CHAPTER III

A MODIFICATION OF FITZGERALD'S CHARACTERIZATION

Fitzgerald [12] proved that an irreducible polynomial

$$P(x) = p_k + p_{k-1}x + \cdots + p_0x^k \in \mathbb{F}_q[x]$$

of degree $k \geq 1$ is primitive if and only if $g(x) := (x^{q^k-1} - 1)/(x - 1)P(x)$ has exactly $q^{k-1}(q-1) - 1$ non-zero terms. Fitzgerald's result is interesting in both its statement and proof. The proof starts by equating and cleverly rearranging the coefficients in $g(x)P(x) = (x^{q^k-1} - 1)/(x - 1)$. This leads to a linear recurring sequence over a finite field and the result follows by suitably appealing to the known results about the number of occurrences of elements in such a sequence.

3.1 Main result and proof

We modify Fitzgerald's technique by noting that the number of coefficients in $g(x)$ can be considerably reduced, at least for large q, by replacing the factor $x-1$ with $x^{q-1}-1$, which is the product of all monic linear polynomials, excluding x, over $\mathbb{F}_q$ and clearly divides $x^{q^k-1} - 1$. Yet the new quotient now has an extra non-polynomial term, which reveals its more general structure. Analyzing this structure enables us to deal with the arising additional difficulties. Our main theorem reads:

Theorem 3.1.1. *Let* $P(x) = p_k + p_{k-1}x + \cdots + p_0x^k \in \mathbb{F}_q[x]$ *be irreducible over* $\mathbb{F}_q$ *and of degree* $k \geq 2$. *Let* $m = q^k - 1$, $t = \frac{m}{q-1}$, $y = x^{q-1}$ *and*

$$G(y) = \frac{y^t - 1}{(y-1)P(y)} = H(y) + \frac{r_0 + r_1y + \cdots + r_{k-1}y^{k-1}}{P(y)},$$

where $H(y) = \varepsilon_{t-k} + \varepsilon_{t-k-1}y + \cdots + \varepsilon_1 y^{t-k-1} \in \mathbb{F}_q[y]$. *Then* $P(x)$ *is primitive over* $\mathbb{F}_q$ *if and only if the number of non-zero terms in* $H(y)$, *considered as polynomial in* y *over* $\mathbb{F}_q$, *is equal to* $q^{k-1}(q-1) - 1 - N$, *where* N *is the number of non-zero terms in the finite sequence* $\varepsilon_{t-k+1}, \varepsilon_{t-k+2}, \ldots, \varepsilon_{m-1}, \varepsilon_m$ *which is defined by*

$$\varepsilon_{t-n} = r_n - \sum_{i=1}^{k-n-1} p_i\varepsilon_{t-n-i} \quad (n = 0, 1, \ldots, k-1)$$

where empty sum is interpreted as 0, *and*

$$\varepsilon_{t+n} = 1 - \sum_{i=1}^{k} p_i\varepsilon_{t+n-i} \quad (n = 1, 2, \ldots, m-t).$$

Proof. Equating the coefficients of y^{t-l} in

$$y^{t-1} + y^{t-2} + \cdots + 1 = \left(p_k + p_{k-1}y + \cdots + p_0y^k\right)\left(\varepsilon_{t-k} + \varepsilon_{t-k-1}y + \cdots + \varepsilon_1 y^{t-k-1}\right) + \left(r_0 + r_1y + \cdots + r_{k-1}y^{k-1}\right),$$

$$\begin{aligned}
y^{t-1} &\;;\; p_0\varepsilon_1 = 1,\\
y^{t-2} &\;;\; p_1\varepsilon_1 + p_0\varepsilon_2 = 1,\\
&\vdots\\
y^{t-k} &\;;\; p_{k-1}\varepsilon_1 + p_{k-2}\varepsilon_2 + p_{k-3}\varepsilon_3 + \cdots + p_0\varepsilon_k = 1,\\
y^{t-(k+1)} &\;;\; p_k\varepsilon_1 + p_{k-1}\varepsilon_2 + p_{k-2}\varepsilon_3 + \cdots + p_0\varepsilon_{k+1} = 1,\\
&\vdots\\
y^{t-l} &\;;\; p_k\varepsilon_{l-k} + p_{k-1}\varepsilon_{l-k+1} + p_{k-2}\varepsilon_{l-k+2} + \cdots + p_0\varepsilon_l = 1,\\
&\vdots
\end{aligned}$$

