Appendix H: Order Reversal Theorems for Irreducible Polynomials

An order-reversed polynomial is one in which the order of the coefficients is reversed. For example, here H(x) is the order-reversed version of h(x),

$$h(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots c_{k-1}x^{k-1} + c_kx^k = \{c_0,c_1,c_2.....c_{k-1},c_k\}$$
$$H(x) = c_k + c_{k-1}x + c_{k-2}x^2 + c_{k-2}x^3 + \ldots + c_1x^{k-1} + c_0x^k = \{c_k, c_{k-1}.....c_2,c_1, c_0\} \quad \text{(H.1)}$$

Peterson and Weldon refer to such polynomials as being reciprocal. If h(x) and H(x) are the same polynomial, we call it a symmetric polynomial (self-reciprocal).

We shall now develop four Facts relating to order-reversed polynomials.

Fact 1: If h(x) is irreducible in R, then so is its order-reversed partner H(x). (H.2)

Corollary: Irreducible polynomials thus come in pairs as long as h(x) is not symmetric. Often tables of irreducible polynomials only state one of the pair in order to save space.

Proof of Fact 1: Let h(x) of degree k be irreducible for GF(p^m). We can write ($c_0 \neq 0$ and $c_k \neq 0$)

$$h(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_kx^k \qquad \text{degree } k \leq m \qquad GF(p^m)\ .$$

If c_0 were 0, we could factor out x and h(x) would be reducible. If c_k were 0, we would not have degree k which we want for this proof. Now consider the order-reversed polynomial,

$$H(x) = c_k + c_{k-1}x + c_{k-2}x^2 + c_{k-2}x^3 + \ldots + c_1x^{k-1} + c_0x^k \qquad \text{degree } k\ .$$

Notice that

$$H(1/x) = c_k + c_{k-1}x^{-1} + c_{k-2}x^{-2} + c_{k-2}x^{-3} + \ldots + c_1x^{-k+1}\ c_0x^{-k}$$
$$= x^{-k}\,[c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_kx^k]$$
$$= x^{-k}\,h(x)\ . \quad \text{(H.3)}$$

Assume h(x) is irreducible and H(x) is reducible. We will find a contradiction and conclude that if h(x) is irreducible, then the order-reversed H(x) must also be irreducible.

If H(x) is reducible then it can be written as the product of two polynomials in R whose degrees add up to the degree of H(x) which is k. So write,

$$H(x) = [g_n(x)][f_{k-n}(x)] \quad \text{(H.4)}$$

where the g_n is of degree n and f_{k-n} is of degree k-n. Values of n range from 1 to k-1, so each factor is at least linear in x, not just a constant. We then find that

$$h(x) = x^k H(1/x) = x^n x^{k-n} [g_n(1/x)][f_{k-n}(1/x)]$$

$$= \{ x^n g_n(1/x) \} \{ x^{k-n} f_{k-n}(1/x) \}$$

$$= \{ G_n(x) \} \{ F_{k-n}(x) \} \qquad (H.5)$$

where $G_n(x)$ and $F_{k-n}(x)$ are both polynomials in R with $1 \le n \le k-1$ so neither factor is a constant. Then h(x) is reducible, and this is our contradiction, QED.

Fact 2: If h(x) is a minimum polynomial in R, then so its order-reversed partner H(x). (H.6)

Corollary: Minimum polynomials thus come in pairs as long as h(x) is not symmetric. Often tables of minimum polynomials only state one of the pair in order to save space.

Proof of Fact 2: If h(x) is a a minimum polynomial in R, we know it is irreducible and it can be factored as

$$h(x) = (x-a_1)(x-a_2)..... (x-a_k) \qquad (H.7)$$

where the a_i are all elements of $GF(p^m)$ and are elements of a conjugate set as defined in Section 5 (c). We already know that H(x) is irreducible from Fact 1, but we need to show that H(x) is a minimum polynomial. From (H.3) ,

$$H(1/x) = x^{-k} h(x) . \qquad (H.3)$$

so that

$$H(x) = x^k h(1/x) = x^k(1/x-a_1)(1/x-a_2)..... (1/x-a_k)$$

$$= (1-a_1x) (1-a_2x)..... (1-a_kx)$$

$$= [(-a_1)(x-a_1^{-1})] [(-a_2)(x-a_2^{-1})] ... [(-a_k)(x-a_k^{-1})]$$

$$= \{(-a_1) (-a_2) ... (-a_k) \} \{(x-a_1^{-1}) (x-a_2^{-1}) ... (x-a_k^{-1}) .$$

Since any product of field elements is a field element, we can call the first factor γ in GF(q). Then

$$H(x) = \gamma (x-a_1^{-1}) (x-a_2^{-1}) ... (x-a_k^{-1}) . \qquad (H.8)$$

According to following Lemma, we know that the inverses of the elements of a conjugate set form a conjugate set, and therefore H(x) is a minimum polynomial, QED.

