

## Perfect Polynomials Revisited

By J. T. B. BEARD, Jr. (Cookeville)\*

**Abstract.** Earlier it was shown that every splitting polynomial  $A = (x^p - x)^{Np^n - 1}$  with  $N|(p-1)$ ,  $n \geq 0$  is perfect over  $GF(p)$ ; i.e., the sum  $\sigma(A)$  of the distinct monic divisors of  $A$  over  $GF(p)$  equals  $A$ . Conversely, it was proved in detail that whenever a splitting polynomial  $A = \prod_{i=0}^{p-1} (x - i)^{N(i)p^{n(i)} - 1}$  is perfect over  $GF(p)$  then the  $N(i)|(p-1)$  and  $n(0) = \dots = n(p-1)$ ; and it was claimed (as already proved by CANADAY for  $p = 2$ ) that  $N(0) = \dots = N(p-1)$ . This note verifies the claim in detail, via an argument on the level divisors of  $A$ . In the process, an equivalence relation is exhibited on the set of splitting perfect polynomials over  $GF(p)$  and an intriguing multinomial identity *modulo*  $p$  is discovered.

In [1] it was shown that every splitting polynomial  $A = (x^p - x)^{Np^n - 1}$  with  $N|(p-1)$ ,  $n \geq 0$  is perfect over  $GF(p)$ . I.e., the sum  $\sigma(A)$  of the distinct monic divisors of  $A$  over  $GF(p)$  equals  $A$ . Conversely, it was proved in detail that whenever a splitting polynomial  $A = \prod_{i=0}^{p-1} (x - i)^{N(i)p^{n(i)} - 1}$  is perfect over  $GF(p)$ , then the  $N(i)|(p-1)$  and  $n(0) = \dots = n(p-1)$ ; and it was claimed (as proved by CANADAY [5] for  $p = 2$ ) that  $N(0) = \dots = N(p-1)$ . The purpose of this note is to verify the claim in detail, via an argument on the level divisors (to be defined) of  $A$ . In the process we exhibit an equivalence relation on the set of splitting perfect polynomials over  $GF(p)$  and discover an intriguing multinomial identity *modulo*  $p$ .

**Theorem 1.** Let  $A = \prod_{i=0}^{p-1} (x - i)^{N(i)p^n - 1}$  be perfect over  $GF(p)$ , with  $p$  odd and  $n \geq 0$ . Then  $N(0) = \dots = N(p-1)$ .

---

\*Written while visiting at the University of Tennessee-Knoxville.

PROOF. First, note that each polynomial  $A = \prod_{i=0}^{p-1} (x-i)^{N(i)p^n-1}$  has a unique description of the form  $A = A(N(0), \dots, N(p-1); n)$ . Thus for any  $n \geq 0$  and all sequences  $N(0), \dots, N(p-1)$ ,

$$\begin{aligned} A &= A(N(0), \dots, N(p-1); n) = \prod_{i=0}^{p-1} \frac{(x-i)^{N(i)p^n}}{(x-i)} = \\ &= \prod_{i=0}^{p-1} \frac{(x-i)^{N(i)p^n} (x-i)^{p^n-1}}{(x-i)^{p^n}} = \\ &= \left( \prod_{i=0}^{p-1} (x-i)^{N(i)-1} \right)^{p^n} (x^p - x)^{p^n-1} = \\ &= [A(N(0), \dots, N(p-1); 0)]^{p^n} (x^p - x)^{p^n-1}. \end{aligned}$$

