Assignment 4: Compute Roos Bound

Ziquan Yang

March 22, 2014

1 Another formulation of Roos Bound

In the original paper by Roos, the Roos Bound is formulated as follows:

Theorem 1.1. Let N and M denote nonempty sets of nth roots of unity in K. If there exists a consecutive set \overline{M} containing M with $|\overline{M}| \leq |M| + d_N - 2$, then $d_{MN} \geq |M| + d_N - 1$.

However, it is not very easy to use this formulation to calculate Roos Bound. Another formulation of Roos Bound is suggested in "Algebraic Codes for Data Transmission":

Theorem 1.2. Let n be a factor of $q^m - 1$ for some m. Let GCD(n, b) = 1. The only vector in $GF(q)^n$ of weight d - 1 or less whose spectral components V_j equal zero for $j = l_1 + l_2 b$ mod n, where $l_1 = 0, \dots, d - s - 2$ and l_2 takes at least s + 1 values in the range $0, \dots, d - 2$, is the all zero vector.

To understand why this is implied by the Roos Bound, we need first to interchange the roles of l_1 and l_2 . Let $V'_j = V_{Bj}$, where $Bb = 1 \mod n$. Then we see in V'_j we can find $j' = Bl_1 + l_2 \mod n$, where l_1 and l_2 still take values as above. Now let $N = \{\alpha^{Bl_1}\}$, $M = \{\alpha^{l_2}\}$ and $\overline{M} = \{\alpha^0, \cdots, \alpha^{d-2}\}$. Using the following corollary of BCH Bound, we see that $d_N \geq d - s$:

Corollary 1.3. Let n be a factor of $q^m - 1$ for some m. Let GCD(n, b) = 1. The only vector in $GF(q)^n$ of weight d-1 or less that has d-1 bth-consecutive components of its spectrum equal to zero is the all-zero vector.

Thus we have $|M| + d_N - 2 \ge (s+1) + (d-s) - 2 = d-1 = |\overline{M}|$, so we can apply Roos Bound to V'_j . However, although theorem 1.2 suggests that l_1 starts from 0, it is rather unnecessory, since the corollary does not require where the consecutive components should start.

2 Computation

Here we only compute the Roos Bound for codes in $GF(2)^{63}$. We first include all the α^k , where k is a multiple of 3 in the defining set of the cyclic codes. Then we include two new cyclotomic cosets in our defining set. We experiment through all the 2-combinations of other cyclotomic cosets, and caculate the bound for each cyclic code generated.

Indices of cosets

- $2 \{1, 2, 4, 8, 16, 32\}$
- 4 {5, 10, 20, 40, 17, 34}
- $5 \{7, 14, 28, 56, 49, 35\}$
- $7 \{11, 22, 44, 25, 50, 37\}$
- $\{13, 26, 52, 41, 19, 38\}$
- $11 \{23, 46, 29, 58, 53, 43\}$
- 13 $\{31, 62, 61, 59, 55, 57\}$

2.1 A brief explanation of algorithm

The main idea of the algorithm is loop through all possible blocklengths from 1 to the length of the longest consecutive subset of the defining set. And for each blocklength, we loop through all possible bs, as described in theorem 1.2.

- 1. For a given blocklength, identify all indices that could be a start of a consecutive subset of the given blocklength. Let it be I.
- 2. For a given b, send each element $i \in I$ to Bi, where B is the inverse of b in the group $(\mathbb{Z}/63\mathbb{Z})^{\times}$. Now consecutive bth indices collapse to consecutive indices.
- 3. Sort the resulting set (as if it is a subset of \mathbb{Z}) and call it v.
- 4. Note for each b we allow at most b-1 missing values. To compute the longest subset with less than or equal to b-1 missing values, we create a matrix A associated with each v, where

$$a_{ij} = \begin{cases} (v_i - v_j)_{63}, & \text{if } (v_i - v_j)_{63} \le (i - j)_{|v|} + (b - 1) \\ 0, & \text{otherwise} \end{cases}$$

5. Search for the largest element in A, and find the starting point and ending point in the original I with given b.

The tables in the result section read as follows: each column means, under the given block-length, (b, s+1, d, starting index, ending index).

