Upper Bound of Code-word Number of Some Separating Codes

Ryul Kim, Myong-son Sihn, Ok-hyon Song
Faculty of Mathematics, Kim Il Sung University, Pyongyang, D. P. R. Korea

ABSTRACT
In this paper, we study upper bounds for separating codes. First, some new upper bound for restricted separating codes is proposed. Finally, we illustrate that the Upper Bound Conjecture for separating Reed-Solomon codes inherited from Silverberg's question holds true for almost all Reed-Solomon codes.

Keywords
Separating code, Fingerprinting, Silverberg's question

1. INTRODUCTION
Separating codes have their applications in collusion-secure fingerprinting for generic digital data, while they are also related to the other structures including hash family, intersection code and group testing. In this paper, since separating codes are powerful weapon of anti-collusion fingerprinting for generic data, many recent works were done in the literatures, e.g., [1]. Particularly, the upper bound on the number of code-words in separating codes for given alphabet size $q$ and code length $n$ has been considered. The strongest upper bound ever found for $w$−FP codes is as follows[2]:

$$M \leq (2w^2 - 3w + 2)q \left\lceil \frac{n(n-1)}{2w} \right\rceil - 2w^2 + 3w - 1,$$

where the result for $(w_1, w_2)$−separating codes was also suggested. Restricted separating codes were introduced in [3], and their behaviors such as the bound of code rate were investigated, e.g., [4] and [5]. They are supposed to have still wider application than separating codes, although their upper bound has not been studied in earlier works.

IPP(Identifiable Parent Property) code is another important class of fingerprinting codes. It can be easily proven that $w$−IPP implies $w$−SFP. The following facts are well known in fingerprinting code theory.

**Theorem 1.** (Theorem 4.4 in [6]) Let $C$ be a code of length $n$. If the minimum distance of $C$ satisfies $d > n(1-1/w^2)$, then $C$ is a $w$−IPP code.

**Theorem 2.** (Proposition 7 in [7]) Let $C$ be a code of length $n$. If the minimum distance of $C$ satisfies $d > n(1-1/w_1w_2)$, then $C$ is a $(w_1, w_2)$−separating code.

In [8], Silverberg considered applications of Reed-Solomon codes as well as other algebraic geometry codes to collusion-secure fingerprinting techniques, where he proposed the following open problem.

**Question 1.** Is it the case that all $w$−IPP Reed-Solomon codes satisfies the condition $d > n(1-1/w^2)$?

For Reed-Solomon codes, $d = n-k+1 = q-k$ which allows replacing in the above statement $d > n(1-1/w^2)$ with $k < (q-1)/w^2 + 1$. Since the number of code-words in Reed-Solomon code of dimension $k$ is $M = q^k$, it equals with $M \leq q^{\left\lceil n/w^2 \right\rceil}$. Thus, Silverberg’s problem conjectures the upper bound of IPP Reed-Solomon codes, which is exactly optimal if true from Theorem 1.

Silverberg’s problem was studied in [9]. They showed that a large family of Reed-Solomon codes holds Question 1 positive. What is interesting for their work is that the family satisfies more general fact. The main result of [9] is as follows. From now we denote Reed-Solomon code of dimension $k$ over GF$(q)$ by $RS_k(q)$.

**Theorem 3.** (Theorem 7 in [9]) Suppose that $k-1 | q-1$. If the code $RS_k(q)$ is $(w_1, w_2)$−separating, then

$$k < (q-1)/(w_1w_2) + 1.$$

We can easily check that Theorem 3 suggests the conjecture of the upper bound $M \leq q^{\left\lceil n/w^2 \right\rceil}$ for separating Reed-Solomon codes.
Question 2. (Upper Bound Conjecture of separating RS codes)
Is it the case that all \((w_j, w_2) - \)separating Reed-Solomon codes satisfy \(k \leq (q - I)/ (w_j w_2) + 1?\)

If Question 2 holds positive for all cases, then it turns out we obtain the optimal upper bound of separating Reed-Solomon codes by Theorem 2. The proof of that, however, is not easy. The goals of this paper is firstly, to get a new upper bound for restricted separating codes, and secondly to illustrate that almost all separating Reed-Solomon codes involving those of [9] allow the positive answer for Question 2.

