<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Constructions for difference triangle sets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Chee, Yeow Meng; Colbourn, Charles J.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>1997</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/6191">http://hdl.handle.net/10220/6191</a></td>
</tr>
</tbody>
</table>

© 2009 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE. This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.
Constructions for Difference Triangle Sets

Yeow Meng Chee and Charles J. Colbourn

Abstract—Difference triangle sets are useful in many practical problems of information transmission. This correspondence studies combinatorial and computational constructions for difference triangle sets having small scopes. Our algorithms have been used to produce difference triangle sets whose scopes are the best currently known.

Index Terms—Algorithms, difference packings, difference triangle sets.

I. INTRODUCTION

An \((n, k)\)-difference triangle set, or \((n, k)\)-D\(\Delta\)S, is a set \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), for \(1 \leq i \leq n\), are sets of integers called blocks, such that the differences \(a_{ij} - a_{ij'}\) for \(1 \leq i \leq n\) and \(0 \leq j \neq j' \leq k\), are all distinct and nonzero. An \((n, k)\)-D\(\Delta\)S is normalized if for \(1 \leq i \leq n\), we have \(0 = a_{i0} < a_{i1} < \cdots < a_{ik}\). All difference triangle sets considered in this correspondence are normalized. The scope of an \((n, k)\)-D\(\Delta\)S, \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), is defined as

\[
m(n, k) = \max \left\{ a \mid a \in \bigcup_{i=1}^{n} X_i \right\}.
\]

The smallest scope possible for an \((n, k)\)-D\(\Delta\)S is

\[
m(n, k) = \min \{m(\mathcal{X})|\mathcal{X}\text{ is an } (n, k)\)-D\(\Delta\)S\}.
\]

An \((n, k)\)-D\(\Delta\)S \(\mathcal{X}\) is optimal if \(m(\mathcal{X}) = m(n, k)\). By counting differences, we easily obtain the trivial lower bound

\[
m(n, k) \geq \binom{n + k + 1}{2}.
\]

Better lower bounds can be found in the papers of Kløve [1], [2]. In particular, we have the following result [1, Theorem 2].

\[m(n, k) \geq \binom{k^2 - 2k\sqrt{k} + \frac{k + \sqrt{k}}{4}}{2}.
\]

Given an \((n, k)\)-D\(\Delta\)S \(\mathcal{X}\), we can obtain an \((n - 1, k)\)-D\(\Delta\)S by omitting from \(\mathcal{X}\) the block containing the largest element. This operation is called a reduction. The operation of omitting the largest element from each block of \(\mathcal{X}\) is called shortening, and this gives an \((n, k - 1)\)-D\(\Delta\)S instead.

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

The existence of a regular \((n, k + 1, C)\)-PSDS gives an \((n, k)\)-D\(\Delta\)S of scope \(C + 1 - n\left(\frac{k + 1}{2}\right)\). There are infinitely many values of \(n\) for which \(m(n, 3) = 6n\).

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

The existence of a regular \((n, k + 1, C)\)-PSDS gives an \((n, k)\)-D\(\Delta\)S of scope \(C + 1 - n\left(\frac{k + 1}{2}\right)\). There are infinitely many values of \(n\) for which \(m(n, 3) = 6n\).

Better lower bounds can be found in the papers of Kløve [1], [2]. In particular, we have the following result [1, Theorem 2].

\[m(n, k) \geq \binom{k^2 - 2k\sqrt{k} + \frac{k + \sqrt{k}}{4}}{2}.
\]

Given an \((n, k)\)-D\(\Delta\)S \(\mathcal{X}\), we can obtain an \((n - 1, k)\)-D\(\Delta\)S by omitting from \(\mathcal{X}\) the block containing the largest element. This operation is called a reduction. The operation of omitting the largest element from each block of \(\mathcal{X}\) is called shortening, and this gives an \((n, k - 1)\)-D\(\Delta\)S instead.

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

Better lower bounds can be found in the papers of Kløve [1], [2]. In particular, we have the following result [1, Theorem 2].

\[m(n, k) \geq \binom{k^2 - 2k\sqrt{k} + \frac{k + \sqrt{k}}{4}}{2}.
\]

Given an \((n, k)\)-D\(\Delta\)S \(\mathcal{X}\), we can obtain an \((n - 1, k)\)-D\(\Delta\)S by omitting from \(\mathcal{X}\) the block containing the largest element. This operation is called a reduction. The operation of omitting the largest element from each block of \(\mathcal{X}\) is called shortening, and this gives an \((n, k - 1)\)-D\(\Delta\)S instead.

