SovietRxiv

Soviet-era science, translated into English

CYBERNETICS AND CONTROL THEORY

R. R. VARSHAMOV

1964

SovietRxiv

View the original and related papers at https://sovietrxiv.org/items/ru-196401.57505

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.

SovietRxiv

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

R. R. VARSHAMOV

ON A THEOREM FROM THE THEORY OF REDUCIBILITY OF POLYNOMIALS

(Presented by Academician V. S. Kulebakin, 5 X 1963)

The theory of reducibility of polynomials modulo a prime, which is of considerable interest in itself, occupies a special place in the modern theory of linear coding ([1]). One of its important and at the same time most difficult problems is the problem of synthesizing irreducible polynomials of a given degree. The present note is devoted to this direction. All polynomials considered below are assumed to have coefficients in the Galois field $GF(q)$. Denote by $L^p f(x)$ the expression

$$F(x) = p(x)^{-1} \sum_{v=0}^{n} \sum_{u=0}^{m} a_v b_u x^{uq^v}, \tag{1}$$

where

$$f(x) = \sum_{v=0}^{n} a_v x^v, \quad p(x) = \sum_{u=0}^{m} b_u x^u \quad (p(x) \neq \text{const}).$$

Lemma. The polynomial $L^p r(x)$ divides $L^p f(x)$ without remainder, where $r(x)$ is any divisor of $f(x)$.*

Proof. Substituting into (1) $f(x) = r(x)h(x)$, where

$$r(x) = \sum_{v=0}^{R} r_v x^v \quad \text{and} \quad h(x) = \sum_{j=0}^{H} h_j x^j,$$

we obtain

$$L^p f(x) = p(x)^{-1} \sum_{j=0}^{H} \sum_{v=0}^{R} \sum_{u=0}^{m} h_j r_v b_u x^{uq^{v+j}} =$$

$$= \sum_{j=1}^{H} h_j p(x)^{-1} \left(\sum_{u=0}^{m} b_u x^u \right)^{q^j} \left(L^p r(x)\right)^{q^j} = \sum_{j=0}^{H} h_j \left(L^p x^j\right) \left(L^p r(x)\right)^{q^j}, \tag{2}$$

SovietRxiv

i.e. $L^p r(x) \mid L^p f(x)$. The lemma is proved.

Main theorem. Let

$$f(x) = \sum_{v=0}^{n} a_v x^v \quad (a_0 \neq 0);$$

$s_1(x), \ldots, s_k(x)$ be the set of all proper divisors of $f(x)$; $K_f[L^p f(x)]$ be the least common multiple of $L^p s_1(x), \ldots, L^p s_k(x)$; N be the exponent of the polynomial $f(x)$,** and $g(x) \neq$ const an irreducible factor of (1) not dividing $K_f[L^p f(x)]$.

Then c, the degree of the polynomial $g(x)$, is a multiple of N, i.e. $(c, N) = N$.

Proof. Suppose the contrary, i.e. $(c, N) \neq N$ $(c \geq 1)$. Then, obviously, the expression $s(x) = (x^c - 1, f(x))$ is a proper divisor of $f(x)$, and, by the lemma,

$$L^p s(x) = \Lambda_1(x) L^p(x^c - 1) + \Lambda_2(x) F(x), \tag{3}$$

since

$$s(x) = \lambda_1(x)(x^c - 1) + \lambda_2(x) f(x).$$

By definition,

$$p(x) L^p(x^c - 1) = \sum_{u=0}^{m} b_u \left(x^{uq^c} - x^u\right),$$

which shows that

---

* In fact, a stronger assertion holds:

$$\left(L^p f_1(x),\ L^p f_2(x)\right) = L^p\left(f_1(x),\ f_2(x)\right).$$

** That is, the least natural number satisfying $x^N \equiv 1 \pmod{f(x)}$.

$x^{c-1} - 1 / p(x) L^p(x^c - 1) L^p(x^c - 1)$ and, simultaneously, $g(x) / p(x) L^p(x_c - 1)$, since the degree of the irreducible polynomial $g(x)$ is equal to c. Let us note, however, that $(g(x), p(x)) =$ const in view of $(p(x) L^p f(x))' = a_0 p'(x)$ $(a_0 \neq 0)$. Therefore it is clear that $g(x) / L^p(x^c - 1)$, and also, by (3), $g(x) / L^p s(x)$. This contradicts the condition of the theorem. Thus our assumption is false; consequently, $(c, N) = N$. The theorem is proved.

