Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Jacob T.B.jun. Beard

Unitary perfect polynomials over GF(q)

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **62** (1977), n.4, p. 417–422.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1977_8_62_4_417_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1977.

Algebra. — *Unitary perfect polynomials over* GF (q) (*). Nota di JACOB T. B. BEARD, JR., presentata (**) dal Socio B. SEGRE.

RIASSUNTO. — Se $A(x), B(x) \in GF[q, x]$ sono due polinomi monici, diciamo che $B(x)$ è un *divisore unitario* di $A(x)$ per esprimere che risulta $(B(x), A(x)/B(x)) = 1$; e che $A(x)$ è *unitariamente perfetto* su GF (q) se la somma $\sigma^*(A(x))$ dei divisori unitari distinti di $A(x)$ uguaglia $A(x)$. In questa Nota vengono caratterizzati i polinomi unitariamente perfetti su GF (p) che sono riducibili in GF $[p, x]$; ed assegnati quei 17 fra essi relativi al caso $p = 2$ che sono della forma $x^n f(x)$ con $n \geq 0, (x, f(x)) = 1$ e grado $f(x) \leq 15$; qualche altro risultato è anche ottenuto per $p = 3,5$.

1. INTRODUCTION AND NOTATION

For a monic polynomial $A(x) \in GF[q, x]$, the monic divisor $B(x) \in GF[q, x]$ of $A(x)$ is called a *unitary divisor* if and only if $(B(x), A(x)/B(x)) = 1$. As a natural complement to the concept of perfect polynomials introduced in [1], we say that the monic polynomial $A(x) \in GF[q, x]$ is *unitary perfect* over GF (q) if and only if the sum $\sigma^*(A(x))$ of the unitary divisors of $A(x)$ equals $A(x)$. The principal result of this note is a characterization of all unitary perfect polynomials over GF(p) which split in GF $[p, x]$.

Monic polynomials over GF (q) are denoted $A, B, C, \cdots$, while prime (monic irreducible) polynomials over GF (q) are denoted $P, Q, R, \cdots$ For brevity, we write $A \to B$ whenever $\sigma^*(A) = B$. It is clear that $\deg A = \deg \sigma^*(A)$ and that σ^* is multiplicative on its domain. Hence whenever $A \in GF[q, x]$ has the canonical decomposition $A = \prod_{i=1}^{n} P_i^{\alpha(i)}$ as the product of powers of distinct primes $P_i \in GF[q, x]$ with $\alpha(i) > 0$, then

$$A = \prod_{i=1}^{n} P_i^{\alpha(i)} \to \prod_{i=1}^{n} \sigma^*(P_i^{\alpha(i)}) = \prod_{i=1}^{n} (P_i^{\alpha(i)} + 1).$$

This fact is used extensively and without further reference. Though trivial, the following result will be appealed to frequently.

LEMMA. *The polynomial* A *is unitary perfect over* GF (q) *if and only if for each prime polynomial* $P \in GF[q, x]$, $m = n$ *whenever* $P^m \| A$ *and* $P^n \| \sigma^*(A)$.

Here, $P^k \| B$ is equivalent to $P^k \mid B$ and $P^{k+1} \nmid B$.

(*) This research was partially supported by an Organized Research Grant from the University of Texas at Arlington.

(**) Nella seduta del 16 aprile 1977.

2. Unitary perfect splitting polynomials

From Theorem 1, we will deduce that whenever the polynomial A is unitary perfect over GF (p) and splits in GF $[p, x]$, then $A = \prod_{i=0}^{p-1} (x - i)^{\alpha(i)}$ where $\alpha(i) > 0$ for $0 \leq i < p$. The analogous statement for $A \in GF[q, x]$ does not hold, by a later example. This is among the reasons we have thus far obtained only a partial characterization for unitary perfect polynomials which split in GF $[q, x]$. After showing each $\alpha(i) > 0$, we first assume $\alpha(i) = k$ for $0 \leq i < p$ and determine all integers k such that the polynomial $A = \prod_{i=0}^{p-1} (x - i)^k$ is unitary perfect over GF (p). Recall that each positive integer k can be uniquely represented to the base p as $k = \sum_{j=0}^{n} k(j) p^j$ where $0 \leq k(j) < p$ for $0 \leq j \leq n$.

