IERG6120 Coding for Distributed Storage Systems Lecture 8 - 06/10/2016

The multiplicative structure of finite field and a construction of LRC

Lecturer: Kenneth Shum *Scribe: Zhouyi Hu*

Notations: We use the notation $GF(q)$ for a finite field of size q, and $GF(q)^*$ for the set of non-zero elements in $GF(q)$. We write $a|b$ as a short-hand notation for a divides b.

1 The order of an element in a group

Consider a finite commutative group $(G, \cdot)$.

Definition For $a \in G$, we define the *order* of a, as

$$ord(a) := \min\{i \geqslant 1 : a^i = e\}$$

where e denotes the identity element of G. The order of an element in a finite commutative group is well-defined, because $a^{|G|} = e$ for each $a \in G$. ($|G|$ is the cardinality of G.) It is guaranteed that some power of a is equal to the identity element. The order corresponds to the smallest one.

Example $GF(9)^*$ is the multiplicative group of $GF(9)$. It can be generated by irreducible polynomial $f(x) = x^2 + 2x + 2$. We have $x^2 = x + 1$ in the finite field so defined. Let $ord(a)$ be the order of a nonzero element a in the multiplicative group $GF(9)^*$.

$ord(x) = 8$

$ord(1 + x) = 4$

$ord(2) = 2$

2 Existence of primitive element

Theorem In the multiplicative subgroup $GF(q)^*$ of a finite field $GF(q)$, there exists an element a whose (multiplicative) order is equal to $q - 1$, i.e., $a^{q-1} = 1$ but $a^i \neq 1$ for $i = 1, 2, \ldots, q - 2$.

Definition An element of order $q - 1$ is called a *primitive element* of $GF(q)$.

To prove the existence of primitive element, we define *Euler's totient function*, $\phi(n)$, as the number of integers between 1 and n that are relatively prime with n.

Definition $\phi(n) \triangleq |\{i : 1 \leqslant i \leqslant n, gcd(i, n) = 1\}|$

Example

$\phi(1) = |\{1\}| = 1$

$\phi(2) = |\{1\}| = 1$

$\phi(3) = |\{1, 2\}| = 2$

$\phi(p) = |\{1, 2, \ldots, p - 1\}| = p - 1$, for prime number p.

$\phi(12) = |\{1, 5, 7, 11\}| = 4$

If the prime factorization of n is $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$, we have the formula

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m}).$$

Theorem For positive integer n, $\sum_{d|n} \phi(d) = n$. (The summation is extended over all divisors d of n.)

The proof is basically a counting argument. We illustrate this by the following example.

Example Consider $n = 12$. We classify the numbers between 1 and 12 according to their greatest common divisor with 12. For $i = 1, 2, \ldots, 12$, if $gcd(i, 12) = 1$, we put i in the first row of the following table. If $gcd(i, 12) = 2$, we put i in the second row. If $gcd(i, 12) = 3$, we put it in the third row, etc.

		1	2	3	4	5	6	7	8	9	10	11	12
$d = 1$	$\phi(12) = 4$	①				⑤		⑦				⑪	
$d = 2$	$\phi(6) = 2$		②								⑩		
$d = 3$	$\phi(4) = 2$			③						⑨			
$d = 4$	$\phi(3) = 2$				④				⑧				
$d = 6$	$\phi(2) = 1$						⑥						
$d = 12$	$\phi(1) = 1$												⑫

Each row of the table is associated to a divisor d of n. We can count $\phi(n/d)$ integers in the row corresponding to divisor d. As each number between 1 and 12 appears exactly in one row, it follows that

$$\begin{aligned} 12 &= \phi(12/1) + \phi(12/2) + \phi(12/3) + \phi(12/4) + \phi(12/6) + \phi(12/12) \\ &= \phi(12) + \phi(6) + \phi(4) + \phi(3) + \phi(2) + \phi(1). \end{aligned}$$

Thus, we have $12 = \sum_{d|12} \phi(d) = 4 + 2 + 2 + 2 + 1 + 1$.

