03683072: Error Correcting Codes. November 2017 – Lecture 2

Polynomial Codes and Cyclic Codes

Amnon Ta-Shma and Dean Doron

1 Polynomial Codes

Fix a finite field $\mathbb{F}_q$. For the purpose of constructing polynomial codes, we identify a word of n elements $c = (c_0, \ldots, c_{n-1})$ with its representing polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$.

Definition 1. *Fix some integer n and let $g(x)$ be some fixed polynomial of degree $m \le n-1$. The* polynomial code *generated by $g(x)$ is the code whose codewords are the polynomials of degree less than n that are divisible (without remainder) by $g(x)$.*

As an example, take $\mathbb{F}_2$, $n = 5$ and $g(x) = x^2 + x + 1$. The code consists of the 8 codewords $0 \cdot g(x), \ldots, (x^2 + x + 1) \cdot g(x)$. Equivalently, we can identify every polynomial with its vector of coefficients to get a codeword in $\mathbb{F}_2^n$.

Verify that a polynomial code is linear and has dimension $k = n - m$. Also, check that if $g(x) = \sum_{i=0}^{n-k} g_i x^i$ is the generator polynomial, then an $n \times k$ generating matrix for the code is given by

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & \\ & & \ddots & \ddots & \cdots & \ddots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}^T .$$

1.1 An example: Reed-Solomon code

To show that Reed-Solomon codes are polynomial codes we need to prove that every Reed-Solomon code is generated by some polynomial. Fix a field $\mathbb{F}_q$ with a generator α and $n = q - 1$ and throughout this subsection, let $\mathcal{C}$ be a $[n, k, n-k+1]_q$ Reed-Solomon code.

First, we prove:

Lemma 2. *Let $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ and $c(x)$ be its representing polynomial. Then, $c \in \mathcal{C}$ if and only if $c(\alpha^t) = 0$ for every $1 \le t \le n-k$.*

Proof. Let H be the $n \times (n-k)$ matrix we defined before, $H_{i,j} = \alpha^{ij}$ for $0 \le i \le n-1$ and $1 \le j \le n-k$. We saw that $H^t G = 0$ and therefore H is the parity check matrix of the code. Thus, for $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$, $c \in \mathcal{C}$ iff $Hc = 0$. However, almost be definition, $Hc = 0$ iff $c(\alpha^t) = 0$ for $1 \le t \le n-k$. The claim follows. □

Theorem 3. *The Reed-Solomon code is a polynomial code.*

Proof. Let $g(x) = \prod_{t=1}^{n-k}(x - \alpha^t)$. The above lemma readily implies that $c(x) \in \mathcal{C}$ if and only if $g(x)$ divides $c(x)$. □

2 Cyclic Codes

Definition 4. *A code $\mathcal{C}$ is* cyclic *if every cyclic shift of a codeword in $\mathcal{C}$ is also a codeword. That is, $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.*

In the notation of representing polynomials, a code $\mathcal{C}$ is cyclic if and only if $c(x) \in \mathcal{C}$ implies

$$x \cdot c(x) \bmod (x^n - 1) \in \mathcal{C}.$$

If a code is linear, then equivalently we can say that $c(x) \in \mathcal{C}$ implies

$$u(x) \cdot c(x) \bmod (x^n - 1) \in \mathcal{C}$$

for every $u \in \mathbb{F}_q[x]$. Hence, $\mathcal{C}$ is a linear cyclic code if and only if $\mathcal{C}$ is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$.

2.1 An example: Reed-Solomon code

We begin with an example – the $[n, k, n-k+1]_q$ Reed Solomon code. Define

$$g(x) = \Pi_{t=1}^{n-k}(x - \alpha^t).$$

We saw $c \in \mathcal{C}$ iff $g \mid c$.

Now suppose $c \in \mathcal{C}$. Let $b = xc (\bmod\ x^n - 1)$. Hence $b = xc + D(x)(x^n - 1)$. However,

$$g(x) = \Pi_{t=1}^{n-k}(x - \alpha^t) \mid \Pi_{t=1}^{n}(x - \alpha^t) = x^{q-1} - 1 = x^n - 1.$$

Thus, $g \mid xc$ and $g \mid x^n - 1$ and therefore $g \mid b$. Hence $b \in \mathcal{C}$.