Theorem 1. *If the polynomial* $A = \prod_{i=1}^{n} P_i^{\alpha(i)}$ *is unitary perfect over* GF(q), *the primes* P_i *are distinct,* $\alpha(i) > 0$, *and* $\alpha(1) \deg P_1 \leq \cdots \leq \alpha(n) \deg P_n$, *then for some integer* $k \geq 1$, $\alpha(1) \deg P_1 = \alpha(i) \deg P_i$ *for each* i *satisfying* $1 \leq i \leq kp$.

Proof. If A is unitary perfect, then the admissible summands of $\sigma^*(A) - A$ having maximum degree are monic and their leading coefficients sum to zero.

Corollary. *If the polynomial* A *is unitary perfect over* GF (p) *and splits in* GF $[p, x]$, *then* $\prod_{i=0}^{p-1} (x - i) \mid A$.

Theorem 2. *The polynomial* $A = \prod_{a \in GF(q)} (x - a)^{p^n}$ *is unitary perfect over* GF (q) *for each* $n \geq 0$.

Proof. For each $a \in GF(q)$,

$$(x - a)^{p^n} \rightarrow (x - a)^{p^n} + 1 = (x - a + 1)^{p^n},$$

so that

$$A = \prod_{a \in GF(q)} (x - a)^{p^n} \rightarrow \prod_{a \in GF(q)} (x - a + 1)^{p^n} = A .$$

From the proof of Theorem 2, it is easy to construct polynomials which are unitary perfect over GF (q) but which are not divisible by $\prod_{a \in GF(q)} (x - a)$. For example, let $q = p^d, d > 1$, and choose any fixed $a \in GF(q)$ such that $a \notin GF(p)$. For any $n \geq 0$ and any $i \in GF(p)$, $(x - a - i)^{p^n} \rightarrow (x - a - i + 1)^{p^n}$, so that $A = \prod_{i=0}^{p-1} (x - a - i)^{p^n} \rightarrow \prod_{i=0}^{p-1} (x - a - i + 1)^{p^n} = A$. Moreover, no linear polynomial in GF $[p, x]$ divides A. Continuing toward our characterization, we have

Theorem 3. *Let* $q = 2^d, d > 1$. *The polynomial* $A = \prod_{a \in GF(q)} (x - a)^{N2^n}$ *is unitary perfect over* GF (q) *whenever* $N \mid (q - 1)$, $N \neq 1$, *and* $n \geq 0$.

Proof. For each fixed $a \in$ GF (q), we have

$$(x-a^{N2^n}) \to (x-a)^{N2^n}+1=(x-a)^{N2^n}-1=[(x-a)^N-1]^{2^n}=$$
$$=\prod_{b\in H}(x-a-b)^{2^n}$$

where H is the unique (multiplicative) subgroup of GF $(q)^*$ of order N. Hence $(x-a)$ is contributed to $\sigma^*(A)$ only in the case $b \in H$ and, in this case, is contributed by

$$(x-a+b)^{N2^n} \to (x-a)^{2^n} \prod_{c\in H-\{b\}} (x-a+b-c)^{2^n}.$$

Since there are N such elements $b \in H$, then $(x-a)^{N2^n} \| \sigma^*(A)$ and we are done by the Lemma.

THEOREM 4. *Let* $q=p^d, p>2$. *If* $\frac{q-1}{N} \equiv 0 (\mathrm{mod}\ 2)$, *the polynomial* $A=\prod_{a\in GF(q)}(x-a)^{Np^n}$ *is unitary perfect over* GF (q) *for each* $n \geq 0$.

Proof. Consider

$$x^{Np^n} \to x^{Np^n}+1=(x^N+1)^{p^n}.$$

Since N divides $q-1$ an even number of times, $(x^N+1) \mid (x^{q-1}-1)$. Thus x^N+1 splits in GF $[q, x]$ as the product of distinct linear factors, say

$$x^N+1=\prod_{i=1}^{N}(x-d_i).$$

It follows that for each fixed $a \in$ GF (q),

$$(x-a)^N+1=\prod_{i=1}^{N}(x-a-d_i),$$

so that

$$(x-a)^{Np^n} \to [(x-a)^N+1]^{p^n}=\prod_{i=1}^{N}(x-a-d_i)^{p^n}.$$

For each j, $1 \leq j \leq N$, there exists a unique $b \in$ GF (q) such that $a=b+d_j$, and

$$(x-b)^{Np^n} \to (x-a)^{p^n}\prod_{i\neq j}(x-b-d_i)^{p^n}.$$

Thus $(x-a)^{Np^n} \| \sigma^*(A)$ and we are done by the Lemma.