Moreover, since  $\sigma$  is multiplicative and  $\sigma((x-i)^{N(i)p^n-1}) = \frac{(x-i)^{N(i)p^n-1}}{x-i-1}$  we find

$$\begin{aligned} \sigma(A(N(0), \dots, N(p-1); n)) &= \prod_{i=0}^{p-1} \frac{(x-i)^{N(i)p^n} - 1}{x-i-1} = \\ &= \prod_{i=0}^{p-1} \left\{ \frac{(x-i)^{N(i)p^n} - 1}{(x-i-1)^{p^n}} \cdot \frac{(x-i-1)^{p^n}}{(x-i-1)} \right\} = \\ &= \left\{ \prod_{i=0}^{p-1} \frac{(x-i)^{N(i)} - 1}{(x-i) - 1} \right\}^{p^n} (x^p - x)^{p^n-1} = \\ &= \{\sigma(A(N(0), \dots, N(p-1); 0))\}^{p^n} (x^p - x)^{p^n-1}. \end{aligned}$$

Thus  $A(N(0), \dots, N(p-1); n)$  and  $A(N(0), \dots, N(p-1); 0)$  are simultaneously perfect, and it suffices to prove the equalities  $N(0) = \dots = N(p-1)$  in the case  $n = 0$ .

Accordingly, consider a perfect polynomial  $B = \prod_{i=0}^{p-1} (x-i)^{N(i)-1} \neq 1$  over  $GF(p)$ , and let  $m = \min\{N(i)\}$ . Since at least  $p$  distinct primes divide every nontrivial perfect polynomial over  $GF(p)$  [1; Theorem 6], then  $m \geq 2$  and we may write

$$B = (x^p - x)^{m-1} \prod_{N(i) > m} (x-i)^{N(i)-m} = B_m \prod_{N(i) > m} (x-i)^{N(i)-m}.$$

Let  $B^{(l)}$  denote the sum of all distinct (monic) divisors of  $B$  whose degrees equal  $\deg B - l$ , and call  $B^{(l)}$  a *level- $l$  summand* of  $\sigma(B)$ . Also, let  $\rho_i B^{(l)}$  denote the elementary symmetric function on the roots of  $B^{(l)}$  taken  $i$  at a time; and let  $\tau B^{(l)}$  be the number of distinct summands of  $B^{(l)}$ , i.e., the number of distinct *level- $l$  divisors* of  $B$ . Note that whenever  $\deg D = l$  and  $l \leq m - 1$ , then  $D|B$  if and only if  $D|B_m$ . Thus whenever  $1 \leq l \leq m - 1$ , the level- $l$  summands of  $\sigma(B)$  and  $\sigma(B_m)$  are related by

$$B^{(l)} = \sum_{\substack{\deg D=l \\ D|B}} \frac{B}{D} = \sum_{\substack{\deg D=l \\ D|B_m}} \frac{B}{D} = \frac{B}{B_m} \sum_{\substack{\deg D=l \\ D|B_m}} \frac{B_m}{D} = \frac{B}{(x^p - x)^{m-1}} B_m^{(l)}.$$

As before [1; Theorem 3],  $m \mid (p - 1)$  and  $B_m$  is perfect, so that

$$\sum_{l=1}^{(m-1)p} B_m^{(l)} = \sigma(B_m) - B_m = 0,$$

from which

$$\begin{aligned} \sum_{l=1}^{m-1} B^{(l)} &= \frac{B}{(x^p - x)^{m-1}} \sum_{l=1}^{m-1} B_m^{(l)} - \frac{B}{(x^p - x)^{m-1}} \sum_{l=1}^{(m-1)p} B_m^{(l)} = \\ &= - \frac{B}{(x^p - x)^{m-1}} \sum_{l=m}^{(m-1)p} B_m^{(l)}. \end{aligned}$$