3 Results

Indices are 2 4 generalized BCH

blocklength: 2

blocklength: 3

blocklength: 4

blocklength: 5

blocklength: 6

Indices are 2 5 generalized BCH

```
13 16 17 19 20
                                                                                                                                                                                                                                                                                                                                       22
                                                                                                                                                                                                                                                                                                                                                                 23

    5
    5
    5
    4
    5
    4
    4
    4
    5
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    4
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5
    5</t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      5
                                                                                                                                                                                                                                                                                                                                                                                                                                                  6
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      2
                                                                                                                                   24
                                                                                                                                                                                        27
                                                                                                                                                                                                                    1
                                                                                                                                                                                                                                                    3
                                                                                                                                                                                                                                                                        54
                                                                                                                                                                                                                                                                                                       48
                                                                                                                                                                                                                                                                                                                                30
                                                                                                                                                                                                                                                                                                                                                                 39
                                                                                                                                                                                                                                                                                                                                                                                          57
```

blocklength: 2

```
10 11 13 16 17 19
                        22
                                          31 \
       3
           3
             2
                 2
                     2
                         2
                                   2
                                       3
                                          3
       5
          5 4
                  4
                        4
                                4
                                   4
   3
                 8
                     7
                               7
       1
          32 15
                        56
                           48
                                   1
                                       6
                                          1
              32
3
       27
           1
                 27
                     27
                        15
   14
```

blocklength: 3

blocklength: 4

```
11 13 16 17 19
                  20
                      22
                          23
                              25
                                  26
                                         31
                           2
        1
           1
                                  1
                       1
                                          6
    5
        5
            5
               6
                   5
                           6
                                  5
                                      6
                       5
                              5
    0
        0
           0
               6
                   0
                       0
                          0
                              0
                                  0
                                      6
                                         1
        0
           0
               0
                                  0
```

```
1 2 4 5 8 10 11 13 16 17 19
                                       23
                                                     31 \
                                 20
                                    22
                          1
                              1
                                                     1
                   6
                       6
                          6
                              6
                                 6
                                     6
                                       6
                                              6
                                                  6
                                                     6
                   0
                       0
                          0
                              0
                                 0
                                     0
                                              0
                                                  0
                                                     0
                0
                       0
                          0
                              0
                                                     0
                    0
                                 0
```

Indices are 2 7 generalized BCH

```
13 16 17 19 20
                                                                                22
                                                                                     23

    5
    5
    5
    5
    5

    6
    6
    6
    6
    6
    6

    0
    0
    0
    22
    0
    44

                                                     5 5
                                                                          5
                                                                                                                   5
                                               6 6
                                                         6
                                                                                                             6
                                                                                            0 \quad 22 \quad 42 \quad 2
                                      0 11 0 37 50 25
                                                                               0 - 42
                               21
                                             0 \quad 1 \quad 42 \quad 0
                                                                         42 	 25
                                                                                              37
```

blocklength: 2

blocklength: 3

blocklength: 4

```
1 2 4 5 8 10 11 13 16 17 19
                                  22
                                     23 \ 25
                                                  31 \
                               20
                        1
                                                  1
                     6 6
                            6
                               6
                                   6
                                     6
                                            6
                                               6
                                                   6
                      0
                        0
                            0
                               0
                                   0
                                           0
                                                0
                                                   0
                0
                      0
                            0
                                                   0
                   0
                               0
```