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]

There is a restricted variant of difference triangle sets, called regular perfect systems of difference sets (see [3] and [4]), that is widely studied in combinatorial design theory. Let \(C\) be a positive integer. An \((n, k)\)-D\(\Delta\)S \(\mathcal{X} = \{X_i|1 \leq i \leq n\}\), where \(X_i = \{a_{ij}|0 \leq j \leq k\}\), is a regular \((n, k + 1, C)\)-PSDS if

\[
\sum_{i=1}^{n}(a_{ij} - a_{ij'}) \leq C + 1 - n\left(\frac{k + 1}{2}\right).
\]
Lemma 1 (Chen, Fan, and Jin): An \(n-D P(v, k)\) is an \((n, k-1)-D\Delta S\), whose scope is at most \(v - 1\).

Furthermore, using Singer’s construction [17] of \(1-DP(q^2 + q + 1)\) for prime powers \(q\) and a technique of Colbourn and Colbourn [18], they constructed two infinite families of difference packings, one of which is given below.

Theorem 3 (Chen, Fan, and Jin): For any prime power \(q\) and prime \(n > q\), there exists an \(n-DP(nq^2 + q + 1), q + 1\).

It is known [1, Theorem 6] that for any fixed \(k\)

\[
\lim_{n \to \infty} m(n, k)/n!k!^2
\]

exists and equals one. Here, we show that the same conclusion holds even if one allows \(k\) to grow with \(n\), provided that it does not grow too fast. The following result of Heath-Brown and Iwaniec [19] on differences between consecutive primes is useful.

Theorem 4 (Heath-Brown and Iwaniec): Let \(p_n\) denote the \(n\)th prime. Then

\[
P_{n+1} - p_n \ll p_n^{11/20 + \epsilon}
\]

for any \(\epsilon > 0\).

Theorem 5: Let \(n\) and \(k\) be positive integers such that \(n > k\) or \(n = 1\). Then there exists an \((n, k)-D\Delta S\) whose scope is at most \((1 + o(1))n!k^2\), where the \(o(1)\) is with respect to \(k\).

Proof: Suppose \(n > k\). Let \(p\) and \(q\) be the smallest prime at least \(n\) and \(k\), respectively, such that \(p > q\). Then Theorem 3 assures us of the existence of a \(p-DP(p(q^2 + q + 1), q + 1)\). This difference packing is a \((p, q)-D\Delta S\) by Lemma 1. Hence, by repeated shortening and reduction (if necessary), we obtain an \((n, k)-D\Delta S\) whose scope \(m\) is upper-bounded by \(p(q^2 + q + 1)\). However, Theorem 4 implies that

\[
p(q^2 + q + 1) \leq (1 + o(1))n!k^2.
\]

For \(n = 1\), we use Singer’s \(1-DP(q^2 + q + 1, q + 1)\) and follow the same argument above.

Corollary 1: Let \(k = f(n)\), where \(f\) is an increasing function such that \(\lim_{n \to \infty} f(n)/n < 1\). Then

\[
\lim_{n \to \infty} \frac{m(n, k)}{n!k^2} = 1.
\]

Proof: For \(n\) large enough, we have \(k < n\) and Theorem 5 can be used to give an \((n, k)-D\Delta S\) of scope at most \((1 + o(1))n!k^2\). This, together with Theorem 1 yields the desired result.

The trivial partial \((n, k)-D\Delta S\) is the empty set, \(\{\}\). For any fixed \(n\), \((n, k)-D\Delta S\) is a partial \((n, k)-D\Delta S\) that is a subset of \((X, \{\})\) for any \(X\). Let \(R(n, k)\) denote the set of all \((n, k)-D\Delta S\) that have a representation by an \(n \times (k + 1)\) array \(R = (r_{ij})\), \(1 \leq i \leq n\) and \(0 \leq j \leq k\), where each cell is either empty or contains a nonnegative integer. The entries of the nonempty cells in row \(i\) of \(R\) are exactly the members of \(X_i\). Let \(R(n, k)\) denote the set of all \((n, k)-D\Delta S\) that have a representation by an \(n \times (k + 1)\) array \(R = (r_{ij})\), \(1 \leq i \leq n\) and \(0 \leq j \leq k\), where each cell is either empty or contains a nonnegative integer. The entries of the nonempty cells in row \(i\) of \(R\) are exactly the members of \(X_i\).