Lemma 1: The set formed by inverting the elements of a conjugate set is a conjugate set. (H.9)

Proof: If α is a primitive element of GF(q), then we can enumerate GF(q) this way from (4.31),

$$\{ 0, 1, \alpha, \alpha^2, \alpha^3, \ldots\ldots \alpha^{q-2} \} \qquad \alpha^{q-1} = 1 \qquad \alpha^q = \alpha \quad . \tag{4.31}$$

The general form of a conjugate set from (5.40) is

$$\{ \alpha^s, \alpha^{sp}, \alpha^{sp^2}, \alpha^{sp^3} \quad , \ldots. \alpha^{sp^{k-1}} \} , \tag{5.40}$$

where α is a primitive element of GF(q) and α^s is some other element of GF(q) where s is an integer which we normally think of as lying in the range 1 to q-1. If we set s = q-2, we get this conjugate set

$$\{ \alpha^{(q-2)}, \alpha^{(q-2)p}, \alpha^{(q-2)p^2}, \alpha^{(q-2)p^3} \quad , \ldots. \alpha^{(q-2)p^{k-1}} \} . \tag{H.10}$$

If α^{-1} is the inverse of α, then $\alpha\ \alpha^{-1} = 1$. On the other hand, we know $\alpha\ \alpha^{q-2} = \alpha^{q-1} = 1$. Therefore we can identify

$$\alpha^{-1} = \alpha^{(q-2)} \tag{H.11}$$

and we can write the above conjugate set as

$$\{ \alpha^{-1}, (\alpha^{-1})^p, (\alpha^{-1})^{p^2}, (\alpha^{-1})^{p^3} \quad , \ldots. (\alpha^{-1})^{p^{k-1}} \} . \tag{H.12}$$

We know that in general

$$(\alpha^n)^{-1} = (\alpha\ \alpha\ \alpha \ldots)^{-1} = \alpha^{-1}\ \alpha^{-1}\ \alpha^{-1} \ldots = (\alpha^{-1})^n \tag{H.13}$$

so we can write the above conjugate set as

$$\{ \alpha^{-1}, (\alpha^p)^{-1}, (\alpha^{p^2})^{-1}, (\alpha^{p^3})^{-1} \quad , \ldots. (\alpha^{p^{k-1}})^{-1} \} \tag{H.14}$$

Since this is a conjugate set, we have shown that the inverses of the elements of a conjugate set form a conjugate set (in general a different one with the same number of elements). QED.

Fact 3: If h(x) is a primitive polynomial in R, then so is its order-reversed partner H(x). (H.15)

Corollary: Primitive polynomials thus come in pairs as long as h(x) is not symmetric (see Fact 4 below). Often tables of primitive polynomials only state one of the pair in order to save space.

Proof of Fact 3: If h(x) is a primitive polynomial of GF(p^m) then it is of degree m and from (5.35) all members of its conjugate set a_i are primitive elements of GF(q). From (H.10) $\alpha^{-1} = \alpha^{(q-2)}$. According to (4.32), if α is primitive, $\alpha^{-1} = \alpha^{(q-2)}$ is also primitive since GCD(q-2,q-1) = 1 (see following Lemma). Now recall from Fact 1 the forms for h(x) and its order-reversed H(x),

$$h(x) = (x-a_1)(x-a_2)..... (x-a_k) \qquad (H.7)$$

$$H(x) = \gamma\ (x-a_1^{-1})\ (x-a_2^{-1})\ ...\ (x-a_m^{-1})\ . \qquad (H.8)$$

Letting $\alpha = a_1$, a primitive element of h(x), we have just shown that $\alpha^{-1} = a_1^{-1}$ is also a primitive element and therefore H(x) is a primitive polynomial (and all the a_i^{-1} are primitive elements of GF(q)).

Lemma 1: The GCD of two sequential integers is 1. (H.16)

Proof: Assume GCD(n,n+1) = N > 1. Then there exist integers I and J such that

$$n/N = I \quad => \quad n = IN$$
$$(n+1)/N = J \quad => \quad n+1 = JN \quad => \quad IN + 1 = JN \quad => \quad N(J-I) = 1\ .$$

We end up then with (J-I) = 1/N which is impossible unless N = 1, QED.

