Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Jacob T.B.jun. Beard, Alice T. Bullock, Mickie Sue Harbin

Infinitely many perfect and unitary perfect polynomials

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **63** (1977), n.5, p. 294–303.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1977_8_63_5_294_0>

Algebra. — *Infinitely many perfect and unitary perfect polynomials* (*). Nota di JACOB T. B. BEARD Jr., ALICE T. BULLOCK e MICKIE SUE HARBIN, presentata (**) dal Socio E. MARTINELLI a nome del compianto Socio B. SEGRE.

RIASSUNTO. — Dopo avere ottenuto vari casi per $q = p^d$ in cui su GF (q) esistono infiniti polinomi irriducibili che sono unitari e perfetti, si studia il numero di tali polinomi in altri casi e si fa per esso una congettura.

1. INTRODUCTION AND NOTATION

The language of this paper is that of [1], [2]. Briefly, a monic polynomial $A = A(x) \in GF[q, x]$, $q = p^d$, $d \geq 1$, is called *perfect* over GF (q) if and only if the sum $\sigma(A)$ of the distinct monic divisors in GF $[q, x]$ of A equals A. If $A, B \in GF[q, x]$ are monic, B is called a *unitary divisor* of A if and only if $(B, A/B) = 1$. The monic polynomial $A \in GF[q, x]$ is *unitary perfect* over GF (q) if and only if the sum $\sigma^*(A)$ of the distinct unitary divisors in GF $[q, x]$ of A equals A. The polynomial $A \in GF[q, x]$ is a *splitting* polynomial over GF (q) if and only if A factors in GF $[q, x]$ as the product of linear irreducibles; otherwise, A is a *non-splitting* polynomial over GF (q). The monic polynomial $P \in GF[q, x]$ is *prime* if and only if P is irreducible over GF (q). For brevity we write $A \to D$ to indicate $\sigma(A) = D$ or, in context, $\sigma^*(A) = D$, and recall that the functions σ and σ^* are multiplicative on their domains. Thus if $A \in GF[q, x]$ has the canonical decomposition $A = \prod_{i=1}^{k} P_i^{\alpha(i)}$ where the primes $P_i \in GF[q, x]$ are distinct and the $\alpha(i) > 0$, then

$$(1) \qquad A \xrightarrow{\sigma} \prod_{i=1}^{k} \sigma(P_i^{\alpha(i)}) = \prod_{i=1}^{k} \sum_{j=0}^{\alpha(i)} P_i^j = \prod_{i=1}^{k} \frac{P_i^{\alpha(i)+1} - 1}{P_i - 1}$$

and

$$(2) \qquad A \xrightarrow{\sigma^*} \prod_{i=1}^{k} \sigma^*(P_i^{\alpha(i)}) = \prod_{i=1}^{k} (P_i^{\alpha(i)} + 1).$$

From [2; Theorem 3] the number SP (q) of splitting perfect polynomials over GF (q) is infinite. Concerning the number NSP (q) of non-splitting perfect polynomials over GF (q), [2; Table I] established NSP $(2) \geq 11$,

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

(**) Nella seduta del 18 novembre 1977.

NSP $(3) \geq 16$, NSP $(5) \geq 13$, the lower bound on NSP (2) remaining that of Canaday [7]. Our present results (Section 4) on the infinitude of NSP (2^d), NSP (3^d), NSP (5^d) are almost incidental. The primary results of this paper have followed the study of numerous examples, hand-constructed by Bullock and Harbin, of non-splitting unitary perfect polynomials over GF (p), $p = 2, 3, 5$. Previously [1; Theorems 6, 7] it was determined that for each q, there are infinitely many splitting unitary perfect polynomials over GF (q), and that there exist at least 28 (3) non-splitting unitary perfect polynomials over GF (2) (GF (3)). Here (Theorem 1) it is established that GF $[q, x]$ contains infinitely many non-splitting unitary perfect polynomials over GF (q) *provided it contains at least one*. This general existence question remains open, but the question it would answer is weak. A natural equivalence relation $\tilde{q}$ defined on GF $[q, x]$ (Section 2) illuminates the better question: to determine the number of distinct $\tilde{q}$ equivalence classes containing (non-splitting) unitary perfect polynomials over GF (q). E.g., the infinite set $\{x^{2^n}(1 + x)^{2^n}\}$ of splitting unitary perfect polynomials over GF (2) is precisely the 2-equivalence class containing $x(1 + x)$, while the 28 non-splitting unitary perfect polynomials over GF (2) given in [1] determine 18 2–equivalence classes as in Section 5. The numbers SUP (q) and NSUP (q) of distinct $\tilde{q}$–classes containing splitting and non-splitting unitary perfect polynomials over GF (q) respectively are discussed in Section 3. Not known to be deterministic, the algorithm used to construct the examples in [1; Table I], [2; Table I] and Table I of Section 5 is discussed briefly.