The proof also shows why taking modulo $x^n - 1$ makes sense. This is because for all the evaluation points α we have $\alpha^n - 1 = 0$, thus from the code point of view we can assume $x^n - 1 = 0$.

2.2 Every cyclic Code is a polynomial code

Theorem 5. *Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_q$ and g the monic polynomial in $\mathcal{C}$ of minimal positive degree (prove that it is unique!). Then g generates $\mathcal{C}$, i.e., $c \in \mathcal{C}$ iff $g \mid c$.*

Proof. Suppose there exists $b \in \mathcal{C}$ such that $g \nmid b$, g, b are polynomials of degree at most $n-1$. Now let $c = gcd(g, b)$. As $\mathbb{F}_q[x]$ is an Euclidean ring, there exist $u, v \in \mathbb{F}_q[x]$ such that

$$c = gu + bv,$$

and therefore also

$$c = gu + bv \bmod (x^n - 1).$$

As $\mathcal{C}$ is ideal, $b = b \bmod (x^n - 1) \in \mathcal{C}$. However, since $g \nmid b$, $\deg(c) < deg(g)$. Also $b \neq 0$. But this is a contradiction to g having the minimal positive degree in $\mathcal{C}$. □

2.3 Cyclic codes are special polynomial codes

In fact, we can state something stronger and exactly characterize the generators of cyclic codes.

Theorem 6. *A polynomial code is cyclic if and only if its generator polynomial divides $x^n - 1$.*

Proof. Assume $\mathcal{C}$ is a cyclic $[n,k]$ code over $\mathbb{F}_q$. Let $g(x)$ be the generator polynomial of $\mathcal{C}$. We know g is the minimal degree non-zero monic polynomial in $\mathcal{C}$. Write $x^n - 1 = h(x)g(x) + r(x)$ where $\deg(r) < \deg(g)$. We have that

$$r(x) = -h(x)g(x) \bmod (x^n - 1),$$

so $r(x) \in \mathcal{C}$. This means that $r(x) = 0$, since no other codeword in $\mathcal{C}$ can have degree smaller than $\deg(g)$.

For the other direction, let $\mathcal{C}$ be an $[n,k]$ polynomial code generated by some $g(x)$ and suppose $g \mid x^n - 1$, i.e.,

$$x^n - 1 = gh,$$

for some $h \in \mathbb{F}_q[x]$. Let $c \in \mathcal{C}$. We will prove that $xc \bmod (x^n - 1) \in \mathcal{C}$ and therefore $\mathcal{C}$ is cyclic.

c has degree at most $n-1$. Also $c = gu$ for some $u \in \mathbb{F}_q[x]$. Hence

$$xc \bmod (x^n - 1) = g \cdot (xu \bmod h),$$

and therefore $xc \bmod (x^n - 1) \in \mathcal{C}$ because $\mathcal{C}$ is polynomial. $\square$

Now, we can reprove what we already saw:

Corollary 7. *The Reed-Solomon code is cyclic.*

Proof. The corollary follows from the fact that $x^n - 1 = \prod_{k=1}^{n}(x - \alpha^i)$ and the fact that the generating polynomial is $g(x) = \prod_{i=1}^{n-k}(x - \alpha^i)$. $\square$

2.4 Dual Codes of Cyclic Codes

Let $\mathcal{C}$ be an $[n,k]$ cyclic code with a generator $g(x) = \sum_{i=0}^{n-k} g_i x^i$. We know that $g \bmod x^n - 1$ and therefore there exists $h(x) = \sum_{i=0}^{k} h_i x^i$ such that $gh = x^n - 1$.