Indices are 2 8 generalized BCH

blocklength: 2

```
5 8 10 11 13 16 17 19
                              20
                                 22
                      2
                         2
                           2
                               2
                                 2
                                    3
                                       3
                                          3
                                             2
                                                3
                   3
5
                           4
                                 4
                                    5
                                          5
                     4 4
                              4
                                       5
                                             4
                     2 15
                           32 	 51
                  38
                                 41 18
                                       1
                                         12
                                             3
                                                1
            51
               12
                     18 32
                           51
                                    1
                                       51
```

blocklength: 3

blocklength: 4

```
1 2 4 5 8 10 11 13 16 17 19
                                  22
                                    23
                                                  31 \
                               20
                        1
                                                  1
                     6
                       6
                            6
                               6
                                  6
                                     6
                                        6
                                           6
                                               6
                                                  6
                      0
                        0
                            0
                              0
                                  0
                                           0
                                               0
                                                  0
               0
                      0
                         0
                            0
                                                  0
                   0
                               0
```

Indices are 2 11 generalized BCH

```
13 16 17 19 20
                                                                                                     22
                                                                                                            23

    5
    5
    5
    5
    5
    5
    5
    5
    5
    5

    6
    6
    6
    6
    6
    6
    6
    6
    6
    6

    0
    0
    0
    43
    0
    23
    42
    32
    0
    58
    8

                                                                                             5
                                                                                                      5
                                                                                                                                                 5
                                                                                             6
                                                                                                                                                 2
                                                                                           46 21
                                                                                                            0 - 21
                                                                                                                              1
                                                                                                                                       0
                                                         21
                                                                 1
                                                                        0 21
                                                                                           0
                                                                                                    46
                                                                                                           29
                                                                                                                    58
```

blocklength: 2

blocklength: 3

blocklength: 4

Indices are 2 13

blocklength: 5

blocklength: 6

,	/ 1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	31 \
1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	2
١	10	9	9	9	9	9	9	9	10	9	9	9	9	9	10	9	9	10
	59	60	60	60	59	60	59	60	59	59	59	60	59	59	60	60	60	60
١	60	60	60	60	59	60	59	60	60	59	59	60	59	59	59	60	60	59 /

Indices are 4 5 generalized BCH

/	′ 1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	31 \
1	4	4	4	5	4	5	4	4	4	5	4	5	4	5	4	4	5	4
١	5	5	5	6	5	6	5	5	5	6	5	6	5	6	5	5	6	5
١	33	3	6	0	12	0	6	57	24	0	30	0	12	34	48	51	10	18
1	36	9	18	20	36	40	39	33	9	5	24	17	15	0	60	3	0	48 /

blocklength: 3

```
5
                    10
                        11
                             13
                                16
                                    17
                                         19
                                              20
                                                  22
                                                      23
                                                          25
                                                               26
                                                                   29
                                                                       31
        4
                8
                                                  1
                                                           1
    1
        1
            1
                1
                     1
                         1
                             1
                                 1
                                      1
                                          1
                                              1
                                                       1
                                                               1
                                                                   1
                                                                       1
5
    5
        5
            5
                5
                     5
                         5
                             5
                                 5
                                      5
                                          5
                                              5
                                                  5
                                                       5
                                                           5
                                                               5
                                                                   5
                                                                       5
   33
       33
            33
                33
                    33
                        33
                             33
                                 33
                                     33
                                              33
                                                  33
                                                      33
                                                          33
                                                              33
                                                                   33
                                                                       33
                                         33
   33
       33
            33
                33
                    33
                         33
                             33
                                 33
                                     33
                                         33
                                              33
                                                  33
                                                      33
                                                          33
                                                               33
                                                                   33
                                                                       33
```

Indices are 4 7 generalized BCH

blocklength: 2

blocklength: 3

```
11
                      16
                          17 19
                                   20
                                       22
                                           23
                                              25
                                                   26
                                                          31
2 4 5 8
           10
                  13
                        1
                           1
                                   1
                                           1
                                               1
                                                   1
                                                           1
                                       1
                    5
                        5
                            5
                                5
                                   5
                                                   5
                                                       5
                                                           5
                                       5
                                           5
                                               5
               9
                    9
                        9
                           9
                                9
                                   9
                                       9
                                           9
                                               9
                                                   9
                                                       9
                                                           9
                            9
                                9
                                           9
```