We gratefully acknowledge the comments and suggestions of Professors Leonard Carlitz and Robert M. McConnel.

2. q–EQUIVALENCE ON GF $[q, x]$

For all $A, B \in$ GF $[q, x]$ we say that A is *q–equivalent* to B, written $A \tilde{q} B$, if and only if there exists an integer l (negative, zero, or positive) such that $A = B^{p^l}$ where $q = p^d, d \geq 1$. It is clear that $\tilde{q}$ is an equivalence relation on GF $[q, x]$, each $\tilde{q}$-class $\bar{A}$ contains a unique polynomial C of minimum degree, and that $C \notin$ GF $[q, x^p]$. We call C *the representative* of the $\tilde{q}$-class $\bar{A}$, and emphasize $\bar{A} = \{C^{p^n}\}_{n \geq 0}$. The concept of q–equivalence is motivated by

THEOREM 1. *Let* $A \in$ GF $[q, x]$, $q = p^d, d \geq 1$, *and let* $n \geq 0$. *Then* A *is unitary perfect over* GF (q) *if and only if* A^{p^n} *is unitary perfect over* GF (q).

Proof. From (2),

$$A^{p^n} = \prod_{i=1}^{k} P_i^{\alpha(i)p^n} \xrightarrow{\sigma^*} \prod_{i=1}^{k} (P_i^{\alpha(i)p^n} + 1) = \prod_{i=1}^{k} (P_i^{\alpha(i)} + 1)^{p^n}$$

$$= \left(\prod_{i=1}^{k} (P_i^{\alpha(i)} + 1) \right)^{p^n} = (\sigma^*(A))^{p^n}.$$

THEOREM 2. *Let* $A, C \in GF[q, x], q = p^d, d \geq 1$. *If* $A \tilde{q} C$, *then* A *and* C *are simultaneously* (*splitting*) ((*non-splitting*)) *unitary perfect polynomials over* GF (q).

Proof. The results are evident from Theorem 1 and its proof.

3. THE NUMBERS SUP (q) AND NSUP (q)

From Theorem 2, either all polynomials in a $\tilde{q}$-class are unitary perfect over GF (q) or else none are. Moreover, all of the polynomials in a $\tilde{q}$-class split over GF (q) or else all of them are non-splitting over GF (q). Thus it is appropriate to define SUP (q) as the number (perhaps infinite) of distinct $\tilde{q}$-classes containing splitting unitary perfect polynomials over GF (q), and NSUP (q) as the number of distinct $\tilde{q}$-classes containing non-splitting unitary perfect polynomials over GF (q).

The splitting unitary perfect polynomials over GF (p) have been characterized [1; Theorem 8] as precisely those polynomials $A = \prod_{i=0}^{p-1} (x - i)^{Np^n}$ where $n \geq 0$ and either i) $p = 2$ and $N = 1$, or ii) $p > 2$ and $(p - 1)/N \equiv 0 \pmod 2$. Letting $\tau_e(m)$ denote the number of even positive divisors of the integer m, we have part of

THEOREM 3. *The number* SUP (q) *of distinct* $\tilde{q}$*-classes of splitting unitary perfect polynomials over* GF (q) *is given by*

$$\text{SUP}(q) = \begin{cases} 1 & , \text{ if } q = 2 \\ \tau_e(q-1) & , \text{ if } q = p > 2 \\ \infty & , \text{ if } q \neq p . \end{cases}$$

Proof. There remains only to show SUP $(q) = \infty$ whenever $q = p^d$ and $d > 1$. We generalize the example following Theorem 2 in [1]. Choose $a_1, \cdots, a_{p^{d-1}} \in GF(q)$ such that $(a_k + GF(p)) \cap (a_j + GF(p)) = \phi$ for $k \neq j$. Then each polynomial $A_k = \prod_{i=0}^{p-1} (x - a_k - i)$ is unitary perfect over GF (q) and the A_k are pairwise relatively prime. For all distinct sequences of integers $n(1), \cdots, n(p^{d-1}) \geq 0$ such that at least one $n(k) = 0$, the polynomials of the form

$$A = \prod_{k=1}^{p^{d-1}} A_k^{p^{n(k)}} = \prod_{k=1}^{p^{d-1}} \prod_{i=0}^{p-1} (x - a_k - i)^{p^{n(k)}} \tag{3}$$

are the representatives of distinct splitting unitary perfect $\tilde{q}$-classes.

