Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Jacob T.B. Jr. Beard, Mickie Sue Harbin

Non-splitting unitary perfect polynomials over GF(q)

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **66** (1979), n.3, p. 179–185.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1979_8_66_3_179_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1979.

Algebra. — *Non-splitting unitary perfect polynomials over* GF(q)[*]. Nota di JACOB T. B. BEARD Jr. e MICKIE SUE HARBIN, presentata[**] dal Socio G. ZAPPA.

RIASSUNTO. — È stata avanzata la congettura che esista un'infinità di classi distinte di p^d equivalenza di polinomi perfetti unitari irriducibili su GF (p^d) per ogni primo p e ogni intero dispari d > 1. La congettura è dimostrata vera nei casi i) $p < 97$, ii) $2 \in$ GF (p) non è un quadrato, iii) $2 \in$ GF (p) è un quadrato e tutti gli intervalli interi positivi determinati da potenze distinte dispari di θ^t contiene un quadrato, ove GF* $(p) = \langle\theta\rangle$. Inoltre, si è determinato che iii) è soddisfatto da 314 primi $p > 97$.

1. *Introduction and notation.* This note continues the study of unitary perfect polynomials begun in [2], [3] and pursues the conjecture [3] that the number NSUP(p^d) of distinct p^d-equivalence classes of non-splitting unitary perfect polynomials over GF (p^d) is infinite for each prime p and each odd integer $d > 1$. The truth of the conjecture for $p \leq 5$ was established in [3], while Harbin [7] has recently constructed examples which confirm it for each $p \leq 19$. These last examples have led to the theoretical results of this paper. The one not covered by the general theory $(p = 17)$ is given in Section 3 (3.4), and other pertinent examples constructed by Harbin appear in Table I (Section 4). Recall that from [3; Theorem 4], NSUP $(p) > 0$ implies NSUP $(p^d) = \infty$ for each odd $d > 1$ whenever there exists a non-splitting unitary perfect polynomial over GF (p) whose prime factors in GF $[p, x]$ have degrees powers of 2. The basic results of this paper are techniques for constructing some such polynomials, and the conjecture is established in the affirmative to the extent of

THEOREM 1. NSUP $(p) > 0$ *and* NSUP $(p^d) = \infty$ *for each odd integer* $d > 1$ *whenever* p *satisfies one of the following*:

i) $p < 97$,

ii) $p = 2^e t + 1$ *with* $(2, t) = 1$ *and* $e \leq 2$,

iii) $p = 2^e t + 1$ *with* $(2, t) = 1, e \geq 3$, *and each integer interval* $[\theta^\tau, \theta^{\tau'}]$ *contains a square in* GF (p), *where* GF* $(p) = \langle\theta\rangle$ *and* $\theta^\tau, \theta^{\tau'}$ *are distinct odd powers of* θ^t.

In Section 2 we prove ii), which together with [3; Theorem 5 $(p = 2)$] establishes i) with the exceptions $p = 17, 41, 73, 89$. A proof of iii) is outlined in Section 3 and it is noted that $p = 41, 73, 89$ satisfy the condition of iii).

[*] This research was partially supported by Organized Research Grants from the University of Texas at Arlington. Written while the first author was visiting at Emory University, Atlanta, GA 30322.

[**] Nella seduta del 13 gennaio 1979.

Briefly, our terminology remains that of [2]. For monic polynomials $A , B \in GF [q , x] , q = p^d , d \geq 1$, B is called a *unitary divisor* of A whenever $(B , A/B) = 1$. The polynomial $A \in GF [q , x]$ is *unitary perfect* over GF (q) provided the sum $\sigma^* (A)$ of the distinct unitary divisors in GF $[q , x]$ of A equals A. In general, we write $A \rightarrow B$ to indicate $\sigma^* (A) = B$. A *non-splitting* polynomial over GF (q) is a monic polynomial over GF (q) which does not factor in GF $[q , x]$ as a product of linear irreducibles. Monic irreducibles $P , Q \in GF [q , x]$ are called *primes*. For any $A , B \in GF [q , x]$, we say A is *q-equivalen* to B if and only if $A = B^{p^l}$ for some integer l, where $q = p^d$, $d \geq 1$ [3].

