A note on the generator polynomials

The goal of this note is to relate the definition of the generator polynomial for a cyclic code given in class to the definition given in the book. As usual, for a field F a $n \in \mathbb{N}$ we let $R_n = R_n(F) = F[x]/(x^n - 1)$ and $\pi : F^n \to R_n(F)$ is the map given by

$$\pi((a_0, \ldots, a_{n-1})) = \sum_{k=0}^{n-1} a_k x^k.$$

Also recall that for $u(x), v(x) \in R_n$ we set $u(x) \odot v(x) = (u(x)v(x)) \mod (x^n - 1)$, the product of $u(x)$ and $v(x)$ in R_n.

The following is the definition of the generator polynomial from the book.

Definition 1. Let C be a nonzero cyclic code of length n over F. The *generator* of C is the unique monic polynomial of smallest possible degree in $\pi(C)$.

Let us see that such a polynomial is indeed unique. First, we need to show that $\pi(C)$ contains at least one monic polynomial. This is clear – since $C \neq 0$ and π is bijective, $\pi(C)$ contains some nonzero polynomial $f(x)$. If we divide $f(x)$ by its leading coefficient, we obtain a monic polynomial which still lies in $\pi(C)$ since $\pi(C)$ is closed under scalar multiplication.

Next we prove uniqueness. Suppose, by way of contradiction, that $\pi(C)$ contains two distinct monic polynomials $g_1(x)$ and $g_2(x)$ which both have degree k, where k is the smallest possible degree of a monic polynomial in $\pi(C)$. Thus, for $i = 1, 2$ we have $g_i(x) = x^k + r_i(x)$ where $\deg r_i(x) < k$. But then $g_1(x) - g_2(x) = r_1(x) - r_2(x)$ is a NONZERO polynomial which still lies in $\pi(C)$. Again dividing $g_1(x) - g_2(x)$ by its leading coefficient, we obtain a monic polynomial of degree $< k$ which lies in $\pi(C)$. This contradicts the choice of k.

Thus, we showed that generator of C is well-defined according to the above definition.

Let us now recall the definition from class:

Definition 2. Let C be a nonzero cyclic code of length n over F. The *generator* of C is the unique polynomial in R_n satisfying the following 3 conditions:

(i) $\langle g(x)\rangle = \pi(C)$
(ii) $g(x)$ is monic
(iii) $g(x)$ divides $x^n - 1$

Theorem 1. *Suppose that $g(x)$ is the generator of C according to Definition 1, that is, $g(x)$ is the unique monic polynomial of smallest possible degree in $\pi(C)$. Then $g(x)$ is also the generator of C according to Definition 2, that is, $g(x)$ satisfies conditions (i)-(iii) above.*

Proof. Condition (ii) holds by assumption.

Let us now check condition (i). Since $g(x) \in \pi(C)$ by assumption and $\pi(C)$ is an ideal, all the multiples of $g(x)$ are also in $\pi(C)$, so

$$\langle g(x)\rangle \subseteq \pi(C).$$

To prove the reverse inclusion, take any $f(x) \in \pi(C)$ and divide it by $g(x)$ with remainder. We get $f(x) = g(x)q(x) + r(x)$ where $\deg r(x) < \deg g(x)$. Since $g(x)q(x) = g(x) \odot q(x) \in \langle g(x)\rangle \subseteq \pi(C)$, we have

$$r(x) = f(x) - g(x)q(x) \in \pi(C).$$

If $r(x) \neq 0$, then dividing $r(x)$ by its leading term, we get a monic polynomial in $\pi(C)$ whose degree is less than $\deg g(x)$, which is impossible. Therefore, $r(x) = 0$ and hence $f(x) = g(x)q(x) = g(x) \odot q(x) \in \langle g(x)\rangle$. Thus, we proved the reverse inclusion $\pi(C) \subseteq \langle g(x)\rangle$ and therefore condition (i).

Finally, let us prove (iii). Again, we can always divide $x^n - 1$ by $g(x)$ with remainder: $x^n - 1 = g(x)Q(x) + R(x)$ where $\deg(R(x)) < \deg g(x)$. Rewriting this equality as $g(x)Q(x) = x^n - 1 - R(x)$ and taking the remainders of both sides mod $x^n - 1$, we get $g(x) \odot Q(x) = -R(x)$ and so $-R(x) \in \langle g(x)\rangle \subseteq \pi(C)$. Since $\deg(-R(x)) < \deg g(x)$, as in the proof of (i) this implies that $R(x) = 0$ and therefore $g(x)$ divides $x^n - 1$, as desired. □

Remark: The proof of (i) actually shows that if $g(x)$ is the generator for C, then

(i)' $\pi(C)$ is the set of all $f(x) \in R_n$ such that $f(x) = g(x)u(x)$ for some $u(x) \in F[x]$ (this is a product in $F[x]$)

A priori (i)' is a stronger condition than (i): if we take an arbitrary element $g(x) \in R_n$, the ideal $\langle g(x)\rangle$ can be strictly larger than the set

$$Mult(g(x)) = \{f(x) \in R_n : f(x) = g(x)u(x) \text{ for some } u(x) \in F[x]\}.$$

For instance, take $g(x) = x$. Then $1 \in \langle g(x)\rangle$ since $x \odot x^{n-1} = (x \cdot x^{n-1}) \bmod (x^n - 1) = 1$, but $1 \notin Mult(g(x))$. However, it is true that $\langle g(x)\rangle = Mult(g(x))$ whenever $g(x)$ is a divisor of $x^n - 1$.