Generator polynomials of cyclic codes

Robin Chapman

25 March 2004 (corrected 28 November 2007)

We consider cyclic codes of length n over Z_p. We use the truncated polynomial ring $Z_p[X]_n$, which consists of polynomials in X over Z_p subject to the extra stipulation that $X^n = 1$ (and so $X^{n+1} = X$, $X^{n+2} = X^2, \ldots, X^{2n} = X^n = 1$ etc.).

We recall some polynomial jargon. Let $f = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d$ be a typical polynomial. If $a_d \neq 0$ we call a_d the *leading coefficient* of f, a_dX^d the *leading term* of f and d the *degree* of f. If the leading coefficient of f is 1 we say that f is *monic*.

Recall the bijection $\Phi : (Z_p)^n \to Z_p[X]_n$ taking $(a_0, a_1, \ldots, a_{n-1})$ to $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$. Also recall that C is a cyclic code if and only if $\Phi(C)$ is an *ideal* of $Z_p[X]_n$, that is

- if f_1, $f_2 \in \Phi(C)$ then $f_1 + f_2 \in \Phi(C)$, and
- if $f \in \Phi(C)$ and $g \in Z_p[X]_n$ then $gf \in \Phi(C)$.

This means that the problem of classifying cyclic codes of length n over Z_p is equivalent to classifying ideals of $Z_p[X]_n$.

A *principal* ideal over $Z_p[X]_n$ is a set of the form

$$\langle g \rangle = \{hg : h \in Z_p[X]_n\}.$$

It is plain that this is an ideal. The main result is that all ideals of $Z_p[X]_n$ are principal, and even more is true.

Theorem 1 *Let $\mathcal{I}$ be an ideal of $Z_p[X]_n$. Then $\mathcal{I} = \langle g \rangle$ where g is a monic polynomial and g is a factor of $X^n - 1$. This g is uniquely determined.*

Proof We first assume that $\mathcal{I}$ contains some nonzero polynomial. If $f \in \mathcal{I}$ is nonzero with leading coefficient a, then $m = bf$ is monic where b is the reciprocal of a in Z_p. Also m has the same degree as f and $m \in \mathcal{I}$. Thus if $\mathcal{I}$

contains a nonzero polynomial, it contains a monic polynomial of the same degree.

Let g be a monic polynomial of least degree in $\mathcal{I}$. By the above $\mathcal{I}$ cannot contain any polynomial of lower degree. If $f \in Z_p[X]$ then there are polynomials u and v in $Z_p[X]$ such that $f = ug + v$ and either $v = 0$ or v has smaller degree than g. In particular, when $f \in \mathcal{I}$ then also $v = f + (-u)g \in \mathcal{I}$ and this means that v must be zero. So $f \in \mathcal{I}$ means that $f = ug \in \langle g \rangle$. Consequently $\mathcal{I} \subseteq \langle g \rangle$. But as $g \in \mathcal{I}$ then $hg \in \mathcal{I}$ for all $h \in Z_p[X]_n$ and so $\langle g \rangle \subseteq \mathcal{I}$. We conclude that $\mathcal{I} = \langle g \rangle$ and so $\mathcal{I}$ is principal.

Next, there are polynomials u and v such that $X^n - 1 = ug + v$ and either $v = 0$ or v has smaller degree than g. Inside $Z_p[X]_n$, $X^n - 1 = 0$ and so $v = -ug \in \mathcal{I}$. Again, this is impossible unless $v = 0$. Thus $X^n - 1 = ug$: that is, g is a factor of $X^n - 1$.

To show that g is unique, suppose that g_1 is monic, g_1 is a factor of $X^n - 1$ and $\mathcal{I} = \langle g_1 \rangle$. Then g is a factor of g_1 and g_1 is a factor of g: thus there are polynomials u and v (which must be monic) with $g_1 = ug$ and $g = vg_1$. Then $f = uvg$ and so $uv = 1$ which implies $u = v = 1$ (as u and v are monic), equivalently $g = g_1$.

We have assumed that $\mathcal{I}$ contains a nonzero polynomial. If it doesn't then $\mathcal{I} = \{0\}$ (a rather uninteresting ideal!) but if we take $g = X^n - 1$ (which is zero inside $Z_p[X]_n$) then the result still holds. □

If C is a cyclic code we call the unique monic g dividing $X^n - 1$ and satisfying $\phi(C) = \langle g \rangle$ the *generator polynomial* of g.

Theorem 2 *Let C be a cyclic code with generator polynomial g of degree d. Then C has dimension $n - d$ and generator matrix*

$$G = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_d & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{d-1} & b_d & 0 & \cdots & 0 \\ 0 & 0 & b_0 & \cdots & b_{d-2} & b_{d-1} & b_d & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & b_2 & \ddots & b_d \end{pmatrix}$$

where

$$g(X) = \sum_{j=0}^{d} b_j X^j.$$

Proof Clearly the matrix G has linearly independent rows. For the moment, let C' denote the code generated by the rows of G. Certainly C' has dimension $n - d$. If $\mathbf{g}_j$ is the j-the row of G, then $\Phi(\mathbf{g}_j) = X^{j-1}g \in \langle g \rangle$ so certainly $C' \subseteq C$.