IV. Greedy Algorithms

We define a partial \((n, k)-D\Delta S\) to be a set \(X = \{X_i\mid 1 \leq i \leq s\}\) satisfying all of the following conditions:

1) \(s \leq n\).
2) \(|X_i| = k_i + 1 \leq k + 1\), for \(1 \leq i \leq s\).
3) \(X_i = \{a_{ij}\mid 0 \leq j \leq k_i\}\) is such that

\[
0 = a_{i0} < a_{i1} \leq \ldots \leq a_{ik_i},
\]

for \(1 \leq i \leq s\).
4) The differences \(a_{ij} - a_{i,j'}\), for \(1 \leq i \leq s\) and \(0 \leq j \neq j' \leq k\) are all distinct and nonzero.

The greedy algorithms we propose can be conveniently described in terms of these array-representations for difference triangle sets.

Our first algorithm, called the set-greedy algorithm, works as follows. We begin with \(R(n, k)\) at each stage of the algorithm, we pick the smallest \(i\) such that the \(i\)th row contains an empty cell. We place in this empty cell the smallest positive integer such that the resulting array remains a representation of a partial \((n, k)-D\Delta S\). The algorithm terminates when the array contains no empty cells. The idea behind this algorithm is to fill the empty cells of \(R(n, k)\) in a row-by-row manner. This suggests the following variant which fills in the empty cells of \(R(n, k)\) column-wise.

The transversal-greedy algorithm also starts with \(R(n, k)\). At each stage of the algorithm, we pick the smallest \(j\) such that the \(j\)th column contains an empty cell. We then fill in the first empty cell of this column with the smallest positive integer so that the resulting array remains a representation of a partial \((n, k)-D\Delta S\). The algorithm terminates when the array contains no empty cells.

In the following sections, we turn to faster heuristics for constructing difference triangle sets.

III. Exhaustive Search

In principle, to construct an \((n, k)-D\Delta S\) of scope \(m\), we must consider all possible sets of \(n\) subsets from a universe of size \(\binom{n}{r}\). This is only feasible for small values of \(n\) and \(k\). Nevertheless, the main advantage of exhaustive search is that it allows us to prove the nonexistence of \((n, k)-D\Delta S\) of certain scopes.

The existing results on difference triangle sets present few unknown values of \(m(n, k)\) that can be determined exactly with today’s technology. The determination of \(m(2, 7)\) is one of these possibilities. It is known that \(61 \leq m(2, 7) \leq 73\) (see [1]). We proved that \(m(2, 7) = 70\) by employing a backtracking algorithm that ran for about a week on a network of 30 machines for undergraduate mathematics students at the University of Waterloo. The blocks of a \((2, 7)-D\Delta S\) of scope 70 are given below:

\[
X_1 = \{0, 1, 4, 21, 40, 54, 67, 69\}
\]

and

\[
X_2 = \{0, 6, 11, 18, 28, 37, 62, 70\}.
\]

We did not attempt to find all \((2, 7)-D\Delta S\) of scope 70.
The induction hypothesis implies that
\[ D' = \{ r_{i2} - n | 1 \leq i \leq j \} \cup \{ r_{i2} - n | 1 \leq i \leq j \}. \]
and hence \( r_{j+1,2} - (j + 1) = u_{j+1}. \) This completes the proof. \( \square \)

Corollary 2: The scope of the \((n, 2)\)-D\(\Delta\)S constructed by the transversal-greedy algorithm is \(\lceil 5 + \sqrt{5} \rceil/2 \) \(n).\)

Proof: Follows from Connell’s result [21] that
\[ u_i = \lfloor (1 + \sqrt{5})i/2 \rfloor. \]

It follows that the \((n, 2)\)-D\(\Delta\)S constructed by the transversal-greedy algorithm is only about a factor of 1.21 worse than the optimal. Analysis of the scope of \((n, k)\)-D\(\Delta\)S constructed by the transversal-greedy algorithm, for any \(k \geq 3\), seems difficult.

V. RANDOMIZED HEURISTICS

We describe in this section some randomized heuristics that have been very effective in constructing difference triangle sets of small scope. These heuristics fit into a general framework. An \((n, k)\)-template is a subset of \(\{1, 2, \ldots, n\} \times \{0, 1, \ldots, k\}.\) There is a natural correspondence between a set of cells of an \(n \times (k + 1)\) array and an \((n, k)\)-template.