$$
\begin{aligned}
y^k = y^{t-(t-k)} \quad &; \quad p_k\varepsilon_{t-2k} + p_{k-1}\varepsilon_{t-2k+1} + p_{k-2}\varepsilon_{t-2k+2} + \cdots + p_0\varepsilon_{t-k} = 1, \\
y^{k-1} = y^{t-(t-k+1)} \quad &; \quad (p_k\varepsilon_{t-2k+1} + p_{k-1}\varepsilon_{t-2k+2} + p_{k-2}\varepsilon_{t-2k+3} + \cdots + p_1\varepsilon_{t-k}) + r_{k-1} = 1, \\
&\vdots \\
y^{t-l} \quad &; \quad (p_k\varepsilon_{l-k} + p_{k-1}\varepsilon_{l-k+1} + p_{k-2}\varepsilon_{l-k+2} + \cdots + p_{l-t+k}\varepsilon_{t-k}) + r_{t-l} = 1, \\
&\vdots \\
y^1 = y^{t-(t-k+(k-1))} \quad &; \quad (p_k\varepsilon_{t-k-1} + p_{k-1}\varepsilon_{t-k}) + r_1 = 1, \\
y^0 = y^{t-(t-k+k)} \quad &; \quad p_k\varepsilon_{t-k} + r_0 = 1.
\end{aligned}
$$

In general, we get

$$\sum_{i+j=l} p_i\varepsilon_j = 1 \quad (l = 1, 2, \ldots, t-k) \tag{3.1.1}$$

and

$$\sum_{i+j=l} p_i\varepsilon_j + r_{t-l} = 1 \quad (l = t-k+1, t-k+2, \ldots, t). \tag{3.1.2}$$

We can, without loss of generality, choose $p_0 = 1$. The strategy now is to think of the two finite sequences $\{p_0 = 1, \ldots, p_k\}$ and $\{r_0, \ldots, r_{k-1}\}$ as given fixed and extend the finite sequence $\{\varepsilon_1, \ldots, \varepsilon_{t-k}\}$ to an infinite linear recurring sequence satisfying (3.1.1) and (3.1.2). Note first that (3.1.1) uniquely determines the values of $\varepsilon_1, \ldots, \varepsilon_{t-k}$. Rewriting (3.1.1) and using it to define further values of ε_i $(i > t-k)$, we get

$$\varepsilon_{n+k} = -\sum_{i=1}^{k} p_i\varepsilon_{n+k-i} + 1 \quad (n \geq 1). \tag{3.1.3}$$

We view (3.1.3) as an (infinite) linear recurring sequence whose initial values $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{t-k}$ are, as mentioned above, computed from (3.1.1). Taking the difference of two consecutive terms, we get a homogeneous recurrence (of order k)

$$\varepsilon_{n+k+1} - \varepsilon_{n+k} = -p_1\varepsilon_{n+k} + \sum_{i=1}^{k-1}(p_i - p_{i+1})\varepsilon_{n+k-i} + p_k\varepsilon_n,$$

i.e.

$$\varepsilon_{n+k+1} = (1-p_1)\varepsilon_{n+k} + \sum_{i=1}^{k-1}(p_i - p_{i+1})\varepsilon_{n+k-i} + p_k\varepsilon_n. \tag{3.1.4}$$

We claim that the characteristic polynomial, $f(y)$, of the homogeneous sequence (3.1.4) is $(y-1)P(y)$. This follows immediately from

$$\begin{aligned} f(y) &= y^{k+1} - (1-p_1)y^k - (p_1-p_2)y^{k-1} - \cdots - (p_{k-1}-p_k)y - p_k \\ &= (y-1)P(y). \end{aligned}$$

Now consider a homogeneous linear recurring sequence, of order $k-1$, with characteristic polynomial $P(y)$,

$$\eta_{n+k} = -p_1\eta_{n+k-1} - p_2\eta_{n+k-2} - \cdots - p_k\eta_n \tag{3.1.5}$$