The above proof-technique easily establishes

THEOREM 4. *Let* $A, B \in GF[q, x]$ *be unitary perfect over* GF (q), $q = p^d$, $d \geq 1$. *If* $(A, B) = 1$ *and* B *does not split in* GF $[q, x]$, *then* NSUP $(q) = \infty$.

In constructing the polynomials A in (3), exactly one of the chosen a_k lies in GF (p), call it a_1. Then the polynomials (for any choices of $n\,(k) \geq 0$) of the form

$$A' = \prod_{k=2}^{p^d-1} \prod_{i=0}^{p-1} (x - a_k - i)^{p^{n(k)}} \tag{4}$$

are splitting unitary perfect polynomials over GF (q) with $\left(A', \prod_{i=0}^{p-1} (x-i)\right) = 1$. In Table I (Section 5) we note the non-splitting unitary perfect polynomials over GF (2):

$$B_1 = x^2 (1+x)^3 (1+x+x^2) \quad , \quad B_2 = x^4 (1+x)^7 (1+x+x^3) (1+x^2+x^3); \tag{5}$$

over GF (3):

$$B_3 = x^2 (1+x)^2 (2+x)^2 (2+x+x^2) (2+2x+x^2); \tag{6}$$

and over GF (5):

$$B_4 = x^4 (1+x)^2 (2+x)^2 (3+x)^2 (4+x)^2 (2+x^2) (3+x^2)^2. \tag{7}$$

Since the irreducible quadratic factors of B_1 (B_3) ((B_4)) over GF (2) (GF (3)) ((GF (5))) remain irreducible over GF (2^d) (GF (3^d)) ((GF (5^d))) for all odd integers $d \geq 1$, then B_1 (B_3) ((B_4)) is a non-splitting unitary perfect polynomial over GF (2^d) (GF (3^d)) ((GF (5^d)) for each odd $d \geq 1$. Similarly, B_2 is a non-splitting unitary perfect polynomial over GF (2^d) for each (even) integer $d \not\equiv 0 \pmod 3$.

THEOREM 5. NSUP (2^d) $= \infty$ *for each odd integer* $d > 1$ *and for each (even) integer* $d \not\equiv 0 \pmod 3$. NSUP (3^d) $= \infty =$ NSUP (5^d) *for each odd integer* $d > 1$.

Proof. Apply Theorem 3, taking $A = A'$ in (4) and $B = B_i$ in (5), (6), (7).

4. THE NUMBER NSP (q)

We are without a " perfect " analog of Theorem 1, but are still able to mimic the preceding arguments beginning with the identified portion of the proof of Theorem 2. In the place of Theorem 1, we appeal to [2; Theorem 1]: the polynomial $A = \prod_{a \in GF(q)} (x-a)^{p^n-1}$ is perfect over GF (q) for each $n \geq 0$. Modifying the polynomials in (4) only by changing the exponents on the linear factors, we generalize the example in [2; Section 3], obtaining polynomials

$$A'' = \prod_{k=2}^{p^d-1} \prod_{i=0}^{p-1} (x - a_k - i)^{p^{n(k)}-1} \tag{8}$$

which are splitting perfect polynomials over GF (q) with $\left(A'', \prod_{i=0}^{p-1}(x-i)\right) = 1$, for all choices of the $n\,(k) \geq 0$. Since the product of relatively prime perfect polynomials over GF (q) is perfect over GF (q), the non-splitting perfect polynomials [2] over GF (2):

$$x\,(1+x)^2\,(1+x+x^2) \quad , \quad x^3\,(1+x)^6\,(1+x+x^3)\,(1+x^2+x^3);$$

over GF (3):

$$x\,(1+x)^3\,(2+x)^2\,(2+2x+x^2);$$

and over GF (5):

$$x^3\,(1+x)^2\,(2+x)^2\,(3+x)^2\,(4+x)\,(2+x^2)\,(3+x^2)\,(3+3x+x^2)$$
$$(4+3x+x^2)\,(3+2x+x^2)\,(4+2x+x^2)\,;$$

together with the appropriate A'' in (8), yield

THEOREM 6. NSP $(2^d) = \infty$ *for each odd integer* $d > 1$ *and for each (even) integer* $d \not\equiv 0 \pmod 3$. NSP $(3^d) = \infty =$ NSP (5^d) *for each odd integer* $d > 1$.