The proof techniques are motivated by [2; Theorem 8] and the algorithm [3] used to construct some of our examples. They hinge on the following fact [3]. Let $B (x) \in GF [q , x]$ have the canonical decomposition $B (x) = \prod_{i=1}^{r} P_i^{\alpha(i)} (x)$ as the product of positive powers of distinct primes $P_i (x) \in GF [q , x]$. Then if $A (x) \rightarrow B (x)$ and $b \in GF (q)$, we have

$$A (x + b) \rightarrow B (x + b) = \prod_{i=1}^{r} P_i^{\alpha(i)} (x + b) , \tag{1.1}$$

and the factorization on the right of (1.1) is the canonical decomposition of $B (x + b)$ in GF $[q , x]$. I.e., the polynomials $Q_i (x) = P_i (x + b) \in GF [q , x]$ are distinct primes. Finally, recall that σ^* is multiplicative and, for powers of primes, that $\sigma^* (P^\alpha) = P^\alpha + 1$.

2. *When 2 is not a square*. Since Theorem 1 is true for $p = 2$ [3], we assume hereafter that $p > 2$. Let $p - 1 = 2^e t , (2 , t) = 1 , e \geq 1$, and let GF $(p) = \{0 , 1 , \cdots , p - 1\}$ be represented by the integers *modulo p*. We let GF$^* (p)$ denote the multiplicative group of non-zero elements of GF (p), and find it convenient to " order " the elements of GF (p) under their natural ordering as integers. We first consider the case $e = 1$, a necessary and sufficient condition that -1 is not a square in GF (p).

THEOREM 2. NSUP $(p) > 0$ *whenever* -1 *is not a square in* GF (p).

Proof. Since one-half of the elements of GF$^* (p)$ are squares, let k be the smallest positive integer such that $-(k + 1)$ is a square in GF (p). Then $x^2 + 1 , \cdots , x^2 + k$ are prime in GF $[p , x]$ and $x^2 + k + 1 = (x + a) (x + b)$ for some $a , b \in GF (p)$. Thus we have the canonical decompositions exhibited in

$$x^2 (x^2 + 1) \cdots (x^2 + k) \rightarrow (x + a) (x + b) (x^2 + 1) \cdots (x^2 + k) . \tag{2.1}$$

By (1.1), from (2.1) we have for $0 \leq i \leq p - 1$,

$$(x - i)^2 \prod_{j=1}^{k} [(x - i)^2 + j] \rightarrow (x - i + a) (x - i + b) \prod_{j=1}^{k} [(x - i)^2 + j]. \tag{2.2}$$

Since the quadratic primes $(x-i_1)^2+j_1$ and $(x-i_2)^2+j_2$ are distinct unless $i_1=i_2$ and $j_1=j_2$, and evidently $\prod_{i=0}^{p-1}(x-i)^2=\prod_{i=0}^{p-1}(x-i+a)(x-i+b)$, then the polynomial $f(x)$ having canonical decomposition given by

$$f(x)=\prod_{i=0}^{p-1}\prod_{j=0}^{k}[(x-i)^2+j] \tag{2.3}$$

is a non-splitting unitary perfect polynomial over $GF(p)$ (having precisely linear and quadratic prime factors).

The general case when -1 is a square in $GF(p)$, i.e., $e\geq 2$, is comprised of two natural subcases, $e=2$ (2 is not a square in $GF(p)$) and $e\geq 3$ (2 is a square in $GF(p)$), by virtue of the proof of

THEOREM 3. $NSUP(p)>0$ *whenever* $p-1=4t$, $(2,t)=1$.

Proof. Let θ be a primitive root *modulo* p, i.e., $GF^*(p)=\langle\theta\rangle$, and consider the canonical decompositions on the left and extreme right of

$$x^4\to x^4+1=x^4-\theta^{2t}=(x^2+\theta^t)(x^2+\theta^{3t})\,. \tag{2.4}$$

It will become clear that we may assume $2\leq\theta^t<\theta^{3t}\leq p-2$.

Case I. Assume that no square in $GF^*(p)$ lies between θ^t and θ^{3t}, and let $k=\theta^{3t}-\theta^t-1$. Then $x^2+\theta^t+l$ is prime for each l, $0\leq l\leq k$, and using (2.4) we have

$$x^4\prod_{l=0}^{k}(x^2+\theta^t+l)(x^2+\theta^{3t})^2\to[(x^2+\theta^{3t})^2+1]\cdot \prod_{l=0}^{k}(x^2+\theta^t+l)(x^2+\theta^{3t})^2\,. \tag{2.5}$$

