n\) and dimension \(k\) over \(F_q\) is defined as follows:

\[ C_q(D, k) = \{ (f(x_1), ..., f(x_n)) \in F_q^n | f(x) \in F_q[x], \deg f(x) \leq k - 1 \}. \]

If \(D = F_q^*\), it is called standard Reed-Solomon code. If \(D = F_q\), it is called extended Reed-Solomon code. For any \([n, k]_q\) linear code \(C\), the minimum distance \(d(C)\) is defined by

\[ d(C) := \min \{ d(x, y) | x \in C, y \in C, x \neq y \}, \]

where \(d(\cdot, \cdot)\) denotes the Hamming distance of two words which is the number of different entries of them and \(w(\cdot)\) denotes the Hamming weight of a word which is the number of its non-zero entries. Thus we have

\[ d(C) = \min \{ d(x, 0) | 0 \neq x \in C \} = \min \{ w(x) | 0 \neq x \in C \}. \]

The error distance to code \(C\) of a received word \(u \in F_q^n\) is defined by \(d(u, C) := \min \{ d(u, v) | v \in C \}\). Clearly \(d(u, C) = 0\) if and only if \(u \in C\). The covering radius \(\rho(C)\) of code \(C\) is defined to be \(\max \{ d(u, C) | u \in F_q^n \}\). For generalized Reed-Solomon code \(C = C_q(D, k)\), we have that the minimum distance \(d(C) = n - k + 1\) and the covering radius \(\rho(C) = n - k\). The most important algorithmic problem in coding theory is the maximum likelihood decoding (MLD): Given a received word, find a word \(v \in C\) such that \(d(u, v) = d(u, C)\) [5]. Therefore, it is very crucial to decide \(d(u, C)\) for the word \(u\). Sudan [6] and Guruswami-Sudan [2] provided a polynomial time list decoding algorithm for the decoding of \(u\) when \(d(u, C) \leq n - \sqrt{nk}\). When the error distance increases, the decoding becomes NP-complete for generalized Reed-Solomon codes [3].
When decoding the generalized Reed-Solomon code $C$, for a received word $u = (u_1, \ldots, u_n) \in F_q^n$, we define the Lagrange interpolation polynomial $u(x)$ of $u$ by

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

i.e., $u(x)$ is the unique polynomial of degree at most $n-1$ such that $u(x_i) = u_i$ for $1 \leq i \leq n$. For $u \in F_q^n$, we define the degree of $u(x)$ to be the degree of $u$, i.e., $\deg(u) = \deg(u(x))$. It is clear that $d(u, C) = 0$ if and only if $\deg(u) \leq k-1$. Evidently, we have the following simple bounds.

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

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

Let $u \in F_q^n$. If $d(u, C) = n - k$, then the word $u$ is called a deep hole. If $\deg(u) = k$, then the upper bound is equal to the lower bound, and so $d(u, C) = n - k$ which implies that $u$ is a deep hole. This immediately gives $(q-1)q^k$ deep holes. We call these deep holes the trivial deep holes. It is an interesting open problem to determine all deep holes.

Cheng and Murray [1] showed that for the standard Reed-Solomon code $[p-1, k]_p$ with $k < p^{1/3} - \epsilon$, the received vector $(f(\alpha))_{\alpha \in F_q^*}$ cannot be a deep hole if $f(x)$ is a polynomial of degree $k + d$ for $1 \leq d < p^{1/3} - \epsilon$. Based on this result they conjectured that there is no other deep holes except the trivial ones mentioned above. Li and Wan [5] use the method of character sums to obtain a bound on the non-existence of deep holes for extended Reed-Solomon code $C_q(F_q, k)$. Wu and Hong [8] found a counterexample to the Cheng-Murray conjecture [1] about standard Reed-Solomon codes.