Randomized Heuristic

Step 1: Let \(R\) be an array representation of any \((n, k)\)-D\(\Delta\)S.
Step 2: Let \(\mathcal{T}\) be a set of \((n, k)\)-templates.
Step 3: Repeat Step 4 to Step 6 \(N\) times:
Step 4: Let \(s\) be the scope of the \((n, k)\)-D\(\Delta\)S represented by \(R\).
Step 5: Randomly choose \((n, k)\)-template in \(\mathcal{T}\) and delete the entries in the cells of \(R\) corresponding to that template.
Step 6: Find all possible ways of filling in the empty cells of \(R\) using nonnegative integers no greater than \(s\). Randomly choose one of these ways and fill in the empty cells of \(R\) accordingly.

The final difference triangle set constructed by the randomized heuristic have scope at most that of the initial difference triangle set, and strictly improves on the scope if at any stage of the algorithm, the cell containing the largest element of the array is emptied and this element is never used to refill any cell.

The sets of templates \(\mathcal{T}\) that we find most effective in constructing difference triangle sets of small scope are the three listed below.

1) \(\mathcal{T}_1 = \{(i, j) | 1 \leq i \leq n, 0 \leq j \leq k\};\)
2) \(\mathcal{T}_2 = \{(i, j) | 0 \leq j \leq k | 1 \leq i \leq n\};\)
3) \(\mathcal{T}_3 = \{(i, j), i | 1 \leq i \leq n | 0 \leq j \leq k\}.\)

The templates \(\mathcal{T}_1, \mathcal{T}_2, \) and \(\mathcal{T}_3\) correspond to emptying single cells, emptying the cells in an entire row, and emptying one cell from each row in Step 5 of the randomized heuristic, respectively. Let us denote by \(\mathcal{H}_i\) the randomized heuristic that uses \(\mathcal{T}_i.\) Naturally, \(\mathcal{H}_1\) is the fastest. \(\mathcal{H}_2\) and \(\mathcal{H}_3\) are much slower but generally give better results when \(n\) and \(k\) are small. \(\mathcal{H}_3\) is effective when \(n/k\) is large whereas \(\mathcal{H}_1\) is effective when \(n/k\) is small. These heuristics work well when the initial array-representation of an \((n, k)\)-D\(\Delta\)S used in Step 1 is that constructed by the transversal-greedy algorithm. We used these three heuristics in combination, typically in the order \(\mathcal{H}_1, \mathcal{H}_3, \mathcal{H}_2, \mathcal{H}_1, \mathcal{H}_3, \mathcal{H}_2\) to obtain a number of improvements on the upper bounds for \(m(n, k)\). Instances of these improvements are given in Table I.

### Table I

<table>
<thead>
<tr>
<th>(k)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
<th>(6)</th>
<th>(7)</th>
<th>(8)</th>
<th>(9)</th>
<th>(10)</th>
<th>(11)</th>
<th>(12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(n) of Blocks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(4)</td>
<td>123</td>
<td>133</td>
<td>146</td>
<td>156</td>
<td>140</td>
<td>150</td>
<td>160</td>
<td>161</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5)</td>
<td>110</td>
<td>130</td>
<td>145</td>
<td>170</td>
<td>186</td>
<td>204</td>
<td>222</td>
<td>234</td>
<td>252</td>
<td>275</td>
<td></td>
</tr>
<tr>
<td>(6)</td>
<td>117</td>
<td>146</td>
<td>172</td>
<td>198</td>
<td>225</td>
<td>251</td>
<td>277</td>
<td>314</td>
<td>340</td>
<td>366</td>
<td>393</td>
</tr>
<tr>
<td>(7)</td>
<td>126</td>
<td>164</td>
<td>206</td>
<td>249</td>
<td>327</td>
<td>368</td>
<td>415</td>
<td>458</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(8)</td>
<td>137</td>
<td>182</td>
<td>224</td>
<td>263</td>
<td>360</td>
<td>400</td>
<td>445</td>
<td>493</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(9)</td>
<td>148</td>
<td>196</td>
<td>242</td>
<td>290</td>
<td>387</td>
<td>435</td>
<td>483</td>
<td>535</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>160</td>
<td>212</td>
<td>264</td>
<td>320</td>
<td>420</td>
<td>472</td>
<td>524</td>
<td>580</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>172</td>
<td>226</td>
<td>284</td>
<td>344</td>
<td>451</td>
<td>509</td>
<td>568</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>185</td>
<td>242</td>
<td>304</td>
<td>370</td>
<td>484</td>
<td>552</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TABLE I

IMPROVED UPPER BOUNDS FOR \(m(n, k)\)
where our improved upper bound is given above the best previous upper bound. The bounds in parentheses “( )” are due to Kløve [1], those in brackets “[ ]” are due to Chen, Fan, and Jin [16], and those in braces “{ }” are due to Chen [15]. The blocks for difference triangle sets with the improved scopes are available from the authors.