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

We next claim that there is a non-zero L and a choice of $\eta_1, \eta_2, \ldots, \eta_k$ in $\mathbb{F}_q$ such that $\varepsilon_i = \eta_i + L$ holds for all $i \geq 1$. To verify this claim, we recall some basic results. For a monic polynomial of positive degree $f(x) \in \mathbb{F}_q[x]$, let $S(f(x))$ denote the vector space (over $\mathbb{F}_q$) of all homogeneous linear recurring sequences in $\mathbb{F}_q$ with characteristic polynomial $f(x)$. Since $P(y)$ is a non-constant monic, irreducible polynomial of degree ≥ 2, from Theorem 2.1.17, it is well-known that

$$S\big(P(y)\big) + S(y-1) = S\big((y-1)P(y)\big).$$

Further, a sequence is in $S(y-1)$ if and only if $s_{n+1} = s_n$ for all n, i.e., if and only if it is a constant sequence. Let this sequence be $s_n = L$ for all n. Since the sequence (3.1.5) is in $S\big(P(y)\big)$, and the sequence (3.1.4) is in $S\big((y-1)P(y)\big)$ by the earlier claim, there is a choice of $\eta_1, \eta_2, \ldots, \eta_k$ in $\mathbb{F}_q$, with $(\eta_n) \in S(P(y))$, for which

$$(\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots) = (\eta_1, \eta_2, \eta_3, \ldots) + (s_1, s_2, s_3, \ldots) = (\eta_1 + L, \eta_2 + L, \eta_3 + L, \ldots),$$

and the claim is verified. Next, we show that $L \neq 0$. Substituting the values of η_n into (3.1.5), we get

$$\varepsilon_{k+1} - L = -p_1(\varepsilon_k - L) - \cdots - p_k(\varepsilon_1 - L) = L(p_1 + \cdots + p_k) - \sum_{i=1}^{k} p_i\varepsilon_{1+k-i},$$

and using (3.1.3), we deduce

$$\varepsilon_{k+1} = L(1 + p_1 + p_2 + \cdots + p_k) + \varepsilon_{k+1} - 1,$$

implying that $L \neq 0$.

We now return to ensure that the extended (infinite) sequence $\{\varepsilon_i\}$ so constructed as in (3.1.3), using (3.1.1), satisfies (3.1.2). Putting $n = t - 2k + 1$ in (3.1.3) and matching it with (3.1.2), we must take

$$\varepsilon_{t-k+1} = -p_1\varepsilon_{t-k} - p_2\varepsilon_{t-k-1} - \cdots - p_k\varepsilon_{t-2k+1} + 1 = r_{k-1}.$$

Putting $n = t - 2k + 2$ and matching it with (3.1.2), we must take

$$\varepsilon_{t-k+2} = -p_1\varepsilon_{t-k+1} - p_2\varepsilon_{t-k} - \cdots - p_k\varepsilon_{t-2k+2} + 1 = r_{k-2} - p_1\varepsilon_{t-k+1}.$$

In general, we must take

$$\varepsilon_{t-m} = r_m - \sum_{i=1}^{k-m-1} p_i\varepsilon_{t-m-i} \quad (m = 0, 1, \ldots, k-1).$$

Since the characteristic polynomial of (3.1.5), $P(y)$, is irreducible over $\mathbb{F}_q$ and $P(0) \neq 0$, the sequence $\{\eta_i\}$ is periodic with least period $e = ord\ (P)$, from Theorem 2.1.13, and so the sequence $\varepsilon_i = \eta_i + L$, in (3.1.4), is also periodic with the same least period e.

For $b \in \mathbb{F}_q$, let $Z_\eta(b)$ be the number of occurrences of b in one least period of the sequence (3.1.5), and define $Z_\varepsilon(b)$ similarly. Since $-L = \eta_i - \varepsilon_i$ for all $i \geq 1$, then $Z_\varepsilon(0) = Z_\eta(-L)$. Since $P(y)$ is irreducible over $\mathbb{F}_q$ with degree k, by Theorem 2.1.14, $e = ord(P) \mid (q^k - 1) = m$. Now $(\varepsilon_1, \varepsilon_2, \ldots)$ being periodic with least period e, shows that the finite set $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ covers $h = m/e$ full periods. The fact, Theorem 2.1.6, that the irreducible polynomial $P(y)$ considered here is primitive if and only if $e = ord(P) = q^k - 1$ is then equivalent to $P(y)$ is primitive if and only if $h = 1$.

