2003

A Characterization of Primitive Polynomials over Finite Fields

Robert W. Fitzgerald
Southern Illinois University Carbondale, rfitzg@math.siu.edu

Published in *Finite Fields and Their Applications*, 9, 117-121

A CHARACTERIZATION OF PRIMITIVE POLYNOMIALS OVER FINITE FIELDS

Robert W. Fitzgerald

Southern Illinois University

1. The Characterization.

Let p be a prime and q a power of p. $GF(q)$ denotes the field of order q.

Theorem. *Let $p(x)$ be an irreducible polynomial of degree k over $GF(q)$. Set $m = q^k - 1$. Define $g(x) = (x^m - 1)/(x-1)p(x)$. Then $p(x)$ is primitive iff $g(x)$ has exactly $(q-1)q^{k-1} - 1$ non-zero terms.*

Proof. Write:

$$p(x) = p_0 x^k + p_1 x^{k-1} + \cdots + p_k = \sum_{i=0}^{k} p_i x^{k-i}$$

$$g(x) = \epsilon_1 x^{m-1-k} + \epsilon_2 x^{m-2-k} + \cdots + \epsilon_{m-k} = \sum_{j=1}^{m-k} \epsilon_j x^{m-j-k}.$$

Note that $p_0 = 1$. Now $p(x)g(x) = (x^m - 1)/(x-1) = x^{m-1} + x^{m-2} + \cdots + x + 1$. Matching the coefficient of $x^{m-\ell}$ gives

$$\sum_{i+j=\ell} p_i \epsilon_j = 1. \tag{1}$$

For $\ell = n + k$, $n \geq 1$, this becomes

$$\sum_{i=0}^{k} p_i \epsilon_{n+k-i} = 1.$$

Since $p_0 = 1$ we can write this as:

$$\epsilon_{n+k} = -\sum_{i=1}^{k} p_i \epsilon_{n+k-i} + 1 \tag{2}$$

We will view (2) as an (infinite) linear recurring sequence. The initial values $\epsilon_1, \epsilon_2, \ldots \epsilon_k$ can be computed from (1) by taking $\ell = 1, 2, \ldots, k$. We form the homogeneous version of

Typeset by $\mathcal{AMS}$-TEX

(2) in the usual way. Write out the formula for ϵ_{n+k+1} and subtract the formula for ϵ_{n+k}. This yields:

$$\epsilon_{n+k+1} = (1-p_1)\epsilon_{n+k} + \sum_{i=1}^{k-1}(p_i - p_{i+1})\epsilon_{n+k-i} + p_k\epsilon_n. \tag{3}$$

Claim 1. The characteristic polynomial of (3) is $(x-1)p(x)$.

By definition, the characteristic polynomial is:

$$f(x) = x^{k+1} + (p_1 - 1)x^k + \sum_{i=1}^{k-1}(p_{i+1} - p_i)x^{k-i} - p_k.$$

This is easily checked to be $(x-1)p(x)$.

We consider the linear recurring sequence with characteristic polynomial $p(x)$, namely:

$$\eta_{n+k} = -p_1\eta_{n+k-1} - p_2\eta_{n+k-2} - \cdots - p_k\eta_n, \tag{4}$$

with the initial values $\eta_1, \eta_2, \ldots, \eta_k$ to be determined.

Claim 2. There is a non-zero K and choices for $\eta_1, \ldots, \eta_k$ such that $\epsilon_i = \eta_i + K$, for all $i \geq 1$.

Let $S(f(x))$ be the vector space of all sequences satisfying $f(x)$. By [1, 6.55]

$$S(p(x)) + S(x-1) = S((x-1)p(x)).$$

A sequence is in $S(x-1)$ iff $s_{n+1} = s_n$ for all n, that is, iff it is a constant sequence. Say $s_n = K$ for all n. Now (4) is in $S(p(x))$ and (3) is in $S((x-1)p(x))$, by **Claim 1**. Hence $\epsilon_i = \eta_i + K$, for all i, for some choice of initial η_i.

