Mathematics 392 – Seminar in Coding Theory
Selected Solutions – Individual Problem Set 3
April 15, 2002

5.1.18. To show: If β is primitive in $\mathbf{F}_{2^r}$, then β^i is primitive $\Leftrightarrow \gcd(i, 2^r - 1) = 1$.

This can be proved in several ways, based on which of the different (equivalent) ways to say that an element is primitive you use. Here are two.

Approach 1. (Using the "direct" definition that an element $\alpha \in \mathbf{F}_{2^r}$ is primitive if the smallest strictly positive power ℓ such that $\alpha^\ell = 1$ is $\ell = 2^r - 1$.)

$\Rightarrow$: Our hypothesis is that β^i is primitive. Then the smallest positive power of β^i that equals 1 is $1 = (\beta^i)^{2^r-1}$, and $(\beta^i)^q = 1$ if $0 < q < 2^r - 1$. Aiming for a contradiction, suppose that $\gcd(i, 2^r - 1) = m > 1$. Then $i = mq_1$ and $2^r - 1 = mq_2$, so $q_2 < 2^r - 1$. But then

$$(\beta^i)^{q_2} = \beta^{iq_2} = \beta^{mq_1q_2} = (\beta^{2^r-1})^{q_1} = 1$$

Since $q_2 < 2^r - 1$, this is a contradiction. Hence

$\Leftarrow$: Now our hypothesis is $\gcd(i, 2^r - 1) = 1$. We want to show that $(\beta^i)^\ell \neq 1$ for $0 < \ell < 2^r - 1$. Again, aiming for a contradiction, assume that $(\beta^i)^\ell = \beta^{i\ell} = 1$ for some $0 < \ell < 2^r - 1$. But then because β is primitive by hypothesis, $i\ell \equiv 0 \bmod 2^r - 1$. Since $\gcd(i, 2^r - 1) = 1$ this implies $\ell \equiv 0 \bmod 2^r - 1$. But that is a contradiction because $0 < \ell < 2^r - 1$. Hence the smallest positive power of β^i that equals 1 is the $2^r - 1$ power.

Approach 2. (Using the equivalent form of the definition of primitive elements – α is primitive if every nonzero element of the field is some power of α.)

$\Rightarrow$: Our hypothesis is that β^i is primitive. Hence $\beta = (\beta^i)^q = \beta^{iq}$ for some q. But since β is primitive, this implies that $iq \equiv 1 \bmod 2^r - 1$, or $iq = 1 + \ell(2^r - 1)$ for some integer ℓ. This equation shows that $\gcd(i, 2^r - 1) = 1$ since any common divisor of i and $2^r - 1$ would also have to divide $iq - \ell(2^r - 1) = 1$.

$\Leftarrow$: Now our hypothesis is $\gcd(i, 2^r - 1) = 1$. This implies that there are integers m_1, m_2 such that $1 = m_1 i + m_2(2^r - 1)$. But then

$$\beta = \beta^{m_1 i + m_2(2^r-1)} = (\beta^i)^{m_1} \cdot (\beta^{2^r-1})^{m_2} = (\beta^i)^{m_1} \cdot 1 = (\beta^i)^{m_1}$$

Since β is a power of β^i, every power of β is also a power of β^i. It follows that every nonzero element of the field is some power of β^i, so β^i is primitive.

A) Given: $m \equiv \overline{m} \bmod n$ or equivalently, $m = \overline{m} + qn$ for some integer q. Then

$$\begin{aligned} x^m + x^{\overline{m}} &= x^{\overline{m}+qn} + x^{\overline{m}} \\ &= x^{\overline{m}}(x^{qn} + 1) \end{aligned}$$

By the factorization for a difference of like powers:

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}),$$

with coefficients in $\mathbf{F}_2$, we have

$$x^{qn} + 1 = (x^n + 1)(x^{(q-1)n} + x^{(q-2)n} + \cdots + x^n + 1)$$

Hence $x^n + 1$ divides $x^m + x^{\overline{m}}$, which is what we had to show.

B) 3) Every polynomial in $\mathbf{F}_2[x]$ can be written in one and only one way as a product of irreducible polynomials (ignoring the order of the factors in the product, of course). In the product

$$\prod_{r=1}^{\infty} \left(\frac{1}{1-t^r}\right)^{N_r} = \prod_{r=1}^{\infty} \left(\prod_{k=1}^{N_r} \left(\frac{1}{1-t^r}\right)\right) \tag{1}$$

there is one factor $\frac{1}{1-t^r} = 1 + t^r + t^{2r} + \cdots$ for each irreducible of degree r. The term t^{kr} in the factor corresponding to a given irreducible of degree r can be thought of as meaning k copies of that irreducible (like the terms in the factors in the product in part 1, which represent different numbers of pennies, nickels, or dimes). Each time we get a t^n term when we multiply out the product, it will come from some terms in the factors, whose exponents add up to n. The factors that multiply together to give each t^n represent a certain number (possibly zero, or > 1) of each of the irreducibles of each degree. The sum of the degrees of the corresponding polynomials is n. Hence when we multiply out the product in (1) and collect the t^n terms, the coefficient of t^n will be the total number of ways of multiplying irreducibles together to get a product of degree n, which is the same as the number of polynomials of degree exactly n. This shows

$$\frac{1}{1-2t} = \sum_{n=0}^{\infty} 2^n t^n = \prod_{r=1}^{\infty} \left(\frac{1}{1-t^r}\right)^{N_r}$$