Indices are 4 8 generalized BCH

blocklength: 2

blocklength: 3

blocklength: 4

Indices are 4 11 generalized BCH

/ 1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	31 \
																	2
3	3	3	10	3	10	5	5	3	10	5	10	5	10	5	5	10	3
5	10	20	43	40	23	12	60	17	58	15	46	24	34	33	57	10	29
6	12	24	20	48	40	45	36	33	5	9	17	27	29	45	9	53	60 /

/ 1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	31 \
1	1	2	1	2	2	2	2	2	1	2	2	2	2	2	2	2	1
3	3	4	3	4	4	4	4	4	3	4	4	4	4	4	4	4	3
5	20	5	5	9	29	9	29	17	17	20	33	17	45	20	42	57	29
5	20	9	5	17	39	20	42	33	17	39	53	39	5	45	5	23	29 /

Indices are 4 13 generalized BCH

blocklength: 2

blocklength: 3

blocklength: 4

Indices are 5 7 generalized BCH

/	1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	$31 \setminus$
	4	4	4	4	4	4	5	5	4	4	5	4	5	4	5	5	4	4
	5	5	5	5	5	5	6	6	5	5	6	5	6	5	6	6	5	5
	48	33	3	39	6	15	0	11	12	57	50	30	0	54	0	22	27	57
	51	39	15	54	30	45	44	0	60	45	0	27	25	60	37	0	51	24

blocklength: 3

Indices are 5 8 generalized BCH

1	1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	31 \	١
1	4	4	4	4	4	4	5	5	4	4	5	4	5	4	5	5	4	4	١
1	5	5	5	5	5	5	6	6	5	5	6	5	6	5	6	6	5	5	l
1	12	24	48	9	33	18	19	0	3	18	0	36	38	3	26	0	12	39	١
1	15	30	60	24	57	48	0	52	51	6	13	33	0	9	0	41	36	6 /	/

blocklength: 3

Indices are 5 11 generalized BCH

1	1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	31 \
1	4	4	4	5	4	5	4	4	4	5	4	5	4	5	4	4	5	4
1	5	5	5	6	5	6	5	5	5	6	5	6	5	6	5	5	6	5
1	27	54	45	43	27	23	24	30	54	58	39	46	48	0	3	60	0	15
1	30	60	57	0	51	0	57	6	39	0	33	0	51	29	15	12	53	45 /

blocklength: 2

blocklength: 3

Indices are 5 13 generalized BCH

blocklength: 3

blocklength: 4

Indices are 7 8 generalized BCH

1	1	2	4	5	8	10	11	13	16	17	19	20	22	23	25	26	29	$31 \setminus$
1	4	4	4	2	4	2	9	9	4	2	9	2	9	2	9	9	2	4
١	5	5	5	3	5	3	10	10	5	3	10	3	10	3	10	10	3	5
	24	48	33	25	3	50	19	11	6	22	50	37	38	52	26	22	19	51
/	27	54	45	30	27	60	44	52	54	39	13	57	25	12	37	41	48	18 /