We now show that the sufficient conditions on N in Theorem 2 – Theorem 4 are necessary.

THEOREM 5. *Let* $q=p^d, p>2$. *If* $(N, p)=1, \frac{q-1}{N} \not\equiv 0 \ (\mathrm{mod}\ 2)$, *and* $n \geq 0$, *then the polynomial* $A=\prod_{a\in GF(q)}(x-a)^{Np^n}$ *is not unitary perfect over* GF (q).

Proof. We consider

$$x^{Np^n} \to (x^N+1)^{p^n}.$$

Since $\frac{q-1}{N} \not\equiv 0 \pmod 2$, then (by ordinary long division) $(x^N+1) \nmid (x^{q-1}-1)$. Moreover, x^N+1 has no repeated roots in GF (q) as $(N, p) = 1$. Thus x^N+1 does not split in GF $[q, x]$. By the Lemma, the polynomial A is not unitary perfect.

The preceding results immediately yield

THEOREM 6. *The polynomial* $A = \prod_{a \in GF(q)} (x-a)^{Np^n}$ *is unitary perfect over* GF (q) *if and only if* $n \geq 0$ *and either* $p = 2$ *and* $N \mid (q-1)$ *or else* $p > 2$ *and* $\frac{q-1}{N} \equiv 0 \pmod 2$.

This partial characterization of splitting unitary perfect polynomials over GF (q) is strengthened considerably over GF (p), as in

THEOREM 7. *The polynomial* $A = \prod_{i \geq 0}^{p-1} (x-i)^k$ *is unitary perfect over* GF (p) *if and only if* $k = Np^n$ *where* $n \geq 0$ *and either* $p = 2$ *and* $N = 1$ *or else* $p > 2$ *and* $\frac{p-1}{N} \equiv 0 \pmod 2$.

Proof. There remains only to prove the necessity in the case $k > p$. Assume k is not of the admitted form, and let $k = \sum_{j=0}^{m} k(j)\, p^j$ where $0 \leq k(j) < p$ for $0 \leq j < m$ and $0 < k(m) < p$. Consider

$$x^k \to x^{k(m)p^m + \cdots + k(1)p + k(0)} + 1 = x^k + 1 .$$

As before, it suffices to show that the polynomial x^k+1 does not split in GF $[p, x]$. If $k(0) \neq 0$, this is easily seen since $x^k + 1 \notin$ GF $[p, x^p]$ and $k > p$. If $k(0) = 0$, then

$$x^k + 1 = (x^{k(m)p^{m-l} + \cdots + k(l)} + 1)^{p^l} = B^{p^l}$$

where l is the least positive integer j such that $k(j) \neq 0$. Note that $l < m$, otherwise we are done by previous arguments. Then $B \notin$ GF $[p, x^p]$ and $\deg B > p$. Hence B does not split in GF $[p, x]$, neither does $x^k + 1$, and we are done.

The unitary perfect polynomials over GF (p) which split in GF $[p, x]$ are fully characterized in our concluding result.

THEOREM 8. *The polynomial* $A = \prod_{i=0}^{p-1} (x-i)^{\alpha(i)}$ *is unitary perfect over* GF (p) *if and only if the following conditions are satisfied*:

i) $\alpha(0) = \alpha(j)$ *for* $0 \leq j < p$,

ii) $\alpha(0) = Np^n$ *where* $n \geq 0$ *and either* $p = 2$ *and* $N = 1$ *or* $p > 2$ *and* $(p-1)/N \equiv 0 \pmod 2$.

Proof. By earlier arguments, each $\alpha(i)$ must be of the admissible form given in Theorem 7. Thus there remains only to establish $\alpha(0) = \alpha(j)$ for $0 \leq j < p$, which is immediate from Theorem 1.