The main theorem has an application in the constructive theory of the synthesis of irreducible polynomials of a given degree modulo a prime. We shall set out some separate results obtained with its aid.

SovietRxiv

Theorem 1. Let

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu \quad (a_0 \neq 0), \qquad p(x) = x.$$

Then c, the degree of the irreducible polynomial $g(x)$ satisfying the conditions of the main theorem, coincides with the exponent of $f(x)$, i.e. $c = N$.

Proof. Since $f(x)/x^N - 1$, it follows, according to the lemma, that $F(x)/L^x(x^N - 1)$ and $g(x)/x^{q^N-1} - 1$, since $L^x(x^N - 1) = x^{q^N-1} - 1$. The polynomial $g(x)$ is irreducible; therefore c/N, and this, together with the main theorem, gives $c = N$. The theorem is proved.

As a consequence of Theorem 1 we obtain some previously known results of Yore, Carlitz, Gleason, and Marsh (see, for example, ([2])) for the cases when the polynomial $f(x)$ is irreducible or when $f(x)$ is a primitive polynomial. Thus, for example, in the field $GF(3)$ the expression $L^x(x^2 + x + 2) = x^8 + x^2 + 2$ is irreducible, since $x^2 + x + 2$ is a primitive polynomial. In addition, for $q = 2^*$ we have:

Theorem 2. Let

$$f(x) = \prod_{i=1}^{\sigma} f_i(x),$$

where $f_i(x)$ $(i = 1, \dots, \sigma)$ are primitive polynomials with pairwise relatively prime degrees n_i, respectively,

$$|\alpha| = \sum_{i=1}^{\sigma} \alpha_i,$$

where α_i are integers $(0 \leq \alpha_i \leq 1)$, and

$$f^{(\alpha)}(x) = \prod_{i=1}^{\sigma} f_i^{\alpha_i}(x).$$

Then the polynomial

$$F_1(x) = \prod_{j=0}^{[\sigma/2]} \left(\prod_{|\alpha|=\sigma-2j-1} L^x f^{(\alpha)}(x) \right)^{-1} \left(\prod_{|\alpha|=\sigma-2j} L^x f^{(\alpha)}(x) \right)$$

is irreducible.

Proof. It is easy to show that the polynomial $F_1(x)$, being a divisor of $L^x f(x)$, is relatively prime to $K_f[L^x f(x)]$. Moreover, a simple calculation establishes that its degree is

$$M_{n_1,\ldots,n_\sigma} = \prod_{i=1}^{\sigma}(2^{n_i}-1).$$

As is known, the exponent of the polynomial $f(x)$ also coincides with $M_{n_1,\ldots,n_\sigma}$. Hence, according to Theorem 1, it follows that the polynomial $F_1(x)$ is irreducible. The theorem is proved.

Theorem 2 makes it comparatively easy to find irreducible polynomials whose degrees are representable in the form of a product of pairwise relatively prime Mersenne numbers. Thus, for example, in the case when $f(x) = (x^2+x+1)(x^3+x^2+1) = x^5+x+1$, we shall have the irreducible polynomial of degree 21

$$F_1'(x) = \frac{L^x(x^5+x+1)}{L^x(x^2+x+1)L^x(x^3+x^2+1)} =$$

$$= x^{21}+x^{19}+x^{18}+x^{15}+x^{14}+x^{11}+x^8+x^7+x^5+x^4+1.$$

---

* The case most interesting in practical applications. In what follows, we have $q = 2$.