5. UNITARY PERFECT q-EQUIVALENCE CLASS REPRESENTATIVES

In Table I, the $\tilde{p}$-class representatives are given for all currently known non-splitting unitary perfect $\tilde{p}$-classes over GF (p) establishing NSUP $(2) \geq 33$, NSUP $(3) \geq 16$, and NSUP $(5) \geq 6$. The polynomials which are starred (*) here are the $\tilde{p}$-class representatives of the $\tilde{p}$-classes determined by the examples in [1; Table 1]. (Several of the starred representatives do not appear in [1] as they were discovered, inexplicably, only after Theorem 1 was realized). In the construction of non-splitting perfect [2] and unitary perfect polynomials, we have relied heavily on [3]–[6] and the algorithm to follow (modified in the obvious fashion to obtain perfect polynomials):

Step 1. Compute and factor $\sigma^*(x^n)$ obtaining

$$x^n \xrightarrow{\sigma^*} \prod_{i=1}^{k} P_i^{\alpha(i)}. \tag{9}$$

Step 2. If the left and right sides of the statement (9) are equal, stop. Otherwise, replace the left side of (9) by the *l.c.m.* of the left and right sides of (9) and compute the new right side of (9). Repeat Step 2.

The trial balloon built into Step 2 frequently has drastic effects, and the algorithm is not thought to be deterministic. Other examples have been found by initiating the algorithm at $x^n\,(1+x)^n$, etc., motivated originally by having obtained examples divisible by both $x^n\,(1+x)^m$ and $x^m\,(1+x)^n$. The ineffec-

tiveness of the algorithm is clear on noting the 2-equivalence class representatives of degrees 23 and 29 divisible by $x^4(1+x)^9$ and $x^9(1+x)^4$, yet only one known representative divisible by $x^9(1+x)^9$. (The two 2-equivalence class representatives involving $x^3(1+x)^5$ were found by an exhaustive computer search [1; Section 3]). In fact, the four examples involving the form $x^4(1+x)^9$ or $x^9(1+x)^4$ were not all determined using the algorithm. Professor Carlitz has reminded us to expect, as in the case of perfect polynomials, the polynomials $A(x), A(x+1), \cdots, A(x+p-1)$ to be simultaneously unitary perfect over GF (p), and two of the aforementioned examples (as well as several others) have been so determined after using the algorithm to discover $A(x)$. The more general expectation holds as well, as in

THEOREM 7. *Let* $A(x) \in GF[q, x]$, $q = p^d$, $d \geq 1$. *If* $A(x)$ *is perfect (unitary perfect) over* GF (q) *and* $b \in GF(q)$, *then* $B(x) = A(x+b)$ *is perfect (unitary perfect) over* GF (q).

Proof. We prove the result in the case $A(x)$ is unitary perfect over GF (q), a similar argument sufficing in the event $A(x)$ is perfect over GF (q). Let $A(x) = \prod_{i=1}^{k} (P_i(x))^{\alpha(i)}$ where the primes $P_i(x) \in GF[q, x]$ are distinct and the $\alpha(i) > 0$. Let GF (q^e) be a splitting field for $A(x)$ over GF (q). Then there exist $a_1, \cdots, a_k \in GF(q^e)$ such that for each i, $1 \leq i \leq k$, we have

$$(P_i(x))^{\alpha(i)} = \prod_{j=0}^{\beta(i)-1} (x - a_i^{q^j})^{\alpha(i)},$$

where $\deg P_i(x) = \beta(i)$. Since the $P_i(x)$ are pairwise relatively prime over GF (q), the $P_i(x)$ are pairwise relatively prime over GF (q^e) [9; p. 119]. Moreover, for each $b \in GF(q)$,

$$P_i(x+b) = \prod_{j=0}^{\beta(i)-1} (x + b - a_i^{q^j}) = \prod_{j=0}^{\beta(i)-1} [x - (a_i - b)^{q^j}].$$