blocklength: 3

Indices are 7 11 generalized BCH

blocklength: 2

blocklength: 3

blocklength: 4

Indices are 7 13 generalized BCH

blocklength: 3

blocklength: 4

Indices are 8 11 generalized BCH

blocklength: 2

blocklength: 3

Indices are 8 13 generalized BCH

blocklength: 2

blocklength: 3

blocklength: 4

Indices are 11 13 generalized BCH

4 Matlab Code

Compute.m

```
clear;
M = gfcosets(6);
R3 = [M(1, :) M(3, :), M(6, :), M(9, :), M(10, :), M(12, :)];
R3 = R3(\tilde{s} \operatorname{isnan}(R3));
ind = [2, 4, 5, 7, 8, 11, 13];
counter = 0;
FID = fopen('table1.tex', 'w');
for i = 1: length(ind);
    for j = (i+1) : 1: length(ind);
         temp = [R3, M(ind(i), :), M(ind(j), :)];
         temp = temp(~isnan(temp));
         temp = sort(temp);
         fprintf(FID, '\\pagebreak Indices are %d %d \\\', ind(i), ind(j));
         [bdata mdata sdata edata] = computeData(temp, 0);
         fprintf(FID, 'generalized BCH');
         fprintf(FID, '\\begin{center} $ %s $\\end{center}', latex(sym([bdata;
           mdata; mdata+1; sdata; edata])));
         for (len = 1 : 1 : mdata(1) - 1)
               subtemp = [];
               for (k = 0: 1: 32)
                    if (\text{mod}(\text{temp}(\text{mod}(k + \text{len}, 33)+1) - \text{temp}(k+1), 63) = \text{len})
                        subtemp = [subtemp temp(k+1)];
                    end;
               end;
               [bdata mdata sdata edata] = computeData(subtemp, len - 1);
               fprintf(FID, 'blocklength: %d', len+1);
               fprintf(FID, '\\begin{center} $ %s $\\end{center}',
                 latex(sym([bdata; mdata; mdata+len+1; sdata; edata])));
         end;
    end;
end;
```

computeData.m

```
function [bdata mdata sdata edata] = computeData(w, miss)
bdata = [];
Bdata = [];
for i = 1 : 1 : 31
    [g, B, un] = gcd(i, 63);
    if (g == 1)
        bdata = [bdata, i];
        Bdata = [Bdata, mod(B, 63)];
    end;
end;
mdata = [];
sdata = [];
edata = [];
A = [[]];
for k = 1 : 1: length(bdata);
    b = Bdata(k);
    B = bdata(k);
    v = mod(w*b, 63);
    v = sort(v);
    len = length(v);
    for i = 1 : 1 : len;
         for j = 1 : 1 : len;
             m = mod(v(i) - v(j), 63);
              d = mod(i-j, len);
              A(i,j) = (d+1)*(m \le (d + miss));
         end;
    end
    myMax = max(A(:));
    [xPos yPos] = find(A \longrightarrow myMax, 1);
    result = mod([v(yPos) \ v(xPos)]*B, 63);
    mdata = [mdata, myMax];
    sdata = [sdata, result(1)];
    edata = [edata, result(2)];
end;
end
```

5 Observations

Theorem 5.1. If a cyclic code C in $GF(2)^{2^m-1}$, $m \geq 2$ has defining set that contains all powers of 3 and cyclotomic cosets of α^s and α^{-s} , where $gcd(s, 2^m - 1) = 1$, then the minimum distance of C is at least 10.

Proof. First observe that α^s and α^{-s} cannot belong to the same cyclotomic coset. Suppose otherwise, then $\alpha^{-s}=\alpha^{2^{\lambda_s}}$ for some $\lambda \leq m$. This implies $2^m-1|(2^{\lambda}+1)s$, however since $\gcd(s,2^m-1)=1,2^m-1|(2^{\lambda}+1)$, which is impossible. Then the set $\alpha^{-4s},\alpha^{-3s},\alpha^{-2s},\alpha^{-s},$ $\alpha^0,\alpha^s,\alpha^{2s},\alpha^{3s},\alpha^{4s}$ will always be in the defining set. Apply generalized BCH Bound and we see that $d\geq 10$.

Theorem 5.2. Two cyclic codes C_1 and C_2 with defining set B_1 and B_2 , such that $\alpha^s \in B_1 \Leftrightarrow \alpha^{-s} \in B_2$, have the same minimum distance.

Proof. There is a natural bijection between C_1 and C_2 that preserves weight of a vector. \square