Now consider  $\deg \sum_{l=m}^{(m-1)p} B_m^{(l)} \leq \deg B_m^{(m)}$ . Since  $B_m = \prod_{i=0}^{p-1} (x - i)^{m-1}$ , then every summand  $C$  of  $B_m^{(m)}$  satisfies

$$C = \frac{B_m}{x^{\lambda_0} (x - 1)^{\lambda_1} \cdots (x - p + 1)^{\lambda_{p-1}}}$$

where  $m = \lambda_0 + \cdots + \lambda_{p-1}$  and  $0 \leq \lambda_i \leq m - 1$  for  $0 \leq i \leq p - 1$ . I. e., there are precisely  $p$  fewer summands  $C$  of  $B_m^{(m)}$  than there are increasing words of length  $m$  on the ordered letters  $x < \cdots < x - p + 1$ . The latter have been enumerated [4; p.23] as  $[p]^m / m! = p(p + 1) \cdots (p + m - 1) / m!$ . Since  $m \leq p - 1$  then  $\tau B_m^{(m)} = [p]^m / m! - p \equiv 0 \pmod{p}$ , so that  $\deg B_m^{(m)} \leq (m - 1)p - (m + 1)$ .

From this,

$$\deg \sum_{l=1}^{m-1} B^{(l)} \leq [\deg B - (m-1)p] + [(m-1)p - (m+1)] < \deg B - m$$

and  $\sum_{\substack{i+l=m \\ 1 \leq l < m}} \rho_i B^{(l)} = 0$ . Thus  $\tau B^{(m)} \equiv 0 \pmod{p}$  since  $\sigma(B) - B = 0$ . To

find  $k = |\{i : N(i) = m\}|$  and complete the proof, we determine  $\tau B^{(m)}$ . Suppose  $C$  is an arbitrary summand of  $B^{(m)}$ . There are precisely  $(p-k)$  summands  $C = B/(x-j)^m$  of  $B^{(m)}$ , and all others are those previously displayed for  $B_m^{(m)}$ . Hence  $\tau B^{(m)} = (p-k) + [p]^m/m! - p \equiv -k \pmod{p}$ . Since  $1 \leq k \leq p$  and  $\tau B^{(m)} \equiv 0 \pmod{p}$ , then  $k = p$ .  $\square$

By the opening remarks in the proof of Theorem 1, every perfect splitting polynomial over  $GF(p)$  has the form  $A = ((x^p - x)^{N-1})^{p^n} \cdot (x^p - x)^{p^n-1}$ , displaying an analog of Euler's characterization of the even perfect numbers. More important, this form displays an equivalence relation on the set of all splitting perfect polynomials over  $GF(p)$ , whose classes,  $\tau(p-1)$  in number, have minimal elements  $C_N = (x^p - x)^{N-1}$ . I.e., call the splitting perfect polynomials  $A, B$  over  $GF(p)$   $\sigma$ -equivalent, and write  $A \sim_\sigma B$ , if there exist integers  $N|(p-1)$  and  $n, m \geq 0$  such that

$$A = (C_N)^{p^n} (x^p - x)^{p^n-1} \quad \text{and} \quad B = (C_N)^{p^m} (x^p - x)^{p^m-1}.$$

(This equivalence relation  $\sim_\sigma$  should not be confused with that defined for unitary perfect polynomials [2].) By Theorem 1 itself, an arbitrary splitting perfect polynomial over  $GF(p)$  can be appropriately denoted  $A(N, n) = ((x^p - x)^{N-1})^{p^n} (x^p - x)^{p^n-1}$ , and our next result is evident.

**Theorem 2.** *Let  $A(N, n), B(M, m)$  be splitting perfect polynomials over  $GF(p)$ . Then  $A(N, n) \sim_\sigma B(M, m)$  if and only if  $N = M$ . Whenever  $A(N, n) \sim_\sigma B(M, m)$ , then  $B|A$  if and only if  $m|n$ .*