Since each $a_i - b$ has degree $\beta(i)$ [8; Lemma 3.3], it follows that each $Q_i(x) = P_i(x+b)$ is prime of degree $\beta(i)$ in GF $[q, x]$, the $Q_i(x)$ are pairwise relatively prime in GF $[q, x]$ and, hence, the primes $Q_i(x)$ are distinct. Thus if $A(x)$ is unitary perfect over GF (q),

$$(10) \qquad A(x) = \prod_{i=1}^{k} (P_i(x))^{\alpha(i)} \xrightarrow{\sigma^*} \prod_{i=1}^{k} [(P_i(x)^{\alpha(i)} + 1] = \prod_{i=1}^{k} (P_i(x))^{\alpha(i)},$$

and from the right-most equality in (10) we obtain the right-most equality in

$$B(x) = A(x+b) = \prod_{i=1}^{k} (Q_i(x))^{\alpha(i)} \xrightarrow{\sigma^*} \prod_{i=1}^{k} [(Q_i(x))^{\alpha(i)} + 1] = \prod_{i=1}^{k} (Q_i(x))^{\alpha(i)},$$

so that $B(x) = A(x+b)$ is unitary perfect over GF (q).

Our failure to obtain examples of non-splitting unitary perfect polynomials over GF (p) for $p \geq 7$ is felt to be due solely to the limited extent

of our factorization tables. Likewise, we expect there are non-splitting perfect polynomials over GF (p) for each $p \geq 7$. Several other conjectures appear reasonable, though strong. Among them are the following:

i) For each q and each prime polynomial $P \in GF[q, x]$, P divides some unitary perfect polynomial over GF (q).

ii) For each p and each unitary perfect polynomial A over GF (p), the polynomial $\prod_{i=0}^{p-1}(x-i)$ divides A.

iii) For each p and each odd integer $d \geq 1$, NSUP $(p^d) = \infty$.

iv) For each p and each integer $d \geq 1$, the polynomial $\prod_{i=0}^{p-1}(x-1)^d$ divides some unitary perfect polynomial over GF (p).

As observed in [1], the statement (ii) holds for $p = 2$.

TABLE I

Some Distinct Non-Splitting Unitary Perfect $\tilde{p}$-Class Representatives

p	Degree		Complete Factorization
2	7	*	$x^2(1+x)^3(1+x+x^3)$
		*	$x^3(1+x)^2(1+x+x^3)$
	10	*	$x^3(1+x)^3(1+x+x^3)^2$
	13	*	$x^4(1+x)^5(1+x^3+x^4)$
		*	$x^5(1+x)^4(1+x+x^2+x^3+x^4)$
	16	*	$x^3(1+x)^3(1+x+x^3)^3(1+x+x^4)$
	17	*	$x^4(1+x)^7(1+x+x^3)(1+x^2+x^3)$
		*	$x^7(1+x)^4(1+x+x^3)(1+x^2+x^3)$
	18	*	$x^5(1+x)^5(1+x^3+x^4)(1+x+x^2+x^3+x^4)$
	19	*	$x^5(1+x)^6(1+x+x^3)^2(1+x+x^2+x^3+x^4)$
		*	$x^6(1+x)^5(1+x+x^2)^2(1+x^3+x^4)$
	20	*	$x^4(1+x)^6(1+x+x^3)^3(1+x+x^4)$
			$x^6(1+x)^4(1+x+x^2)^3(1+x+x^4)$
	22		$x^5(1+x)^7(1+x+x^3)(1+x^2+x^3)(1+x+x^2+x^3+x^4)$
		*	$x^7(1+x)^5(1+x+x^3)(1+x^2+x^3)(1+x^3+x^4)$
	23		$x^4(1+x)^9(1+x+x^3)^2(1+x+x^3+x^4+x^6)$
			$x^6(1+x)^7(1+x+x^3)^2(1+x+x^3)(1+x^2+x^3)$
			$x^7(1+x)^6(1+x+x^3)^2(1+x+x^3)(1+x^2+x^3)$
		*	$x^9(1+x)^4(1+x+x^3)^2(1+x^3+x^6)$
	26		$x^7(1+x)^7(1+x+x^3)^2(1+x^2+x^3)^2$