For the reverse inclusion write $X^n - 1 = gh$. Then h has degree $n - d$. Let $f \in Z_p[X]$. We can write $f = uh + v$ where u and v are polynomials with v zero or its degree is less than that of h, namely $n - d$. Thus $v = c_0 + c_1X + \cdots + c_{n-d-1}X^{n-d-1}$. Thus

$$fg = uhg + vg = (X^n - 1)g + vg.$$

Inside $Z_p[X]_n$, $X^n - 1 = 0$, and so

$$fg = vg = \sum_{j=0}^{n-d-1} c_j X^j g = \sum_{j=0}^{n-d-1} c_j \Phi(\mathbf{g}_{j+1}) = \Phi(\mathbf{x})$$

where

$$\mathbf{x} = (c_0\ c_1\ c_2 \cdots c_{n-d-1})G \in C'.$$

Hence $fg \in \Phi(C')$. If $\mathbf{a} \in C$ then $\Phi(\mathbf{a}) = fg$ for some polynomial f, and so $\Phi(\mathbf{a}) = \Phi(\mathbf{x})$ for some $\mathbf{x} \in C'$. Thus $\mathbf{a} = \mathbf{x} \in C'$. We conclude that $C \subseteq C'$ and so $C = C'$. □

If C is a cyclic $[n, k]$-code with generator polynomial g then g has degree $n - k$. Also $X^n - 1 = gh$ where h has degree h. We call h the *parity-check polynomial* of C.

Theorem 3 *Let C be a cyclic $[n, k]$-code with generator polynomial g and parity-check polynomial h. Then $\Phi(C)$ consists of those polynomials $f \in Z_p[X]$ with the property that $hf = 0$ in $Z_p[X]$. Also*

$$H = \begin{pmatrix} c_k & c_{k-1} & c_{k-2} & \cdots & c_0 & 0 & 0 & \cdots & 0 \\ 0 & c_k & c_{k-1} & \cdots & c_1 & c_0 & 0 & \cdots & 0 \\ 0 & 0 & c_k & \cdots & c_2 & c_1 & c_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & c_k & c_{k-1} & c_{k-2} & \ddots & c_0 \end{pmatrix}$$

is a parity-check matrix for C where

$$h(X) = \sum_{j=0}^{k} c_j X^j.$$

Proof Note that $\Phi(C) = \langle g \rangle$. If $f \in \langle g \rangle$ then $f = ug$ for some polynomial and so $hf = ugh = u(X^n - 1) = 0$ in $Z_p[X]_n$. Conversely if $hf = 0$ in $Z_p[X]_n$ then $hf = v(X^n - 1)$ for some polynomial v and so $hf = vgh$ whence $f = vg \in \langle g \rangle$.

Let $f = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in Z_p[X]_n$. If we expand out hf inside $Z_p[X]_n$ we find that the coefficient of X^k is

$$c_k a_0 + c_{k-1} a_1 + \cdots + c_0 a_k = \mathbf{c} \cdot \mathbf{a}$$

where $\mathbf{c} = c_k c_{k-1} \cdots c_0 0 \cdots 0$ and $\mathbf{a} = a_0 a_1 \cdots a_{n-1}$. If $\mathbf{a} \in C$ then $f \in \phi(C) = \langle g \rangle$ and so $fh = 0$; consequently $\mathbf{c} \cdot \mathbf{a} = 0$ and so $\mathbf{c} \in C^\perp$. Thus the top row of H lies in $C^\perp$. As C is cyclic, so is $C^\perp$ and so all rows of H lie in $C^\perp$. It is clear that the rows of H are linearly independent, so H is a generator matrix for a code C' of dimension d with $C' \subseteq C^\perp$. As these codes have the same dimension, $C' = C^\perp$: H is a generator matrix for $C^\perp$, that is H is a parity-check matrix for C. □

A polynomial over Z_p is *irreducible* if it has degree at least one and is not a product of polynomials of smaller degree. A theorem of algebra states that each monic polynomial in $Z_p[X]$ can be written in a unique fashion as a product of irreducible monic polynomials (the proof is basically the same as that concerning unique prime factorization of integers). If we group together identical irreducible polynomials we find that an arbitrary monic polynomial m can be written as

$$f = q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k}$$

where the q_j are distinct irreducible monic polynomials and the r_j are positive integers. As a further consequence of the unique factorization theorem, each factor of f has the form

$$g = q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$$

where $0 \leq s_j \leq r_j$. This means that if we can factorize f into irreducibles then we can write down all its factors. In particular, taking $f = X^n - 1$ allows us to find all possible generator polynomials of cyclic $[n, k]$-codes. Algorithms for factorizing polynomials into irreducibles are beyond the scope of this course, but they are implemented in `MAPLE`. In particular

```
> Factor(f) mod p;
```

factorizes the polynomial f over Z_p.

My thanks to Erol Chartan for pointing out an error in the original version.