Fact 4: A primitive polynomial h(x) for GF(p^m) *cannot* be symmetric if p and m are in these ranges:

p = 2 with m ≥ 3
p = 3 with m ≥ 2
p > 3 (H.17)

Corollary: Thus, the only fields for which h(x) *can* be symmetric are GF(2), GF(2^2) and GF(3). This means there are no symmetric primitive polynomials of degree greater than 2 for any GF(q). As was shown in Chapter 5 (c), for GF(2) and GF(3) the only primitive polynomial is 1+x, and for GF(2^2) the only one is $1 + x + x^2$ as we found in (5.29). Thus, in the only cases in which h(x) *can* be symmetric, it *is* symmetric (Murphy's Law). (H.18)

Proof of Fact 4: The conjugate set of h(x) with respect to GF(p^m) looks like this, where α is a primitive element of GF(p^m) :

$$\{\ \alpha,\ \alpha^p,\ \alpha^{p^2},\ \alpha^{p^3}\ ,\ ....\ \alpha^{p^{m-1}}\ \} \qquad \alpha^{p^m} = \alpha \qquad \text{m conjugates} \qquad (5.16)$$

The conjugate set of H(x) we found from (H.10) is, with k = m now since h(x) is primitive,

$$\{\ \alpha^{(q-2)},\ \alpha^{(q-2)p},\ \alpha^{(q-2)p^2},\ \alpha^{(q-2)p^3}\ ,\ ....\ \alpha^{(q-2)p^{m-1}}\ \}\ . \qquad (H.10)$$

In order to have h(x) = H(x), these two conjugate sets have to be the same. One must be at worst a rearrangement of the other. But we shall now show that the element α is *missing* from the second set under the conditions stated above, and therefore the two sets cannot be the same, and therefore we cannot have H(x) = h(x) and therefore h(x) cannot be symmetric.

In order to have α be present in the second set we would have to have

$$\alpha = \alpha^{(q-2)p^i} \qquad \text{for some i in range 0 to m-1}$$

Multiply both sides by α^{p^i} to get

$$\alpha^{p^i+1} = \alpha^{(q-1)p^i} = [\alpha^{q-1}]^{p^i} = [1]^{p^i} = 1 \quad .$$

Since α is a primitive element of GF(p^m), we know that $\alpha^{q-1} = 1$. In order for the above equation to be true, we must have p^i+1 be a multiple of $q-1 = p^m - 1$ for some i in (0,m-1):

$$p^i+1 = K(p^m - 1) \qquad K = \text{integer} \qquad \text{(H.19)}$$

Obviously K = 0 does not work. We try K = 1 next. But for (p,m) in the ranges stated below, we will show that in fact $p^i+1 < (p^m - 1)$, so K = 1 does not work nor does any K > 1 work.

In order to show that $p^i+1 < (p^m - 1)$ for all i in our range 0 to m-1, if suffices to show this for the largest exponent i = m-1, for then it will be true as well for all smaller i. So we want to show that, for a certain range of p and m, we have

$$p^{m-1}+1 < (p^m - 1)$$

or

$$p^m - p^{m-1} > 2$$

or

$$p^{m-1}(p-1) > 2$$

Lemma 2 below shows that this inequality is true for p and m in these ranges

p = 2	m ≥ 3		
p = 3	m ≥ 2		
p > 3	m ≥ 1	or just	p > 3

These then are the ranges for which no K exists in (H.18) and therefore α which is in the conjugate set of h(x) is NOT in the conjugate set of H(x). These sets are then different, so h(x) ≠ H(x) which means h(x) cannot have symmetric coefficients for p and m as shown above.

Lemma 2: The inequality $p^{m-1}(p-1) > 2$ is true for the following values of p and m:

p = 2	true for m ≥ 3
p = 3	true for m ≥ 2
p > 3	true for m ≥ 1

(H.20)

Proof: Start with p = 2

$$2^{m-1} * 1 > 2 \qquad ?$$

For m ≥3 this is clearly true, but it is not true for m = 1 or m = 2.

Now consider p = 3.

$$3^{m-1}(2) > 2 \qquad ?$$

This is true for $m \geq 2$. Finally, consider $p > 3$.

$$p^{m-1}(p-1) > 2 \qquad ?$$

In this case $(p-1) > 2$ all by itself and so this is valid for $m \geq 1$. QED.