TABLE I (*Cont.*)

p	Degree		Complete Factorization
2	29		$x^4(1+x)^9(1+x+x^2)^3(1+x+x^4)(1+x+x^3+x^4+x^6)$
		*	$x^9(1+x)^4(1+x+x^2)^3(1+x+x^4)(1+x^3+x^6)$
	37		$x^8(1+x)^{11}(1+x^3+x^4)^2(1+x+x^2+x^7+x^8+x^9+x^{10})$
		*	$x^{11}(1+x)^8(1+x+x^2+x^3+x^4)^2$ $(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10})$
	38		$x^9(1+x)^9(1+x+x^2)^4(1+x^3+x^6)(1+x+x^3+x^4+x^6)$
	39		$x^8(1+x)^{15}(1+x+x^2)^2(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$
		*	$x^{15}(1+x)^8(1+x+x^2)^2(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$
	41		$x^8(1+x)^{13}(1+x+x^2)^4(1+x^3+x^4+x^7+x^8+x^{11}+x^{12})$
		*	$x^{13}(1+x)^8(1+x+x^2)^4$ $(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12})$
	58		$x^{11}(1+x)^{11}(1+x+x^2+x^3+x^4)^2(1+x^3+x^4)^2$ $(1+x+x^2+x^7+x^8+x^9+x^{10})$ $(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10})$
	62		$x^{15}(1+x)^{15}(1+x+x^2)^4(1+x+x^4)^2(1+x^3+x^4)^2$ $(1+x+x^3+x^3+x^4)^2$
	66		$x^{13}(1+x)^{13}(1+x+x^2)^8(1+x^3+x^4+x^7+x^8+x^{11}+x^{12})$ $(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12})$
	86		$x^{17}(1+x)^{17}(1+x+x^2)^2(1+x+x^3)(1+x^2+x^3)(1+x^2+x^5)$ $(1+x+x^2+x^4+x^5)(1+x+x^2+x^4+x^6+x^7+x^8)$ $(1+x^2+x^3+x^5+x^8)(1+x^3+x^4+x^5+x^8)$ $(1+x^2+x^3+x^4+x^5+x^7+x^8)$
3	12	*	$x^2(1+x)^2(2+x)^2(1+x^2)(2+x+x^2)(2+2x+x^2)$
	18		$x^3(1+x)^3(2+x)^5(2+x+x^2+x^3)(2+2x+x^2+x^3+x^4)$
			$x^3(1+x)^5(2+x)^3(1+2x+x^2+x^3)(1+2x+x^2+x^4)$
			$x^5(1+x)^3(2+x)^3(2+x^2+x^3)(1+2x+x^2+2x^3+x^4)$
	25		$x^2(1+x)^3(2+x)^8(1+x^2)(2+x+x^2)(1+x^2+2x^3+x^4)$ $(2+x+2x^2+2x^3+x^4)$
			$x^3(1+x)^8(2+x)^2(2+x+x^2)$ $(2+2x+x^2)(1+x^2+x^3+x^4)(2+2x+2x^2+x^3+x^4)$
		*	$x^8(1+x)^2(2+x)^3(1+x^2)(2+2x+x^2)(2+x^2+x^4)(2+2x^2+x^4)$
	36		$x^4(1+x)^4(2+x)^4(1+x^2)^2(2+x+x^2)^2(2+2x+x^2)^2(2+2x^2+x^4)$ $(2+x+2x^2+2x^3+x^4)(2+2x+2x^2+x^3+x^4)$
			$x^5(1+x)^5(2+x)^5(2+x^2+x^3)(1+2x+x^2+x^3)(2+x+x^2+x^3)$ $(1+2x+x^2+x^4)(1+2x+x^2+2x^3+x^4)(2+2x+x^2+x^3+x^4)$