2. MAIN RESULTS
Our new bound for restricted \((w, w) - \)separating code is stated in Theorem 4. Note that the bound is independent alphabet size \(q.\)

Theorem 4. Let \(w \geq 3\) be a positive integer. If \(C\) is a code of length \(n\) with \(M\) codeword and satisfies restricted \((w, w) - \)separation property, then

\[M \leq 2^{\left(n - w^2/2\right)} + w - 2\]

Proof. See [10].

Now we are dealing with separating codes included in Reed-Solomon codes family and are proving the Upper Bound Conjecture derived from Silverberg’s problem, which is to be optimal. Let \(GF(q)\) be a finite field of characteristic \(p\) with a primitive element \(\alpha.\) Denote the set of all non-zero polynomials over \(GF(q)\) of degree less than \(k\) by \(P_k.\) The proof of the following lemma is trivial.

Lemma 1. Assume that \(RS_k(q)\) is not \((w_j, w_2) - \)separating. Then

1. \(q - I \geq l \geq k\) implies that \(RS_k(q)\) is not \((w_j, w_2) - \)separating.
2. \(w_j \geq w_j, w_2 \geq w_2\) implies that \(RS_k(q)\) is not \((w_j, w_2) - \)separating.

In [9], they gave the equivalent condition with separation property of Reed-Solomon codes before they evolved the relation between \(k\) and \(q,\) namely, \(k - l \mid q - l.\) Similarly, we state the following sufficient condition for non-separation of Reed-Solomon codes at the first.

Lemma 2. Let \(f\) be a non-constant polynomial belonging to \(P_k.\) Suppose there exists two subsets \(E, F\) of \(Im f\) such that \(l \leq |E| \leq w_j, l \leq |F| \leq w_2\) and either of the two facts \(Im f = EF\) or \(Im f = E + F\) holds true. Then, the code \(C = RS_k(q)\) is not \((w_j, w_2) - \)separating.

Proof. See [10].

Lemma 2 allows us to discuss the relation between \(k, q, w_j, w_2\) that are parameters specifying separation property and Reed-Solomon codes to meet the positive answer about Question 2. First, we give a different proof of Theorem 3 using Lemma 2 to show generality of our results.

Proof of Theorem 3. Assume \(k \geq (q - I)/(w_j w_2) + 1\) and define \(f(x) = x^{k-1}\). Then \(f\) is a polynomial in \(P_k,\) while it is a multiplicative homomorphism over \(GF(q)\). Therefore \(Im f\) is a subgroup of \(GF(q)\), thus is cyclic. Let \(\gamma\) be a generator of \(Im f\), and set

\[E := \{\gamma^i \mid 0 \leq i \leq w_j - 1\}, F := \{\gamma^j \mid 0 \leq j \leq w_2 - 1\}.

Applying group theory, we get \(|Im f| = (q - I)/(k - 1) \leq w_j w_2\) and \(Im f = EF,\) since \(|Ker f| = k - 1.\) Thus, the conditions of Lemma 3 satisfies and \(RS_k(q)\) is not \((w_j, w_2) - \)separating. □

Here we are to find new relation of parameters for satisfying Upper Bound Conjecture in terms of Lemma 2. Let \(r_j := \log_p w_j, r_2 := \log_p w_2.\)

Theorem 5. Suppose \(k - l \mid q\) and at least one of the following conditions are true.

1. \(k - l \geq p q/(w_j w_2),\)
2. \((w_j / p^q)/(w_2 / p^q) < p,\)
3. \([w_j / p^q]/[w_2 / p^q] \geq p.\)

If \(RS_k(q)\) is \((w_j, w_2) - \)separating, then

\[k < (q - I)/(w_j w_2) + 1.\]

Proof. See [10].

If for some \(k\) we know that \((w_j, w_2) - \)separation property of \(RS_k(q)\) implies \(k < (q - I)/(w_j w_2) + 1,\) then for all integers larger than \(k\) the same holds true by Lemma 1. It inspired us to believe that all Reed-Solomon codes employs the conjecture. The following corollaries are simple to prove.