VI. CONCLUDING REMARKS

One of the problems suggested by the results in Section II is the determination of the asymptotic behavior of \( m(n, k) \). Our results show that for \( f(n) \) satisfying \( \lim \sup_{n \to \infty} f(n)/n < 1 \), we have \( \lim_{n \to \infty} m(n, f(n)/n) f(n)^2 = 1 \). It would be interesting to know what happens if \( f(n) \) is allowed to grow at a faster rate.

We have also described algorithms that are used to construct difference triangle sets with the best known scopes for many intermediate values of \( n \) and \( k \).

REFERENCES


Contribution to Munuera’s Problem on the Main Conjecture of Geometric Hyperelliptic MDS Codes

Hao Chen and Stephen S.-T. Yau, Senior Member, IEEE

Abstract—In coding theory, it is of great interest to know the maximal length of MDS codes. In fact, the Main Conjecture says that the length of MDS codes over \( F_3 \) is less than or equal to \( q + 1 \) except for some special cases, Munuera proposed a new way to attack the Main Conjecture on MDS codes for geometric codes. In particular, he proved the conjecture for codes arising from curves of genus one or two when the cardinal of the ground field is large enough. He also asked whether a similar theorem can be proved for any hyperelliptic curve. The purpose of this correspondence is to give an affirmative answer. In fact, our method also proves the Main Conjecture for geometric MDS codes for \( q = 2 \) if the genus of the hyperelliptic curve is either 1, 2 or 3, and for \( q = 3 \) if the genus of the curve is 1.

Index Terms—Algebraic curves, algebraic-geometric codes, divisors, hyperelliptic curves, zeta function.

I. INTRODUCTION

Let \( F_q \) be a finite field with \( q \) elements and \( X \) be a nonsingular projective curve defined over \( F_q \) with genus \( g \). We shall write \( X(F_q) \) to indicate the finite set of \( F_q \)-rational points on \( X \). The function field of \( X \) over \( F_q \) is denoted by \( K(X) \). Let \( \mathcal{P} = \{ P_1, \ldots, P_n \} \) be a set of \( n \) distinct rational points on \( X \). By abusing notation, we also sometimes identify \( \mathcal{P} \) as a divisor. Let \( G \) be a rational divisor with support disjoint from \( \mathcal{P} \).

\[
L(G) := \{ f \in F_q(X) : (f) + G \geq 0 \} \cup \{ 0 \} = H^0(X, \mathcal{O}_G)
\]

where \( [G] \), the line bundle corresponding to the divisor \( G \), is a vector space, and we denote \( \ell(G) \) its dimension. The complete linear system associated to \( G \), denoted by \( |G| \), is

\[
\{ f \in F_q(X) : (f) + G \geq 0 \}/F_q^*.
\]

Definition: The algebraic geometry code \( C(X, \mathcal{P}, G) \) associated to the pair \((\mathcal{P}, G)\) is the linear code of length \( n \) defined as the image of the linear map

\[
\alpha : L(G) \rightarrow \mathbb{F}_q^m, \quad f \mapsto (f(P_1), \ldots, f(P_n)).
\]

We shall let \( k \) denote the dimension of this linear code. Then \( k = \ell(G) - \ell(G - \mathcal{P}) \). In what follows, we shall always assume that

\[
2g - 2 < \deg G < n.
\]

It is well known that the dimension \( k \) and the minimum distance \( d \) of the algebraic geometric code \( C(X, \mathcal{P}, G) \) satisfy the following relations [11]:

\[
k = \ell(G) - \deg G + 1 - g \geq n - \deg G.
\]

Manuscript received July 12, 1996; revised February 3, 1997. The work of H. Chen was supported by the NSF of China and by the Guangdong Provincial NSF of China. The work of S. S.-T. Yau was supported in part by ARO DAAH04-1-0530 and NSF DMS 9321262.

H. Chen is with the Department of Mathematics, Zhongshan University, Guangzhou, Guangdong 510275, P.R. China.
S. S.-T. Yau is with the Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, Chicago, IL 60607-7045 USA.

Publisher Item Identifier S 0018-9448(97)03868-6.