Both sides of (2.5) are completely factored over $GF(p)$ excepting

$$(x^2+\theta^{3t})^2+1=(x^2+\theta^{3t}+\theta^t)(x^2+\theta^{3t}-\theta^t)=x^2(x^2-2\,\theta^t)\,, \tag{2.6}$$

and we examine $x^2-2\,\theta^t$. Since $(2/p)=(-1)^{(p^2-1)/8}=-1$ [1], 2 is a non-square in $GF(p)$, so that the product $2\,\theta^t$ is a square in $GF(p)$. Thus for some e_1, e_2 (2.6) becomes

$$(x^2+\theta^{3t})^2+1=x^2(x+\theta^{e_1})(x+\theta^{e_2})\,. \tag{2.7}$$

Hence (2.5) becomes

$$x^4\prod_{l=0}^{k}(x^2+\theta^t+l)(x^2+\theta^{3t})^2\to \to x^2(x+\theta^{e_1})(x+\theta^{e_2})\prod_{l=0}^{k}(x^2+\theta^t+l)(x^2+\theta^{3t})^2\,, \tag{2.8}$$

both sides of (2.8) now completely factored in $GF[p,x]$. From (1.1), the distinctness of the translates by i, $0 \leq i \leq p - 1$, of the quadratic primes in (2.8) (consider the coefficients of x), and $\prod_{i=0}^{p-1} (x-i)^4 = \prod_{i=0}^{p-1} (x-i)^2$ $(x - i + \theta^{e_1})(x - i + \theta^{e_2})$, the polynomial $f(x)$ with the canonical decomposition given by

$$(2.9) \qquad f(x) = \prod_{i=0}^{p-1} \prod_{l=0}^{k} (x-i)^4 [(x-i)^2 + \theta^t + l] [(x-i)^2 + \theta^{3t}]^2$$

is unitary perfect over GF (p).

Case II. Now assume that some square $a \in \text{GF}(p)$ satisfies $\theta^t < a < \theta^{3t}$. Let k_1, k_3 be the smallest positive integers such that $\theta^t + k_1 + 1$, $\theta^{3t} + k_3 + 1$ are squares in GF* (p) (recall $p - 1$ is a square), say

$$(2.10) \qquad x^2 + \theta^t + k_1 + 1 = x^2 - \theta^{2e_1} = (x + \theta^{e_1})(x + \theta^{2t+e_1}),$$

$$(2.11) \qquad x^2 + \theta^{3t} + k_3 + 1 = x^2 - \theta^{2e_3} = (x + \theta^{e_3})(x + \theta^{2t+e_3}).$$

From (2.4), (2.10), (2.11) we have

$$(2.12) \qquad x^4 \prod_{j=0}^{k_1} (x^2 + \theta^t + j) \prod_{l=0}^{k_3} (x^2 + \theta^{3t} + l) \rightarrow$$

$$(x + \theta^{e_1})(x + \theta^{2t+e_1})(x + \theta^{e_3})(x + \theta^{2t+e_3}) \prod_{j=0}^{k_1} (x^2 + \theta^t + j) \prod_{l=0}^{k_3} (x^2 + \theta^{3t} + l).$$

Arguing as before, the polynomial $f(x)$ with canonical decomposition given by

$$(2.13) \qquad f(x) = \prod_{i=0}^{p-1} (x-i)^4 \prod_{j=0}^{k_1} ([x-i)^2 + \theta^t + j] \prod_{l=0}^{k_3} [(x-i)^2 + \theta^{3t} + l]$$

is unitary perfect over GF (p).

3. *When 2 is a square.*

A partial generalization of Theorem 3 is available as indicated by the proof of Case II.

THEOREM 4. NSUP $(p) > 0$ *whenever* $p - 1 = 2^e t$ *with* $(2, t) = 1$, $e \geq 3$, *and each positive integer interval* $[\theta^{\tau}, \theta^{\tau'}]$ *contains a square in* GF (p), *where* GF* $(p) = \langle\theta\rangle$ *and* θ^{τ}, $\theta^{\tau'}$ *are distinct odd powers of* θ^t.