Lemma Let $(G, \cdot)$ be a group written multiplicatively. If a is an element in G with order n, i.e., $a^n = e$ but $a \neq e$ for $k = 1, 2, \ldots, n-1$, then for $k = 1, 2, \ldots, n-1$, we have

$$ord(a^k) = \frac{n}{gcd(k, n)}.$$

Proof We let m denote the number $\frac{n}{gcd(k,n)}$. We want to show that m is the smallest integer such that $(a^k)^m$ is equal to the identity element e in group G. Firstly, we check that $(a^k)^m$ is indeed equal to the identity element e:

$$\begin{aligned} (a^k)^m &= a^{n\frac{k}{gcd(k,n)}} \\ &= e^{\frac{k}{gcd(k,n)}} \\ &= e. \end{aligned}$$

Next, we show by contradiction that $(a^k)^j$ is not equal to e for $1 \leqslant j < m$.

Suppose that $(a^k)^j = r$ for some integer j strictly less than m. Since n is the order of a, we must have $n|kj$. Divides both n and kj by $gcd(k, n)$, we get

$$\frac{n}{gcd(k,n)} \Big| \frac{k}{gcd(k,n)} j$$

or

$$m \Big| \frac{k}{gcd(k,n)} j$$

by the definition of m.

But m and $\frac{k}{gcd(k,n)}$ are relatively prime. Hence m must be a divisor of j. This contradicts the assumption that j is strictly less than m. □

We now prove the theorem at the beginning of this section. Indeed, we will establish a stronger result.

Theorem In the multiplicative group $GF(q)^*$, there are $\phi(d)$ elements with order d, for $d|(q-1)$. In particular, there are $\phi(q-1)$ primitive elements in $GF(q)$.

Proof Let $\theta(d)$ denote the number of elements in $GF(q)^*$ with multiplicative order d. We want to show that $\theta(d) = \phi(d)$ for all divisors d of $q-1$. For each divisor d of $q-1$, we distinguish two cases: either there is no nonzero element with order d, or there exists at least one nonzero element with order d. In the first case, we have $\theta(d) = 0$.

Consider the second case. Let a be an element in $GF(q)^*$ with order d. We note that an element of order d must be a root of polynomial $x^d - 1$. Indeed, if $ord(b) = d$, then $b^d = 1$ and hence $b^d - 1 = 0$. The following powers of a,

$$a,\ a^2,\ a^3,\ \ldots, a^d \tag{1}$$

are distinct roots of polynomial $x^d - 1$. (We can check that for $i = 1, 2, \ldots, d$, $(a^i)^d = (a^d)^i = 1^i = 1$.) We have thus found all the roots of $x^d - 1$ in $GF(q)$, because the number of roots of a polynomial is no more than the degree of the polynomial (at this point we are using the property of polynomials over a field). An element of order d must be in the list in (1). However, not all elements in (1) have order d. By the lemma in p.2, a^i has order d precisely when $gcd(i, d) = 1$, for $i = 1, 2, \ldots, d$. Hence, there are exactly $\phi(d)$ powers of a which have order d. It follows that $\theta(d) = \phi(d)$ in the second case.

In either case, we have $\theta(d) \leqslant \phi(d)$.

On the other hand, we have

$$\sum_{d|q-1} \theta(d) = q - 1.$$

This equality follows by a counting argument. Since α^{q-1} for all non-zero α in $GF(q)$, any nonzero element in $GF(q)$ should have some order, and the order must be a divisor of $q-1$. If we group the $q-1$ nonzero elements in $GF(q)$ according to their orders, then each of them must be counted exactly once in $\theta(d)$, with d ranging over all divisors of $q-1$.