3. Unitary perfect non-splitting polynomials

Most of the unitary perfect polynomials given in this section were obtained on an IBM 360/155 using (unpublished) complete factorization tables previously obtained by Beard and Karen I. West for all monic polynomials $f(x)$ with $(x, f(x)) = 1$ over GF (p) of degree m satisfying

$$\begin{aligned} p = 2,&\quad 2 \leq m \leq 15; \\ 3,&\quad 2 \leq m \leq 9; \\ 5,&\quad 2 \leq m \leq 6. \end{aligned}$$

For $n \geq 0$ there are no non-splitting unitary perfect polynomials over GF (3) or GF (5) of the form $x^n f(x)$ where $f(x)$ satisfies the above conditions. The Table at the end includes the complete factorization of all non-splitting unitary perfect polynomials over GF (2) of the form $x^n f(x)$ where $n \geq 0$, $(x, f(x)) = 1$, and $\deg f(x) \leq 15$. The remaining examples in that Table have been constructed by two students, Alice T. Bullock and Mickie S. Harbin. We note that of the 28 listed polynomials $x^n f(x)$ over GF (2), 22 of the factors $f(x)$ are reciprocal polynomials. Ongoing attempts to find non-splitting unitary perfect polynomials over GF (5) are fruitless thus far.

We are reminded that Canaday [2] considered the 11 non-splitting perfect polynomials over GF (2) as likely to be all such, and of the open question as to whether $x \mid A$ whenever A is perfect over GF (p). It is easily verified that $x(x - 1) \mid A$ whenever A is unitary perfect over GF (2).

Non-splitting Unitary Perfect Polynomials Over GF (p)

p	degree	Complete Factorization
2	7	$x^3(1+x)^2(1+x+x^2)$, $x^2(1+x)^3(1+x+x^2)$
	10	$x^3(1+x)^3(1+x+x^2)^2$
	13	$x^5(1+x)^4(1+x+x^2+x^3+x^4)$, $x^4(1+x)^5(1+x^3+x^4)$
	14	$x^6(1+x)^4(1+x+x^2)^2$, $x^4(1+x)^6(1+x+x^2)^2$
	16	$x^3(1+x)^3(1+x+x^2)^3(1+x+x^4)$
	17	$x^7(1+x)^4(1+x+x^3)(1+x^2+x^3)$, $x^4(1+x)^7(1+x+x^3)(1+x^2+x^3)$
	18	$x^5(1+x)^5(1+x^3+x^4)(1+x+x^2+x^3+x^4)$
	19	$x^6(1+x)^5(1+x+x^2)^2(1+x^3+x^4)$, $x^5(1+x)^6(1+x+x^2)^2(1+x+x^2+x^3+x^4)$
	20	$x^6(1+x)^6(1+x+x^2)^4$, $x^6(1+x)^4(1+x+x^2)^3(1+x+x^4)$
	22	$x^7(1+x)^5(1+x+x^3)(1+x^2+x^3)(1+x^3+x^4)$
	23	$x^9(1+x)^4(1+x+x^2)^2(1+x^3+x^6)$
	26	$x^{10}(1+x)^8(1+x+x^2+x^3+x^4)^2$
	28	$x^{12}(1+x)^8(1+x+x^2)^4$
	34	$x^{14}(1+x)^8(1+x+x^3)^2(1+x^2+x^3)^2$
	37	$x^{11}(1+x)^8(1+x+x^2+x^3+x^4)^2(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10})$

p	degree	Complete Factorization
2	41	$x^{13}(1+x)^8(1+x+x^2)^4(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12})$
	52	$x^{20}(1+x)^{16}(1+x+x^2+x^3+x^4)^4$
	56	$x^{24}(1+x)^{16}(1+x+x^2)^8$
	58	$x^{18}(1+x)^8(1+x+x^2)^6(1+x+x^4)^2(1+x^3+x^6)^2$
	74	$x^{22}(1+x)^{16}(1+x+x^2+x^3+x^4)^4(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10})^2$
	78	$x^{30}(1+x)^{16}(1+x+x^2)^4(1+x+x^4)^2(1+x^3+x^4)^2(1+x+x^2+x^3+x^4)^2$
	82	$x^{26}(1+x)^{16}(1+x+x^2)^8(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12})^2$
3	12	$x^2(1+x)^2(2+x)^2(1+x^2)(2+x+x^2)(2+2x+x^2)$
	25	$x^8(1+x)^2(2+x)^3(1+x^2)(2+2x+x^2)(2+x^2+x^4)(2+2x^2+x^4)$
	36	$x^6(1+x)^6(2+x)^6(1+x^2)^3(2+x+x^2)^3(2+2x+x^2)^3$

REFERENCES

[1] J. T. B. BEARD, JR., J. R. OCONNELL, Jr. and K. I. WEST – *Perfect polynomials over* GF (q), « Rend. Acc. Naz. Lincei ».

[2] E. F. CANADAY (1941) – *The sum of the divisors of a polynomial*, « Duke Math. J. », 7, 721–737.