Let $l$ be a positive integer. In this paper, we investigate the deep holes of generalized Reed-Solomon codes whose evaluation set $D := F_q \setminus \{a_1, \ldots, a_l\}$, where $a_1, \ldots, a_l$ are any fixed $l$ distinct elements of $F_q$. Our method here is different from [8]. Write $D = \{x_1, \ldots, x_{q-l}\}$. Let

$$f(D) := (f(x_1), \ldots, f(x_{q-l})), $$

for any $f(x) \in F_q[x]$. Then we can rewrite the generalized Reed-Solomon code with evaluation set $D$ to be

$$C_q(D, k) = \{f(D) \in F_q^{q-1} | f(x) \in F_q[x], \deg(f(x)) \leq k-1\}.$$

Actually, by constructing some suitable polynomials, we find a new class of deep holes. That is, we have the following result.

**Theorem 1.2.** Let $q \geq 4$ and $2 \leq k \leq q - l - 1$. For $1 \leq j \leq l$, define

$$(1.1) \quad u_j(x) := \lambda_j(x - a_j)^{q-2} + r_j(x),$$

where $\lambda_j \in F_q^*$ and $r_j(x) \in F_q[x]$ is a polynomial of degree at most $k-1$. Then the received words $u_1(D), \ldots, u_l(D)$ are deep holes of the generalized Reed-Solomon code $C_q(D, k)$.

The proof of Theorem 1.2 will be given in Section 2.

The materials presented here is part of the first author’s PhD thesis [7], which was finished on April 15, 2012.
2. The proof of Theorem 1.2

Evidently, for any \( x \in \mathbb{F}_q \), we have

\[
\prod_{i=1}^{q-l} (x - x_i) \prod_{j=1}^{l} (x - a_j) = x^q - x = 0,
\]

and for any \( x \in D \), we have

\[
N(x) := \prod_{i=1}^{q-l} (x - x_i) = 0.
\]

For \( f(x) \in \mathbb{F}_q[x] \), by \( \bar{f}(x) \in \mathbb{F}_q[x] \) we denote the reduction of \( f(x) \mod N(x) \). Therefore, for any \( x_i \in \bar{D} \), we have \( f(x_i) = \bar{f}(x_i) \).

First we give a lemma about error distance. In what follows, we let \( G \) denote the set of all the polynomials in \( \mathbb{F}_q[x] \) of degree at most \( k - 1 \).

**Lemma 2.1.** Let \( \#(D) = n \) and let \( u, v \in \mathbb{F}_q^n \) be two words. If \( u = \lambda v + f_{\leq k-1}(D) \), where \( \lambda \in \mathbb{F}_q^* \) and \( f_{\leq k-1}(x) \in \mathbb{F}_q[x] \) is a polynomial of degree at most \( k - 1 \), then

\[
d(u, C_q(D, k)) = d(v, C_q(D, k)).
\]

Furthermore, \( u \) is a deep hole of \( C_q(D, k) \) if and only if \( v \) is a deep hole of \( C_q(D, k) \).

**Proof.** From the definition of error distance we immediately get that

\[
d(u, C_q(D, k)) = \min_{g \in G} \{d(u, g(D))\}
\]

\[
= \min_{g \in G} d(\lambda v + f_{\leq k-1}(D), g(D))
\]

\[
= \min_{g \in G} d(\lambda v + f_{\leq k-1}(D), g(D) + f_{\leq k-1}(D))
\]

\[
= \min_{g \in G} d(\lambda v, g(D))
\]

\[
= \min_{g \in G} d(\lambda v, \lambda g(D)) \quad \text{(since} \ \lambda \neq 0)\]

\[
= \min_{g \in G} d(v, g(D))
\]

\[
= d(v, C_q(D, k)).
\]

So Lemma 2.1 is proved. \( \square \)

Now we are in the position to prove Theorem 1.2.