Proof. The condition of the theorem is equivalent to asking that each integer interval $[\theta^{\tau(j)}, \theta^{\tau(j+1)}]$ contain a square, $1 \leq j \leq 2^{e-1} - 1$ where $\theta^{\tau(1)} < \cdots < \theta^{\tau(2^{e-1})}$ is the natural ordering of the odd powers of θ^t as positive integers. Base the argument indicated by the proof of Theorem 3, Case II on the canonical decomposition of $\sigma^*(x^{2^e}) = x^{2^e} + 1$ given by

$$(3.1) \qquad x^{2^e} \rightarrow x^{2^e} + 1 = \prod_{j=1}^{2^e-1} (x^2 + \theta^{jt}), \qquad j \text{ odd}.$$

One obtains a unitary perfect polynomial $f(x)$ over GF (p) whose canonical decomposition has the form given by

$$f(x) = \prod_{i=0}^{p-1} (x-i)^{2^e} \prod_{j=1}^{2^e-1} \prod_{l=0}^{k_j} [(x-i)^2 + \theta^{jt} + l], \quad j \quad \text{odd.} \tag{3.2}$$

The complete factorization of $x^{16}+1$ in GF $[17, x]$,

$$x^{16}+1 = (x^2+3)(x^2+5)(x^2+6)(x^2+7)(x^2+10)(x^2+11)\cdot (x^2+12)(x^2+14), \tag{3.3}$$

indicates some of the difficulties encountered when 2 is a square in GF (p) and the odd powers of θ^{τ} are not interlaced with squares. This particular gap in the theory is filled by the unitary perfect $f(x) \in$ GF $[17, x]$ of degree 153 having the canonical decomposition given by

$$f(x) = \prod_{i=0}^{16} (x-i)^3 \prod_{l=1}^{3} [(x-i)^2 + 16(x-i) + l]. \tag{3.4}$$

To conclude our proof of Theorem 1, we note that $41 = 2^3 \cdot 5 + 1$, $73 = 2^3 \cdot 9 + 1$, and $89 = 2^3 \cdot 11 + 1$ fulfill the hypothesis of Theorem 4: for $x^8 + 1 = (x^2+3)(x^2+14)(x^2+27)(x^2+38) \in$ GF $[41, x]$ we have "the" squares $4, 16, 31, 39 \in$ GF (41); for $x^8+1 = (x^2+10)(x^2+22)(x^2+51)$ $(x^2+63) \in$ GF $[73, x]$ "the" squares $12, 23, 54, 64 \in$ GF (73); and for $x^8+1 = (x^2+12)(x^2+37)(x^2+52)(x^2+77) \in$ GF $[89, x]$ "the" squares $16, 39, 53, 78 \in$ GF (89).

4. *Remarks and examples.* The extent of the primes p which satisfy the condition of Theorem 4 is not known, though we hesitantly conjecture that for each fixed $e \geq 3$ there exists an integer t_e such that $p = 2^e t + 1$ satisfies the condition for all odd admissible $t > t_e$(*). A computer study of 338 cases run on a Univac 90/80 at Emory University using input data from [8] shows the condition to be satisfied for the given values of e and admissible $t \geq 3$ excluding the 21 exceptional values of $t \geq 3$ for which the condition fails:

e	*Admissible* $t \geq 3$	*Exceptional values of t*
3	$t \leq 1,251$	none
4	$t \leq 603$	none
5	$t \leq 365$	3, 11, 29
6	$t \leq 465$	3, 75, 229, 247, 337, 423, 429
7	$t \leq 167$	5, 9, 11, 21, 35, 75, 89, 105, 119, 125, 165

(*) Added at galley: Beard, J. K. Doyle, and K. I. Mandelberg have recently proved that $t_3 = 1$.

The condition fails to be satisfied whenever $t = 1$, since the number of pairs of consecutive quadratic non-residues is positive for $p > 3$ [1 ; p. 132].

The examples in Table I of non-splitting unitary perfect polynomials over GF (p) were obtained by Harbin using [4]-[6], and are representatives of p-equivalence classes distinct from those in [3] and those determined by the proof of Theorem 1. The totality of these examples and theory now establish NSUP $(5) \geq 7$, NSUP $(7) \geq 3$, NSUP $(11) \geq 2$, with NSUP $(2) \geq 33$ and NSUP $(3) \geq 16$ unchanged since [3] to our knowledge.