The concept of level- $l$  divisors of polynomials becomes interesting in its own right. Early on, we suspicioned our proof (Theorem 1) to be weak that  $\sum_{\substack{i+l=N \\ 1 \leq l < N}} \rho_i B^{(l)} = 0$ , now writing  $B = B(N, 0)$  as just described. Using

iterated sums and formal derivatives to manipulate  $B^{(l)}$ , for  $1 \leq l \leq 3 < N$  we established

$$(1) \quad \deg B(N, 0)^{(l)} = \deg B(N, 0) - lp$$

from

$$(2) \quad B^{(l)} = \frac{(-1)^l B}{(x^p - x)^l},$$

which is equivalent to

$$(3) \quad \sum_{\substack{\lambda_0 + \dots + \lambda_{p-1} = l \\ 0 \leq \lambda_i \leq l}} \frac{1}{x^{\lambda_0} (x-1)^{\lambda_1} \dots (x-p+1)^{\lambda_{p-1}}} = \\ = (-1)^l \sum_{\substack{\lambda_0 + \dots + \lambda_{p-1} = l \\ 0 \leq \lambda_i \leq l}} \frac{l!}{\lambda_0! \dots \lambda_{p-1}!} \cdot \frac{1}{x^{\lambda_0} (x-1)^{\lambda_1} \dots (x-p+1)^{\lambda_{p-1}}}$$

by the multinomial expansion [4] of  $(y_0 + \dots + y_{p-1})^l$  with  $y_i = 1/(x-i)$ , both sides of (3) yielding  $B^{(l)}$  when multiplied by  $B$ . Proofs of our conjecture that (1)–(3) hold for  $1 \leq l \leq N-1$  have been given independently by MARSHALL BUCK and the referee, to whom we acknowledge our appreciation. The upcoming proof of (2) for  $1 \leq l \leq N-1 < p$  succinctly handles the intricacies displayed when  $l = 3 < N$ :

$$\begin{aligned} 6B^{(3)} &= 6 \sum_{0 \leq j_1 \leq j_2 \leq j_3 \leq p-1} \frac{B}{(x-j_1)(x-j_2)(x-j_3)} = \\ &= \sum_{j_1=0}^{p-1} \sum_{j_2=0}^{p-1} \sum_{j_3=0}^{p-1} \frac{B}{(x-j_1)(x-j_2)(x-j_3)} + \\ &\quad + 3 \sum_{j_1=0}^{p-1} \sum_{j_2=0}^{p-1} \frac{B}{(x-j_1)(x-j_2)^2} + 2 \sum_{j=0}^{p-1} \frac{B}{(x-j)^3} = \\ &= B \sum_{j_1=0}^{p-1} \frac{1}{(x-j_1)} \sum_{j_2=0}^{p-1} \frac{1}{(x-j_2)} \sum_{j_3=0}^{p-1} \frac{1}{(x-j_3)} + \\ &\quad + 3B \sum_{j_1=0}^{p-1} \frac{1}{(x-j_1)} \sum_{j_2=0}^{p-1} \frac{1}{(x-j_2)^2} + 2B \sum_{j=0}^{p-1} \frac{1}{(x-j)^3} = \end{aligned}$$

$$\begin{aligned}
&= -\frac{B}{(x^p - x)^3} - 3B \left( \frac{1}{x^p - x} \right) \left( \frac{1}{(x^p - x)^2} \right) + \\
&\quad + 2B \sum_{j=0}^{p-1} D_x \left[ \frac{-1}{2(x-j)^2} \right] = \\
&= -\frac{4B}{(x^p - x)^3} - 2B \left( D_x \left[ \sum_{j=0}^{p-1} \frac{1}{2(x-j)^2} \right] \right) = \\
&= -\frac{4B}{(x^p - x)^3} - B \cdot D_x \left[ \frac{1}{(x^p - x)^2} \right] = \\
&= -\frac{4B}{(x^p - x)^3} - \frac{2B}{(x^p - x)^3} = \\
&= 6 \frac{-B}{(x^p - x)^3}.
\end{aligned}$$

Notice that  $N|(p-1)$  is not used in these arguments, only that  $1 \leq l \leq N \leq p-1$ .