We get

$$0 = \sum_{d|q-1} \theta(d) - \sum_{d|q-1} \phi(d) = \sum_{d|q-1} [\theta(d) - \phi(d)].$$

The difference in the square bracket is less than or equal to zero. We thus have a bunch of non-positive numbers which sum to zero. This is possible only if each of the non-positive numbers is zero. Therefore, we get $\theta(d) = \phi(d)$ for all $d|(q-1)$. □

3 Tamo-Barg construction of LRC

Using the multiplicative structure of finite field, we have the following simplified version of Tamo-Barg construction of locally repairable code (LRC) [1]. Suppose that we want to construct an LRC with locality r, meaning that any code symbol is a function of r other code symbols. The value of r is a system parameter and is usually less than the dimension of the code. In the followings we give a construction of LRC whose length n is a multiple of $r+1$. We choose the size of a finite field $q > n$ such that $q-1$ is a multiple of $r+1$. In $GF(q)$, we can find precisely $r+1$ elements whose $(r+1)$-st power is equal to 1. For example, we can pick a primitive element, say β, of $GF(q)$, and let $\alpha = \beta^{(q-1)/(r+1)}$. Then

$$A_1 := \{1, \alpha, \alpha^2, \ldots, \alpha^r\}$$

is a multiplicative subgroup of $GF(q)^*$.

A coset of A_1 is a subset of elements in the form

$$\gamma A_1 := \{\gamma z :\ z \in A_1\}$$

where γ is a nonzero element in $GF(q)$. The cosets partition $GF(q)^*$, and each coset contains $r+1$ elements. We use the key property that the function $g(x) = x^{r+1}$ is constant on each of these cosets. In fact, if $\omega \in \gamma A_1$, then $\omega = \gamma\alpha^i$ for some integer i, and $g(\omega) = (\gamma\alpha^i)^{r+1} = \gamma^{r+1}(\alpha^i)^{r+1} = \gamma^{r+1}$ depends on γ only.

Let m be $n/(r+1)$, which is an integer by our assumption on n. Suppose that A_2, $A_3, \ldots, A_m$ are $m-1$ other cosets of A_1. Let P be the union of A_1, $A_2, \ldots, A_m$. The set P contains n distinct elements in $GF(q)$.

Let $D(k, r)$ be the set of the k smallest non-negative integers whose residue is not equal to r mod $r+1$. For example if $r = 2$ and $k = 4$, then $D(4, 2) = \{0, 1, 3, 4\}$.

Construction. With the above notations, define a linear code over $GF(q)$ whose codewords are obtained by evaluating polynomials of the form:

$$\sum_{i \in D(k,r)} c_i x^i$$

on the elements in P. The above polynomial is called the message polynomial. The coefficients c_i's are elements in $GF(q)$, and are the message symbols to be encoded.

The integers in $D(k, r)$ are the exponents of the message polynomial. There is no polynomial with degree one less than a multiple of $r + 1$. The code can be considered as a subcode of RS code. We note that if $r = k$, then the above construction gives an RS code.

Theorem The code obtained by the above construction has locality r, dimension k, and minimum distance $n - \max D(k, r)$.

We illustrate the construction by the following example.

Example: We have an LRC with $r = 2$, $r + 1 = 3$, and let $GF(13)$ be the alphabet. Then, we can check that 2 is a primitive element in $GF(13)$.

i	1	2	3	4	5	6	7	8	9	10	11	12
2^i	2	4	8	3	6	12	11	9	5	10	7	1

Furthermore, the field elements $2^4 = 3$, $2^8 = 9$ and $2^{12} = 1$ are elements whose 3^{rd} power is equal to 1. Hence, Let A_1 be the set $\{3, 9, 1\}$, A_2 be the coset $2 \cdot A_1 = \{6, 5, 2\}$ and A_3 be the coset $2^2 \cdot A_1 = \{12, 10, 4\}$. We check that $g(x) = x^3$ is constant on each of these cosets.

If we want a code with dimension 4, we note that $D(4, 2) = \{0, 1, 3, 4\}$, and the message polynomial has the form

$$a_0 + a_1 x + a_3 x^3 + a_4 x^4,$$

where a_0, a_1, a_3 and a_4 are message symbols in $GF(13)$. The codewords are obtained by evaluating a message polynomial on the points in $A_1 \bigcup A_2 \bigcup A_3$. Note that we skip the degree 2 in the message polynomial.