**Proof of Theorem 1.2.** Let \( f(x), g(x) \in \mathbb{F}_q[x] \). One can deduce that

\[
d(f(D), g(D)) = \# \{ x_i \in D \mid f(x_i) \neq g(x_i) \}
\]

\[
= \# \{ x_i \in D \mid f(x_i) - g(x_i) \neq 0 \}
\]

(2.1)

Then by Equation (2.1), we infer that

\[
d(f(D), C_q(D, k)) = \min_{h \in G} d(f(D), h(D))
\]

\[
= \min_{h \in G} \{ \#(D) - \# \{ x_i \in D \mid f(x_i) - h(x_i) = 0 \} \}
\]

(2.2)

\[
= q - l - \max_{h \in G} \# \{ x_i \in D \mid f(x_i) - h(x_i) = 0 \}.
\]
Let $1 \leq j \leq l$ and $f_j(x) := (x - a_j)^{q - 2} \in \mathbb{F}_q[x]$. For any $y \in D$, we have $y - a_j \neq 0$, and so $f_j(y) = \frac{1}{y - a_j}$. We claim that

\begin{equation}
\max_{h \in G} \# \{ y \in D \mid f_j(y) - h(y) = 0 \} = k. \tag{2.3}
\end{equation}

In order to prove the claim, we pick $k$ distinct elements $c_{j_1}, \ldots, c_{j_k}$ of $\mathbb{F}_q \setminus \{a_1 - a_j\}_{i=1}^l$ (since $k \leq q - l - 1$). Now we define a polynomial $g_j(x)$ of degree $k - 1$ as follows:

$$g_j(x) = \frac{1}{x} \left( 1 - \prod_{i=1}^k (1 - c_{j_i}^{-1}x) \right) \in \mathbb{F}_q[x].$$

Since for any $y \in D$, we have

$$f_j(y) - g_j(y - a_j) = \frac{1}{y - a_j} - g_j(y - a_j)$$

$$= \frac{1}{y - a_j} (1 - (y - a_j)g_j(y - a_j))$$

$$= \frac{1}{y - a_j} \prod_{i=1}^k (1 - c_{j_i}^{-1}(y - a_j)),$$

it then follows that $c_{j_1} + a_j, \ldots, c_{j_k} + a_j$ are the roots of $f_j(x) - g_j(x - a_j) = 0$ over $\mathbb{F}_q$. Noticing that $c_{j_1}, \ldots, c_{j_k} \in \mathbb{F}_q \setminus \{a_1 - a_j, \ldots, a_l - a_j\}$, we have $c_{j_1} + a_j, \ldots, c_{j_k} + a_j \in D$. Therefore

\begin{equation}
\# \{ y \in D \mid f_j(y) - g_j(y - a_j) = 0 \} = k. \tag{2.4}
\end{equation}

On the other hand, for any $h \in G$, $1 - (x - a_j)h(x) = 0$ has at most $k$ roots over $\mathbb{F}_q$, and so it has at most $k$ roots over $D$. But $\frac{1}{y - a_j} \neq 0$ for any $y \in D$. Thus

$$f_j(y) - h(y - a_j) = \frac{1}{y - a_j} - h(y - a_j)$$

$$= \frac{1}{y - a_j} (1 - (y - a_j)h(y - a_j)).$$

Hence for any $h \in G$, we have

\begin{equation}
\# \{ y \in D \mid f_j(y) - h(y) = 0 \} \leq k. \tag{2.5}
\end{equation}

From (2.4) and (2.5) we arrive at the desired result (2.3). The claim is proved.

Now from (2.2) and (2.3), we derive immediately that $d(f_j(D), C_q(D, k)) = q - l - k$. In other words, $f_j(D)$ is a deep hole of the generalized Reed-Solomon $C_q(D, k)$. Finally by Lemma 2.4, we know that $u_j(D)$ is a deep hole of $C_q(D, k)$. This completes the proof of Theorem 1.2. \hfill \Box

**REFERENCES**


MATHEMATICAL COLLEGE, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA
E-mail address: eugen.woo@163.com

YANGTZE CENTER OF MATHEMATICS, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA
E-mail address: sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com