Assume that $P(y)$ is primitive, i.e. $h = 1$. Clearly, we may choose the initial values $\eta_1, \eta_2, \ldots, \eta_k$ not all zero. Since $(\eta_1, \eta_2, \ldots)$ is a homogeneous linear recurring sequence in $\mathbb{F}_q$ with primitive characteristic polynomial $P(y)$ and non-zero initial values, it is a maximal period sequence in $\mathbb{F}_q$, by Definition 2.1.15. By a well-known result, Definition 2.1.18,

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

Using $\varepsilon_i - L = \eta_i$, we consequently get

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

Since $L \neq 0$, we have $Z_\varepsilon(0) = q^{k-1}$, and so the number of zero terms among $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ is $hZ_\varepsilon(0) = Z_\varepsilon(0) = q^{k-1}$. Thus the number of non-zero terms among $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ is $m - q^{k-1} = q^{k-1}(q-1) - 1$. Consequently, the number of non-zero terms in $H(y)$ is equal to $q^{k-1}(q-1) - 1 - N$.

On the other hand, suppose that the number of non-zero terms in $H(y)$ is $q^{k-1}(q-1) - 1 - N$ but $P(x)$ is not primitive over $\mathbb{F}_q$. Then $h \geq 2$ and

$$\begin{aligned} m - hZ_\varepsilon(0) &= \text{the number of non-zero terms among } \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \\ &= \text{the number of non-zero terms among } \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{t-k} \\ &\quad + \text{the number of non-zero terms among } \varepsilon_{t-k+1}, \varepsilon_{t-k+2}, \ldots, \varepsilon_m \\ &= \text{the number of non-zero terms of } H(y) + N \\ &= q^{k-1}(q-1) - 1, \end{aligned}$$

which implies $hZ_\varepsilon(0) = q^{k-1}$. But $he = m = q^k - 1$, which is a contradiction and the theorem is proved. □

Immediate from the proof of the theorem is another, perhaps simpler, characterization.

Corollary 3.1.2. *An irreducible polynomial* $P(x) = p_k + p_{k-1}x + \cdots + p_1 x^{k-1} + x^k \in \mathbb{F}_q[x]$ *is primitive if and only if the finite sequence* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$, *so defined as in the theorem, contains no two (identical) periodic subsequences.*

We end this section with two further remarks.

1. Both the starting expressions $g(x) = \frac{x^{q^k-1}-1}{(x-1)P(x)}$ in Fitzegerald's theorem and $\frac{y^t-1}{(y-1)P(y)} = G(y) = G(x^{q-1}) = \frac{(x^{q-1})^t-1}{(x^{q-1}-1)P(x^{q-1})}$ in our theorem have the same numerator. Yet, the denominator of $G(x^{q-1})$ is of higher degree, so the number of terms to be counted in $G(x^{q-1})$ is fewer than that in $g(x)$.

2. Although in our theorem, we additionally have to determine the number of non-zero terms, N, in the finite sequence $\varepsilon_{t-k+1}, \varepsilon_{t-k+2}, \ldots, \varepsilon_m$, this is generally not difficult because of their explicitly given form.

3.2 Examples

We give in this section a few examples in order to compare the number of coefficients involved in our main theorem with that of Fitzgerald.

Example 3.2.1. Take $q = k = 3$ and $P(x) = x^3 + 2x + 1$, which is irreducible over $\mathbb{F}_q$. Here $m = 26, t = 13, p_0 = 1, p_1 = 0, p_2 = 2, p_3 = 1$.

Using Fitzgerald's result, we compute

$$\begin{aligned} g(x) &= \frac{x^{q^k-1} - 1}{(x-1)P(x)} \\ &= x^{22} + x^{21} + 2x^{20} + x^{19} + 2x^{18} + 2x^{16} + 2x^{15} + x^{13} + 2x^{12} + 2x^{11} + 2x^{10} \\ &\quad + x^9 + x^8 + x^6 + 2x^4 + 2x + 1, \end{aligned}$$

which has $q^{k-1}(q-1) - 1 = 17$ non-zero terms, and so $P(x)$ is primitive over $\mathbb{F}_q$.