TABLE I

Some New Non-splitting Unitary Perfect $\bar{p}$-Class Representatives.

p	DEGREE	COMPLETE FACTORIZATION
7	105	$x^5 (1 + x)^5 (2 + x)^5 (3 + x)^5 (4 + x)^5 (5 + x)^5 (6 + x)^5 (4 + x^2)$ $(6 + x + x^2) (5 + 2x + x^2) (1 + 3x + x^2) (1 + 4x + x^2)$ $(5 + 5x + x^2) (6 + 6x + x^2) (4 + 2x + 5x^2 + x^4) (5 + 2x + 5x^2 + x^4)$ $(2 + 5x + x^2 + x^3 + x^4) (3 + 5x + x^2 + x^3 + x^4)$ $(5 + 4x + 3x^2 + 2x^3 + x^4) (6 + 4x + 3x^2 + 2x^3 + x^4)$ $(1 + 2x + 4x^2 + 3x^3 + x^4) (2 + 2x + 4x^2 + 3x^3 + x^4)$ $(5 + 2x + 4x^2 + 4x^3 + x^4) (6 + 2x + 4x^2 + 4x^3 + x^4)$ $(3 + 3x^2 + 5x^3 + x^4) (4 + 3x^2 + 5x^3 + x^4) (1 + 6x + x^2 + 6x^3 + x^4)$ $(2 + 6x + x^2 + 6x^3 + x^4)$
	224	$x^6 (1 + x)^6 (2 + x)^6 (3 + x)^6 (4 + x)^6 (5 + x)^6 (6 + x)^6 (1 + x^2)^3$ $(2 + x^2)^2 (4 + x^2)^2 (3 + x + x^2)^3 (4 + x + x^2)^2 (6 + x + x^2)^2$ $(2 + 2x + x^2)^3 (3 + 2x + x^2)^2 (5 + 2x + x^2)^2 (1 + 3x + x^2)^2$ $(5 + 3x + x^2)^3 (6 + 3x + x^2)^2 (1 + 4x + x^2)^2 (5 + 4x + x^2)^3$ $(6 + 4x + x^2)^2 (2 + 5x + x^2)^3 (3 + 5x + x^2)^2 (5 + 5x + x^2)^2$ $(3 + 6x + x^2)^3 (4 + 6x + x^2)^2 (6 + 6x + x^2)^2 (3 + x^2 + x^4)$ $(5 + 4x^2 + x^4) (6 + 4x^2 + x^4) (2 + 6x + x^3 + x^4) (3 + 6x + x^3 + x^4)$ $(2 + x + 4x^2 + x^3 + x^4) (3 + x + 2x^2 + 2x^3 + x^4)$ $(4 + x + 2x^2 + 2x^3 + x^4) (2 + 5x + 6x^2 + 2x^3 + x^4)$ $(5 + x + 3x^3 + x^4) (3 + 2x + 3x^2 + 3x^3 + x^4)(4 + 2x + 3x^2 + 3x^3 + x^4)$ $(5 + 6x + 4x^3 + x^4)(3 + 5x + 3x^2 + 4x^3 + x^4) (4 + 5x + 3x^2 + 4x^3 + x^4)$ $(3 + 6x + 2x^2 + 5x^3 + x^4) (4 + 6x + 2x^2 + 5x^3 + x^4)$ $(2 + 2x + 6x^2 + 5x^3 + x^4) (2 + x + 6x^3 + x^4) (3 + x + 6x^3 + x^4)$ $(2 + 6x + 4x^2 + 6x^3 + x^4)$
11	55	$x^3 (1 + x)^3 (2 + x)^3 (3 + x)^3 (4 + x)^3 (5 + x)^3 (6 + x)^3 (7 + x)^3$ $(8 + x)^3 (9 + x)^3 (10 + x)^3 (9 + x^2) (1 + x + x^2) (10 + 2x + x^2)$ $(3 + 3x + x^2) (2 + 4x + x^2) (7 + 5x + x^2) (7 + 6x + x^2)$ $(2 + 7x + x^2) (3 + 8x + x^2) (10 + 9x + x^2) (1 + 10x + x^2)$

REFERENCES

[1] G. E. ANDREWS (1971) – *Number Theory*, Philadelphia.

[2] J. T. B. BEARD, Jr. (1977) – *Unitary perfect polynomials over* GF (q), « Rend. Acc. Naz. Lincei », Series VIII, Vol. LXII, 417–422.

[3] J. T. B. BEARD, Jr., A. T. BULLOCK and M. S. HARBIN (1977) – *Infinitely many perfect and unitary perfect polynomials*, « Rend. Acc. Naz. Lincei », Series VIII, Vol. LXII, 294–303.

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

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

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

[7] M. S. HARBIN (1978) – *Non-splitting unitary perfect polynomials over* GF (p), $7 \leq p \leq 19$ « A. M. S. Notices », *25*, A–351.

[8] A. E. WESTERN and J. C. P. MILLER (1968) – *Tables of Indices and Primitive Roots*, « Royal Society Mathematical Tables », *9*, Cambridge.