TABLE I (*Cont.*)

p	Degree	Complete Factorization
3	37	$x^6(1+x)^6(2+x)^7(1+x^2)^3(2+2x+x^2)^3(1+2x^2+x^3+2x^5+x^6)$
		$(2+2x^2+x^3+2x^5+x^6)$
		$x^6(1+x)^7(2+x)^6(1+x^2)^3(2+x+x^2)^3(1+x^3+2x^4+2x^5+x^6)$
		$(2+x^3+2x^4+2x^5+x^6)$
		$x^7(1+x)^6(2+x)^6(2+x+x^2)^3(2+2x+x^2)^3$
		$(1+2x+x^2+2x^3+x^4+2x^5+x^6)$
		$(2+2x+x^2+2x^3+x^4+2x^5+x^6)$
	54	$x^8(1+x)^8(2+x)^8(1+x^2)(2+x+x^2)(2+2x+x^2)(2+x^2+x^4)$
		$(2+2x^2+x^4)(1+x^2+x^3+x^4)(1+x^2+2x^3+x^4)$
		$(2+2x+2x^2+x^3+x^4)(2+x+2x^2+2x^3+x^4)$
	57	$x^7(1+x)^7(2+x)^7(1+2x+x^2+2x^3+x^4+2x^5+x^6)$
		$(1+2x^2+x^3+2x^5+x^6)(1+x^3+2x^4+2x^5+x^6)$
		$(2+2x+x^2+2x^3+x^4+2x^5+x^6)(2+2x^2+x^3+2x^5+x^6)$
		$(2+x^3+2x^4+2x^5+x^6)$
	60	$x^{10}(1+x)^{10}(2+x)^{10}(1+x^2)(2+x+x^2)(2+2x+x^2)$
		$(1+2x+x^3+x^4)(1+x+2x^3+x^4)(2+x+x^4)(2+2x+x^4)$
		$(2+x^3+x^4)(2+2x^3+x^4)$
	90	$x^{11}(1+x)^{11}(2+x)^{11}(1+x^2)(2+x+x^2)(2+2x+x^2)$
		$(1+2x^2+x^3)(1+x+2x^2+x^3)(2+2x+2x^2+x^3)$
		$(1+2x+x^3+x^4)(2+x+x^4)(2+2x^3+x^4)(1+2x+2x^2+2x^3+x^5)$
		$(1+2x^2+2x^3+2x^4+x^5)(2+2x+2x^4+x^5)$
		$(2+2x+2x^3+x^4+x^5)(1+x^2+x^4+x^5)(2+2x+x^2+x^3+x^5)$
5	18	$x^2(1+x)^2(2+x)^2(3+x)^2(4+x)^4(3+3x+x^2)(4+3x+x^2)^2$
		$x^2(1+x)^2(2+x)^2(3+x)^4(4+x)^2(1+x+x^2)(2+x+x^2)^2$
		$x^2(1+x)^2(2+x)^4(3+x)^2(4+x)^2(1+4x+x^2)(2+4x+x^2)^2$
		$x^2(1+x)^4(2+x)^2(3+x)^2(4+x)^2(3+2x+x^2)(4+2x+x^2)^2$
		$x^4(1+x)^2(2+x)^2(3+x)^2(4+x)^2(2+x^2)(3+x^2)^2$
	35	$x^3(1+x)^3(2+x)^3(3+x)^3(4+x)^3(2+x^2)(3+x^2)(1+x+x^2)$
		$(2+x+x^2)(3+2x+x^2)(4+2x+x^2)(3+3x+x^2)$
		$(4+3x+x^2)(1+4x+x^2)(2+4x+x^2)$

REFERENCES

[1] J. T. B. BEARD, JR. (1977) – *Unitary perfect polynomials over* GF (q), « Rend. Accad. Lincei », *62*, 417–422.

[2] J. T. B. BEARD, J. R. OCONNELL, JR. and K. I. WEST (1977) – *Perfect polynomials over* GF (q), « Rend. Accad. Lincei », *62*, 283–291.

[3] J. T. B. BEARD and K. I. WEST (1974) – *Factorization tables for* $x^n - 1$ *over* GF (q), « Math. Comp. », *28*, 1167–1168 + microfiche.

[4] J. T. B. BEARD and K. I. WEST – *Factorization tables for binomials over* GF (q), « Math. Comp. », to appear.

[5] J. T. B. BEARD and K. I. WEST (1976) – *Factorization tables for trinomials over* GF (q), « Math. Comp. », *30*, 179–183 + microfiche.

[6] J. T. B. BEARD and K. I. WEST – *Factorization tables for* GF [q , x], unpublished.

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

[8] A. F. LONG, JR. (1973) – *Factorization of irreducible polynomials over a finite field with the substitution* $x^{p^r} - x$ *for* x, « Duke Math. J. », *40*, 63–76.

[9] S. PERLIS (1952) – *Theory of Matrices*, Reading, Mass.