Corollary 1. Suppose that \(w_j w_2 \geq q - I\) or \(w_j w_2 \mid q - I.\) If the code \(RS_k(q)\) is \((w_j, w_2) - \)separating, then

\[k < (q - I)/(w_j w_2) + 1.\]

Corollary 2. Suppose \(w_j w_2 \mid q.\) If the code \(RS_k(q)\) is \((w_j, w_2) - \)separating, then \(k < (q - I)/(w_j w_2) + 1.\)

Table 1 shows the rate of solution to Silverberg’s open problem by containing frequencies of Reed-Solomon codes holding Question 2 positive for some \(w\) and \(q\) in case \(w = w_1 = w_2.\) The first row have the values of \(q,\) meanwhile the first column is of \(w.\) In each cell, the percent of the number of Reed-Solomon codes proven to be non-\((w_j, w_2) - \)separating against the total number of \(k\) satisfying the inequality \(q - I \geq k \geq (q - I)/(w_j w_2) + 1.\) The number of the left side is the rate proven by the works till [9], and the right side one shows the rate of our result.

Table 1 is a intuitive inspiration of Silverberg’s conjecture to state that almost all Reed-Solomon codes except few cases
with \( w \) in \( 2^{25} \) and \( q \) in \( 2^{4096} \) meets the optimal upper bound \( M \leq q^{\left\lceil n/m \right\rceil} \).

### Table 1. Solution Rates of Silverberg’s Problem
(Each cell, left side: previous result, right side: our result. Unit %)

<table>
<thead>
<tr>
<th>( w )</th>
<th>( 8 )</th>
<th>( 27 )</th>
<th>( 64 )</th>
<th>( 128 )</th>
<th>( 243 )</th>
<th>( 512 )</th>
<th>( 625 )</th>
<th>( 1024 )</th>
<th>( 2187 )</th>
<th>( 4096 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>100/100</td>
<td>100/100</td>
<td>29/100</td>
<td>54/54</td>
<td>76/100</td>
<td>25/100</td>
<td>50/50</td>
<td>25/100</td>
<td>100/100</td>
<td>75/100</td>
</tr>
<tr>
<td>3</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>23/100</td>
<td>100/100</td>
<td>12/47</td>
<td>78/78</td>
<td>90/90</td>
<td>33/45</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>57/100</td>
<td>6/100</td>
<td>73/73</td>
<td>44/100</td>
<td>100/100</td>
<td>69/100</td>
</tr>
<tr>
<td>5</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>5/38</td>
<td>91/91</td>
<td>29/33</td>
<td>100/100</td>
<td>44/44</td>
</tr>
<tr>
<td>6</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>67/67</td>
<td>25/100</td>
<td>83/83</td>
<td>52/100</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>2/100</td>
<td>36/36</td>
<td>100/100</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>2/100</td>
<td>36/36</td>
<td>100/100</td>
<td>100/100</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>100/100</td>
<td>75/100</td>
<td></td>
</tr>
</tbody>
</table>

3. CONCLUSION AND FUTURE WORK

The upper bounds for restricted separating codes as well as the separating Reed-Solomon codes and their optimality were dealt in the paper. Developing upper bounds for separating codes is still an important topic in theory and practice.

Restricted separation property is quite strong condition, thus it is assumed that the upper bound for them will be still smaller than the one of simple separating codes. Therefore, improvement of Theorem 4 could be a possible topic.

From the work of [9] to this paper, we confirmed that Silverberg’s conjecture is true in almost all cases and it derives the optimal upper bound of separating Reed-Solomon codes. Experimental results tell us that almost all (about 90 percent) Reed-Solomon codes except few cases with \( w \) in \( 2^{25} \) and \( q \) in \( 2^{4096} \) meets the optimal bound \( M \leq q^{\left\lceil n/m \right\rceil} \).

In-depth study on separating codes and algebraic geometry codes seems to allow the complete solution to Silverberg’s open problem.

4. ACKNOWLEDGMENTS

Authors thank to the managing editor Yaser Sadra and the anonymous referees for kindly inviting and reviewing my article and giving advice.

5. REFERENCES