In an analogous way, in the case $f(x) = (x^2+x+1)(x^5+x^2+1)$ we obtain the irreducible polynomial of degree 93

$$F_1(x) = (x^7+1)^3(x^4+x^2+x+1)(x^{68}+x^{37}+x^{12}+x^9+x^6+x^4)+1.$$

Theorem 3. Let

$$f(x) = \sum_{v=0}^{n} a_v x^v, \qquad \omega(x) = \sum_{u=0}^{\Omega} \omega_u x^u,$$

$$\sigma(\omega) = f(1) + xL^x\omega(x), \qquad \Lambda(x) = (x+f(1))\omega(x)f(x), \qquad \Lambda(0) \neq 0,$$

$$H_{\omega f} = K_f[L^{\sigma(\omega)}f(x)]K_\omega[L^{\sigma(\omega)}f(x)]$$

and let $g(x) \neq \text{const}$ be an irreducible divisor of $L^{\sigma(\omega)}f(x)$ which does not divide $H_{\omega f}$. Then the degree of the polynomial $g(x)$ coincides with the exponent of $\Lambda(x)$.

Proof. We have

$$\sigma(\omega)L^{\sigma(\omega)}f(x) = \sum_{v=0}^{n}\sum_{u=0}^{\Omega} a_v\omega_u(x^u q)^v + f(1)\sum_{v=0}^{n} a_v =$$

$$= xL^x\left(\sum_{v=0}^{n}\sum_{u=0}^{\Omega} a_v\omega_u x^{u+v}\right) + f(1)\sum_{v=0}^{n} a_v = xL^x\omega(x)f(x) + f(1).$$

However, according to (2),

$$xL^x\omega(x)f(x) + f(1) = (L^x(x + f(1))\omega(x)f(x))(L^x\omega(x)f(x))^{-1},$$

therefore

$$\sigma(\omega)(L^x\omega(x)f(x))L^{\sigma(\omega)}f(x) = L^x\Lambda(x). \tag{4}$$

It follows from this (since the expression $L^x\Lambda(x)$ has no multiple roots, in view of $(xL^x\Lambda(x))' = \Lambda(0) \neq 0$) that

$$(\sigma(\omega)L^x\omega(x)f(x),\ L^{\sigma(\omega)}f(x)) = 1. \tag{5}$$

We now show that $g(x) \nmid K_\Lambda[L^x\Lambda(x)]$. Indeed, in the case $g(x)/K_\Lambda[L^x\Lambda(x)]$ we would have $g(x)/L^x\Lambda^1(\lambda)$, where $\Lambda^1(x)$ is a proper divisor of $\Lambda(x)$, and, by virtue of (5), $x + f(1)/\Lambda^1(x)$. Let

$$\Lambda^1(x) = (x + f(1))\omega^1(x)f^1(x) \quad (\omega^1/\omega,\ f^1/f,\ \omega^1 f^1 \neq \omega f).$$

According to (4),

$$\sigma(\omega^1)(L^x\omega^1(x)f^1(x))L^{\sigma(\omega^1)}f^1(x) = L^x\Lambda^1(x),$$

and therefore $g(x)/\sigma(\omega^1)(L^x\omega^1(x)f^1(x))L^{\sigma(\omega^1)}f^1(x)$. But, by the lemma,

$$L^x\omega^1(x)f^1(x)/L^x\omega(x)f(x),$$

and in view of the obvious identity

$$\sigma(\omega)L^x\omega(x) \equiv L^x\omega(x)(x + f(1)),$$

also

$$\sigma(\omega^1)L^x\omega^1(x)/\sigma(\omega)L^x\omega(x).$$

Moreover, by virtue of (5), $g(x) \nmid L^x\omega(x)f(x)$ and $g(x) \nmid \sigma(\omega)L^x\omega(x)$. Therefore it is clear that $g(x)/L^{\sigma(\omega^1)}f^1(x)$, or, what is the same, $g(x)/H_{\omega f}$, and this contradicts the condition of the theorem; consequently,

$$g(x) \nmid K_\Lambda[L^x\Lambda(x)].$$

Thus we are convinced that the polynomial $g(x)$, being a divisor of $L^x\Lambda(x)$, is relatively prime to $K_\Lambda[L^x\Lambda(x)]$. Hence, according to Theorem 1, it follows that its degree coincides with the exponent of the polynomial $\Lambda(x)$. The theorem is proved.