We lastly check that $K \neq 0$. We have:

$$\begin{aligned}
\eta_{k+1} &= -p_1\eta_k - p_2\eta_{k-1} - \ldots - p_k\eta_1 \\
\epsilon_{k+1} - K &= -p_1(\epsilon_k - K) - p_2(\epsilon_{k-1} - K) - \cdots - p_k(\epsilon_1 - K) \\
&= K(p_1 + \cdots + p_k) - p_1\epsilon_k - \cdots - p_k\epsilon_1 \\
&= K(p_1 + \cdots + p_k) + \epsilon_{k+1} - 1,
\end{aligned}$$

from (2). We thus have $K(1 + p_1 + \cdots + p_k) = 1$ and so $K \neq 0$. (Note that in fact $K = 1/p(1)$.) This completes the proof of **Claim 2**.

Now (4) is periodic with least period $e = \text{ord}(p(x))$ by [1, 6.28]. Thus (3) is also periodic with least period e, by **Claim 2**. For $b \in GF(q)$ let $Z_\eta(b)$ be the number of occurrences of b in one period of (4). Define $Z_\epsilon(b)$ similarly. Note that $Z_\epsilon(0) = Z_\eta(-K)$.

Let $h = m/e$. Then h full periods give $\epsilon_1, \epsilon_2, \ldots \epsilon_m$. But we are only concerned with the coefficients of $g(x)$, namely, $\epsilon_1, \epsilon_2, \ldots, \epsilon_{m-k}$. We need to verify:

Claim 3. $\epsilon_{m-k+1} = \epsilon_{m-k+2} = \cdots = \epsilon_m = 0$.

From (2) we have

$$\epsilon_{m-k+1} = -p_1\epsilon_{m-k} - \cdots - p_k\epsilon_{m-2k+1} + 1.$$

Matching coefficients of x^{k-1} in $p(x)g(x) = x^{m-1} + \cdots + x + 1$ gives

$$p_1\epsilon_{m-k} + \cdots + p_k\epsilon_{m-2k+1} = 1.$$

Hence $\epsilon_{m-k+1} = 0$.

Again, from (2) we have

$$\begin{aligned}\epsilon_{m-k+2} &= -p_1\epsilon_{m-k+1} - \cdots - p_k\epsilon_{m-2k+2} + 1\\ &= -p_2\epsilon_{m-k} - \cdots - p_k\epsilon_{m-2k+2} + 1,\end{aligned}$$

since $\epsilon_{m-k+1} = 0$. Matching coefficients of x^{k-2} gives

$$p_2\epsilon_{m-k} + \cdots + p_k\epsilon_{m-2k+2} = 1.$$

Thus $\epsilon_{m-k+2} = 0$. Finish by induction.

First suppose $p(x)$ is primitive. By [1, p. 244]

$$Z_\eta(b) = \begin{cases} q^{k-1}, & \text{if } b \neq 0\\ q^{k-1} - 1, & \text{if } b = 0.\end{cases}$$

Then by **Claim 2**

$$Z_\epsilon(b) = \begin{cases} q^{k-1}, & \text{if } b \neq K\\ q^{k-1} - 1, & \text{if } b = K.\end{cases}$$

Since $K \neq 0$, we have $Z_\epsilon(0) = q^{k-1}$. Then the number of non-zero coefficients of $g(x)$ is, by **Claim 3**,

$$q^k - 1 - q^{k-1} = (q-1)q^{k-1} - 1.$$

Now suppose $p(x)$ is not primitive (so that $h > 1$). The number of zero terms among $\epsilon_1, \ldots, \epsilon_m$ is $hZ_\epsilon(0)$. The number of zero terms among $\epsilon_1, \ldots, \epsilon_{m-k}$ is $hZ_\epsilon(0) - k$ by **Claim 3**. Hence the number of non-zero terms in $g(x)$ (of degree $m-1-k$) is:

$$q^k - 1 - k - (hZ_\epsilon(0) - k) = q^k - 1 - hZ_\epsilon(0).$$

Suppose, by way of contradiction, that the number of non-zero terms of $g(x)$ is $(q-1)q^{k-1} - 1$. Then we have $hZ_\epsilon(0) = q^{k-1}$. But q is a power of some prime p and so h (recall $h > 1$) is also a power of p. But $he = m = q^k - 1$, a contradiction. Thus the number of non-zero terms of $g(x)$ is not $(q-1)q^{k-1} - 1$. □