On the other hand, using our theorem, we compute

$$G(x^2) = G(y) = \frac{y^{13}-1}{(y-1)(y^3+2y+1)}$$
$$= y^9 + y^8 + 2y^7 + y^6 + 2y^5 + 2y^3 + 2y^2 + 1 + \frac{2y^2 - y}{y^3 + 2y + 1}.$$

Here $H(y) = y^9 + y^8 + 2y^7 + y^6 + 2y^5 + 2y^3 + 2y^2 + 1$ has 8 non-zero terms. Next we determine the finite sequence

$$\varepsilon_{t-k+1} = \varepsilon_{11} = 2, \quad \varepsilon_{t-k+2} = \varepsilon_{12} = 2, \quad \varepsilon_{13} = 2, \quad \varepsilon_{14} = 1, \quad \varepsilon_{15} = 1, \quad \varepsilon_{16} = 0,$$
$$\varepsilon_{17} = 1, \quad \varepsilon_{18} = 0, \quad \varepsilon_{19} = 2, \quad \varepsilon_{20} = 0, \quad \varepsilon_{21} = 0, \quad \varepsilon_{22} = 2, \quad \varepsilon_{23} = 1, \quad \varepsilon_{24} = 0,$$
$$\varepsilon_{25} = 0, \quad \varepsilon_m = \varepsilon_{26} = 0,$$

and so $N = 9$. The number of non-zero terms in $H(y)$ is then equal to $q^{k-1}(q-1) - 1 - N = 18 - 1 - 9 = 8$, showing that $P(x)$ is primitive over $\mathbb{F}_q$.

Example 3.2.2. Take $q = 5, k = 2$ and $P(x) = x^2 + 3x + 3$, which is irreducible over $\mathbb{F}_q$. Here $m = 24, t = 6, p_0 = 1, p_1 = 3, p_2 = 3$.

Using Fitzgerald's result, we compute

$$g(x) = \frac{x^{q^k-1} - 1}{(x-1)P(x)}$$
$$= x^{21} + 3x^{20} + 4x^{19} + 4x^{17} + 4x^{16} + 2x^{15} + 3x^{14} + x^{13} + 4x^{12} + x^{11} + x^{10}$$
$$+ 3x^8 + 2x^7 + x^6 + 2x^5 + 2x^4 + 4x^3 + 3x^2 + 2,$$

which has $q^{k-1}(q-1) - 1 = 19$ non-zero terms, and so $P(x)$ is primitive over $\mathbb{F}_q$.

Using our result, we compute

$$G(x^4) = G(y) = \frac{y^6 - 1}{(y-1)(y^2+3y+3)} = y^3 + 3y^2 + 4y + \frac{4y+1}{y^2+3y+3}.$$

Here $H(y) = y^3 + 3y^2 + 4y$ has 3 non-zero terms. We now determine

$$\varepsilon_{t-k+1} = \varepsilon_5 = 4, \quad \varepsilon_{t-k+2} = \varepsilon_6 = 4, \quad \varepsilon_7 = 2, \quad \varepsilon_8 = 3, \quad \varepsilon_9 = 1, \quad \varepsilon_{10} = 4, \quad \varepsilon_{11} = 1,$$
$$\varepsilon_{12} = 1, \quad \varepsilon_{13} = 0, \quad \varepsilon_{14} = 3, \quad \varepsilon_{15} = 2, \quad \varepsilon_{16} = 1, \quad \varepsilon_{17} = 2, \quad \varepsilon_{18} = 2, \quad \varepsilon_{19} = 4,$$
$$\varepsilon_{20} = 3, \quad \varepsilon_{21} = 0, \quad \varepsilon_{22} = 2, \quad \varepsilon_{23} = 0, \quad \varepsilon_m = \varepsilon_{24} = 0,$$

and so $N = 16$. The number of non-zero terms in $H(y)$ is equal to $q^{k-1}(q-1) - 1 - N = 20 - 1 - 16 = 3$, showing that $P(x)$ is primitive over $\mathbb{F}_q$.