Relying on Theorem 3, one can prove the following fact.

Theorem 4. Let δ denote one of the numbers 0 or 1; let $\omega(x) = x^{1+\delta} + 1$, and let $f_i(x)$ $(i = 1, \dots, \sigma)$ be primitive polynomials with pairwise relatively prime degrees n_i, respectively.

Then the polynomial

$$F_2(x) = \prod_{j=0}^{\left[\frac{\sigma}{2}\right]} \left(\prod_{|\alpha|=\sigma-2j-1} L^{\sigma(\omega)}f^{(\alpha)}(x) \right)^{-1} \left(\prod_{|\alpha|=\sigma-2j} L^{\sigma(\omega)}f^{(\alpha)}(x) \right) \qquad (6)$$

is irreducible.

Proof. We first show that $F_2(x) \nmid K_\Lambda[L^x\Lambda(x)]$. Indeed, suppose the contrary, i.e. $F_2(x) \mid K_\Lambda[L^x\Lambda(x)]$. Then, obviously, $F_2(x) \mid L^x\Lambda^1(x)$, where $\Lambda^1(x)$ is a proper divisor of $\Lambda(x)$, and, by virtue of (5), and also according to the condition of the theorem $(\omega(x) = x^{1+\delta} + 1)$, $\Lambda^1(x) = (x+1)\omega(x)f^1(x)$ $(f^1 \neq f)$. Hence, by (4), (5), and since $F_2(x) \mid L^{\sigma(\omega)}f(x)$, it follows that $F_2(x) \mid L^{\sigma(\omega)}f^1(x)$. This contradicts the condition of the theorem, since from formula (6) it is seen that $F_2(x) \nmid K_f[L^{\sigma(\omega)}f(x)]$.

Thus, our assumption is false; consequently, $F_2(x) \nmid K_\Lambda[L^x\Lambda(x)]$. We now note that the degree of the polynomial $F_2(x)$ $(= 2^{1+\delta}M_{n_1,\dots,n_\sigma})$ coincides with the exponent of the polynomial $\Lambda(x)$. Therefore, by Theorem 3, the polynomial $F_2(x)$ is irreducible. The theorem is proved.

Theorem 4 extends the possibilities for constructing irreducible polynomials. With its help, for example, one can find irreducible polynomials whose degrees are represented in the form $2^{1+\delta}M_{n_1,\dots,n_\sigma}$. Thus, for example, in the case $\delta = 0$ and $f(x) = x^5 + x + 1$, we obtain the irreducible polynomial of degree 42

$$F_2(x) = \frac{L^{\sigma(x+1)}(x^5 + x + 1)}{L^{\sigma(x+1)}(x^2 + x + 1)\, L^{\sigma(x+1)}(x^3 + x^2 + 1)} =$$

$$= x^{42} + x^{41} + x^{40} + x^{35} + x^{32} + x^{30} + x^{29} + x^{28} + x^{27} +$$

SovietRxiv

$$+x^{26}+x^{25}+x^{23}+x^{18}+x^{15}+x^{14}+x^{13}+x^{8}+x^{6}+1.$$

Similarly, for $\delta = 1$ and $f(x) = x^3 + x + 1$, we shall have the irreducible polynomial of degree 28

$$F_2(x) = L^{\sigma(x^2+1)}(x^3+x+1) =$$

$$= (x^{17}+x^2)(x^{11}+x^8+x^7+x^5+x^3+x^2+x+1)+1.$$

Institute of Automation
and Telemechanics

Received
4 X 1963

CITED LITERATURE

1. W. W. Peterson, *Error-Correcting Codes*, N. Y.–London, 1961.

2. N. Zierler, J. Soc. Ind. Appl. Math., 7, No. 1, 31 (1959).

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.