2. Application to BCH codes.

We will only be concerned with primitive, narrow -sense BCH codes over $GF(2)$. Call a code $\mathcal{C}$ *trivial* if it consists only of the zero vector and the vector of all 1's. We are interested in the non-trivial BCH codes of maximal designed distance. The following is well-known.

Proposition. *Set $m = 2^k - 1$. Let $\mathcal{C} \subset GF(2^k)$ be a BCH code of designed distance δ. If $\delta \geq 2^{k-1}$ then $\mathcal{C}$ is trivial. If $\delta = 2^{k-1} - 1$ then:*

1. $\dim \mathcal{C} = k + 1$.
2. *The true minimal distance of $\mathcal{C}$ is δ.*
3. *The check polynomial $h(x)$ of $\mathcal{C}$ is $(x-1)p(x)$, where $p(x)$ is a primitive polynomial of degree k.*

Proof. Let α be a primitive element of $\mathbb{F}_{2^k}$. Let $g(x)$ be the generating polynomial. Then $\dim \mathcal{C} = m - \deg g(x)$ and $\deg g(x)$ is the number of i, $1 \leq i \leq m$, with some cyclic permutation of its binary expansion $\leq \delta - 1$ [2, Theorem 9 of 9.3]. For $\delta = 2^{k-1}$, the binary expansion of $\delta - 1$ is $011\ldots11$. Hence every i, except $i = m$ has a permutation less than or equal to $\delta - 1$. So $\deg g(x) = m - 1$ and $\dim \mathcal{C} = 1$. Hence $\mathcal{C}$ is trivial. For $\delta = 2^{k-1} - 1$, the binary expansion of $\delta - 1$ is $0111\ldots110$. Then the binary expansion of i has a permutation $\leq \delta - 1$ iff the expansion contains $\leq k-2$ ones. Thus $\deg g(x) = m-k-1$ and $\dim \mathcal{C} = k + 1$. This proves (1). (2) follows from [2, Theorem 5 of 9.2].

To prove (3), first note that 1 is not a root of $g(x)$ hence $h(x) = (x-1)p(x)$, for some polynomial $p(x)$ of degree k by (1). Now $(\delta, m) = 1$ so that α^δ is primitive. We check that α^δ is not a root of $g(x)$. If it were then $\delta \equiv j2^i \pmod{m}$ for some $1 \leq i < k$ and some odd j, $1 \leq j \leq \delta - 2$. So

$$j \equiv 2^{k-i}\delta \equiv 2^{k-i-1} - 2^{k-i} = -2^{k-i-1} \pmod{m}.$$

Then $j + 2^{k-i-1} = 2^k - 1$ and $j \geq 2^{k-1}$, which is impossible. $\square$

Our Theorem gives slightly more information. This was the motivation for (1.1).

Corollary. *Set $m = 2^k - 1$. Let $\mathcal{C} \subset GF(2^k)$ be a BCH code of designed distance $2^{k-1} - 1$. Then the generating polynomial $g(x)$ has weight $2^{k-1} - 1$, the minimal weight of $\mathcal{C}$.*

Proof. We have $g(x) = (x^m - 1)/h(x)$ and, by (3) of the proposition, $h(x) = (x-1)p(x)$, where $p(x)$ is primitive of degree k. Hence, by the Theorem, $g(x)$ has weight $2^{k-1} - 1$. $\square$

References

1. R. Lidl and H. Niederreitter, *Introduction to Finite Fields and Their Applications*, Revised edition, Cambridge University Press, Cambridge, 1994.
2. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland Mathematics Library, Vol. 16, North-Holland, Amsterdam, 1977.

Carbondale, IL 62901
E-mail address: rfitzg@math.siu.edu