Example 3.2.3. Take $q = 7, k = 2$ and $P(x) = x^2 + x + 6$, which is irreducible over $\mathbb{F}_q$. Here $m = 48, t = 8, p_0 = 1, p_1 = 1, p_2 = 6$.

Using Fitzgerald's result, we compute

$$\begin{aligned} g(x) &= \frac{x^{q^k-1} - 1}{(x-1)P(x)} \\ &= x^{45} + 2x^{43} + 6x^{42} + 4x^{41} + 3x^{40} + 2x^{39} + 2x^{38} + x^{37} + 2x^{36} + 3x^{34} + 5x^{33} \\ &\quad + 6x^{32} + x^{29} + 2x^{27} + 6x^{26} + 4x^{25} + 3x^{24} + 2x^{23} + 2x^{22} + x^{21} + 2x^{20} + 3x^{18} \\ &\quad + 5x^{17} + 6x^{16} + x^{13} + 2x^{11} + 6x^{10} + 4x^9 + 3x^8 + 2x^7 + 2x^6 + x^5 + 2x^4 \\ &\quad + 3x^2 + 5x + 6, \end{aligned}$$

which has 36 non-zero terms and $36 \neq 41 = q^{k-1}(q-1) - 1$, and so $P(x)$ is not primitive over $\mathbb{F}_q$. Using our result, we compute

$$G(x^6) = G(y) = \frac{y^8 - 1}{(y-1)(y^2 + y + 6)} = y^5 + 2y^3 + 6y^2 + 4y + 3 + \frac{2y+4}{y^2+y+6}.$$

Here $H(y) = y^5 + 2y^3 + 6y^2 + 4y + 3$ has 5 non-zero terms. We now determine

$$\begin{aligned} &\varepsilon_1 = 1, \ \varepsilon_2 = 0, \ \varepsilon_3 = 2, \ \varepsilon_4 = 6, \ \varepsilon_5 = 4, \ \varepsilon_6 = 3, \ \varepsilon_7 = 2, \ \varepsilon_8 = 2, \\ &\varepsilon_9 = 1, \ \varepsilon_{10} = 2, \ \varepsilon_{11} = 0, \ \varepsilon_{12} = 3, \ \varepsilon_{13} = 5, \ \varepsilon_{14} = 6, \ \varepsilon_{15} = 0, \ \varepsilon_{16} = 0, \\ &\varepsilon_{17} = 1, \ \varepsilon_{18} = 0, \ \varepsilon_{19} = 2, \ \varepsilon_{20} = 6, \ \varepsilon_{21} = 4, \ \varepsilon_{22} = 3, \ \varepsilon_{23} = 2, \ \varepsilon_{24} = 2, \\ &\varepsilon_{25} = 1, \ \varepsilon_{26} = 2, \ \varepsilon_{27} = 0, \ \varepsilon_{28} = 3, \ \varepsilon_{29} = 5, \ \varepsilon_{30} = 6, \ \varepsilon_{31} = 0, \ \varepsilon_{32} = 0, \\ &\varepsilon_{33} = 1, \ \varepsilon_{34} = 0, \ \varepsilon_{35} = 2, \ \varepsilon_{36} = 6, \ \varepsilon_{37} = 4, \ \varepsilon_{38} = 3, \ \varepsilon_{39} = 2, \ \varepsilon_{40} = 2, \\ &\varepsilon_{41} = 1, \varepsilon_{42} = 2, \ \varepsilon_{43} = 0, \ \varepsilon_{44} = 3, \ \varepsilon_{45} = 5, \ \varepsilon_{46} = 6, \ \varepsilon_{47} = 0, \ \varepsilon_{48} = 0, \end{aligned}$$

and so $N = 31$. The number of non-zero terms in $H(y)$ is not equal to $q^{k-1}(q-1) - 1 - N = 42 - 1 - 31 = 10$, showing that $P(x)$ is not primitive over $\mathbb{F}_q$. Alternatively, we note that the finite sequence $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ contains three identical subsequences $\{1, 0, 2, 6, 4, 3, 2, 2, 1, 2, 0, 3, 5, 6, 0, 0\}$ and so by the corollary, $P(x)$ is not primitive.