Let $c \in \mathcal{C}$. As g generates $\mathcal{C}$ we have $c = ga$ for some $a \in \mathbb{F}_q[x]$. Therefore

$$hc \bmod (x^n - 1) = hga \bmod (x^n - 1) = 0.$$

This translates to the n constraints:

$$c_0 h_i + c_1 h_{i-1} + \ldots + c_{n-k} h_{i-n+k} \;=\; 0,$$

for every $0 \le i \le n-1$, where the indices are modulo n. It follows that

$$H^T \;=\; \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & & & & \\ & h_k & h_{k-1} & \cdots & h_0 & & & \\ & & \ddots & \ddots & \cdots & \ddots & & \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix} \tag{1}$$

is a $(n-k)\times n$ matrix of parity checks of $\mathcal{C}$, and because it has the correct rank $n-k$ it is a parity check matrix of $\mathcal{C}$.

Looking at the generator matrix of a polynomial code we see that:

Theorem 8. *Let $\mathcal{C}$ be an $[n,k]$ cyclic code generated by $g(x)$ and let $h(x)=\frac{x^n-1}{g(x)}$. Then, the dual code of $\mathcal{C}$ is a cyclic $[n,n-k]$ code whose generator polynomial is $x^k h(x^{-1})$. The polynomial $h(x)$ is called the* check polynomial *of $\mathcal{C}$.*

Proof. Clearly, the dual code of $\mathcal{C}$ is generated by the polynomial $\sum_{j=0}^{k} h_{k-j}x^j$. The only thing remaining is to note that

$$\sum_{j=0}^{k} h_{k-j}x^j=\sum_{j=0}^{k} h_j x^{k-j}=x^k h(x^{-1}).$$

□

3 The Hamming code is cyclic

Any binary Hamming code is equivalent to a cyclic code.

Theorem 9. *Fix a field $\mathbb{F}_{2^r}$ and let $n=2^r-1$. Then, there exists a $[n,k=n-r,3]_2$ cyclic code. Since the only code with such length, dimension and distance is the Hamming code, the Hamming code is cyclic.*

Proof. Let α be a generator of $\mathbb{F}_{2^r}^*$. Let g be the minimal polynomial of α over $\mathbb{F}_q$. Then $g \mid x^n-1$ because $\alpha^n-1=0$. Also, g is irreducible and $\deg(g)\le r$. As α generates $\mathbb{F}_{2^r}^*$ we must have $\deg(g)=r$. The code $\mathcal{C}$ generated by g is therefore a cyclic $[n,n-r]_2$ code. The minimal polynomial g vanishes on α and all its conjugates, so $g(x)=\Pi_{i=0}^{m-1}(x-\alpha^i)$ (and this also determines what is h such that $gh=x^n-1$).

The code $\mathcal{C}$ can be described as all elements $c=(c_0,\ldots,c_{n-1})\in\mathbb{F}_2^r$ such that $c(\alpha)=0$, or equivalently, that $H^t(c)=0$ where

$$H^T = \begin{pmatrix} v_0 & v_1 & \cdots & v_{n-1}\end{pmatrix} \tag{2}$$

where v_i is a column vector representing α^i in $\mathbb{F}_2^r$, with some fixed basis of F_{2^r} as an r dimensional vector space over $\mathbb{F}_2$. Notice that it is also true that $c(\alpha^{2^i})=0$ for any i, but these equations are redundant, because they are implied from the equation $c(\alpha)=0$.

Now, what is the distance of $\mathcal{C}$? Check that no two columns of H^t are dependent (otherwise, $\alpha^i=b\alpha^j$, for $i\ne j$ and $b\in\mathbb{F}_2$, and that is wrong (why?). Hence the distance of $\mathcal{C}$ is at least 3. As the Hamming code is perfect it is exactly 3. □

An *automorphisim* of a $[n,k]$ code $\mathcal{C}$ is a permutation π on the set of n coordinates that preserves the code. For example, cyclic codes are preserved by permutations that map i to $i+k \bmod n$. Automorphisims are closed under composition and inverse and therefore give rise to an *automorphim group* of the code. For example, if we take the $[n=2^r-1,k=n-r]_2$ Hamming code and index the coordinates by $\mathbb{F}_n^*=\left\{\alpha^i\right\}$ in the natural order, then the permutation $x\to\alpha x$ is an automorphism (corresponding to a cyclic shift), and also the Frobenius mapping $x\to x^2$ (again, applied on the coordinates) is an automorphism (check!).

References

[1] Ron Roth. *Introduction to coding theory.* Cambridge University Press, 2006.