A generator matrix can be computed as below:

A_1			A_2			A_3			
3	9	1	6	5	2	12	10	4	
1	1	1	1	1	1	1	1	1	x^0
3	9	1	6	5	2	12	10	4	x^1
1	1	1	8	8	8	12	12	12	$x^3 = g(x)$
3	9	1	9	1	3	1	3	9	$x^4 = x^1 g(x)$

In the first row we list the elements in A_0, A_1 and A_2. In the next four rows we tabulate the zeroth, first, third and fourth powers of the elements.

Thus, we have

$$G = \left[\begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 3 & 9 & 1 & 6 & 5 & 2 & 12 & 10 & 4 \\ \hline 1 & 1 & 1 & 8 & 8 & 8 & 12 & 12 & 12 \\ 3 & 9 & 1 & 9 & 1 & 3 & 1 & 3 & 9 \end{array}\right]$$

The generator matrix can be divided into six blocks. The block on the bottom left is equal to the block in the upper left. The first three columns form a submatrix of row-rank 2. Since row-rank is equal to column-rank, the column-rank of this submatrix is also equal to 2. This implies that the first three columns are linearly dependent. In this example, it is obvious that the first and second columns of G are identical. The first three code symbols form a local group. Any symbol in this group can be uniquely determined by the other two.

The two blocks in the middle are scalar multiple of each other. The submatrix formed by the middle three columns has rank 2. The middle three columns are linearly dependent, and the three code symbols in the middle form a local group. Likewise, we can see that last three symbols form another local group.

By reducing the generator matrix to row-echelon form, we can write down a parity-check matrix as follows,

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 11 & 9 & 0 & 10 & 8 \\ 0 & 1 & 0 & 0 & 12 & 8 & 0 & 2 & 3 \\ 0 & 0 & 1 & 0 & 2 & 5 & 0 & 4 & 1 \\ 0 & 0 & 0 & 1 & 3 & 9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 9 \end{bmatrix}.$$

The last row is a parity-check equation for the last three code symbols. The second last row is a parity-check equation for the middle three code symbols. We can check that the vector [1 3 9 0 0 0 0 0 0] is also in the dual code. Hence, every code symbol has locality 2.

Another choice of the parity-check matrix is

$$P = \begin{bmatrix} 1 & 3 & 9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 9 \\ 1 & 0 & 0 & 0 & 11 & 9 & 0 & 10 & 8 \\ 0 & 1 & 0 & 0 & 12 & 8 & 0 & 2 & 3 \end{bmatrix}.$$

Since the message polynomial has degree less then or equal to 4, the minimum distance is larger than or equal to $9 - 4 = 5$. This is indeed the minimum distance, because this achieves the bound of LRC by Gopalan *et al.* [2]

$$d \leqslant n - k - \left\lceil \frac{k}{r} \right\rceil + 2.$$

We shall prove the bound by Gopalan *et al.* in lecture 9.

Exercises:

1. Find all primitive elements in $GF(17)$.
2. Construct a linear locally repairable code over $GF(17)$ with locality 3, length 15, and dimension 10. Write down either the generator matrix or the parity-check matrix. Illustrate how to recover a single loss of code symbol by accessing 3 other symbols. Determine the minimum distance of the code.
3. Is it true that any LRC obtained by the construction in p.4 achieves the bound by Gopalan *et al.* with equality?

References

[1] I. Tamo and A. Barg, "A family of optimal locally recoverable codes," *IEEE Trans. Information Theory*, vol. 60, no.8, pp.4661–4676, 2014.

[2] P. Gopalan, C. Huang, H. Simitci and S. Yakhanin, "On the locality of codeword symbols," *IEEE Trans. on Information Theory*, vol. 58, no. 11, pp.6925–6934, 2012.