The pertinent result for formal derivatives over  $GF(p)$  is this

**Lemma.** For any prime  $p$  and all integers  $l \geq 1$ ,

$$\sum_{j=0}^{p-1} \frac{1}{(x-j)^l} = \frac{(-1)^l}{(x^p - x)^l}.$$

PROOF. We argue by induction on  $l$ . From the Product Rule, when  $l = 1$  we have

$$\sum_{j=0}^{p-1} \frac{1}{(x-j)} = \frac{D_x \left[ \prod_{j=0}^{p-1} (x-j) \right]}{x^p - x} = \frac{D_x [x^p - x]}{x^p - x} = \frac{-1}{x^p - x}.$$

Assume the result is true for some integer  $l \geq 1$ . Then

$$\begin{aligned}
\sum_{j=0}^{p-1} \frac{1}{(x-j)^{l+1}} &= \sum_{j=0}^{p-1} D_x \left[ \frac{-1}{l(x-j)^l} \right] = \frac{-1}{l} D_x \left[ \sum_{j=0}^{p-1} \frac{1}{(x-j)^l} \right] = \\
&= \frac{-1}{l} D_x \left[ \frac{(-1)^l}{(x^p - x)^l} \right] = \frac{(-1)^{l+1}}{(x^p - x)^{l+1}}. \quad \square
\end{aligned}$$

**Theorem 3.** Let  $B = (x^p - x)^{N-1} \in GF[p, x]$ . Whenever  $1 \leq l \leq N - 1 < p$ ,

$$B^{(l)} = \frac{(-1)^l B}{(x^p - x)^l}.$$

PROOF. Let  $M_l$  denote the set of all non-increasing sequences  $\{i_1, \dots, i_r\}$  of positive integers which partition  $l$ , and let  $\prec$  be any linear order on  $M_l$ . Then whenever  $1 \leq l \leq N - 1$ , there exist positive integers  $c_{i_1, \dots, i_r}$  such that  $l!B^{(l)}$  has the common values

$$\begin{aligned} (4) \quad B \sum_{\substack{\lambda_0 + \dots + \lambda_{p-1} = l \\ 0 \leq \lambda_i \leq l}} \frac{l!}{x^{\lambda_0} (x-1)^{\lambda_1} \dots (x-p+1)^{\lambda_{p-1}}} = \\ = B \sum_{\{i_1, \dots, i_r\} \in M_l} c_{i_1, \dots, i_r} \sum_{j_1=0}^{p-1} \sum_{j_2=0}^{p-1} \dots \sum_{j_r=0}^{p-1} \frac{1}{(x-j_1)^{i_1} (x-j_2)^{i_2} \dots (x-j_r)^{i_r}} \end{aligned}$$

where the left-most summation on the right-hand side is due to the ordering  $\prec$  on  $M_l$ . The coefficient of  $P = \sum_{j=0}^{p-1} \frac{1}{(x-j)^l}$  in the sum on the left-hand side of (4) is  $l!$ . In the outermost sum on the right-hand side of (4), the coefficient of  $P$  is  $\sum_{\{i_1, \dots, i_r\} \in M_l} c_{i_1, \dots, i_r}$ , since we get  $P$  as a term in the iterated sum precisely when  $j_1 = \dots = j_r$ . Thus  $l! = \sum_{\{i_1, \dots, i_r\} \in M_l} c_{i_1, \dots, i_r}$ .

Hence on rewriting the right-hand side of (4) and applying the Lemma:

$$\begin{aligned} l!B^{(l)} &= B \sum_{\{i_1, \dots, i_r\} \in M_l} c_{i_1, \dots, i_r} \sum_{j_1=0}^{p-1} \frac{1}{(x-j_1)^{i_1}} \sum_{j_2=0}^{p-1} \frac{1}{(x-j_2)^{i_2}} \dots \\ &\quad \dots \sum_{j_r=0}^{p-1} \frac{1}{(x-j_r)^{i_r}} = \\ &= B \sum_{\{i_1, \dots, i_r\} \in M_l} c_{i_1, \dots, i_r} \frac{(-1)^{i_1+i_2+\dots+i_r}}{(x^p - x)^{i_1+i_2+\dots+i_r}} = \\ &= \frac{B(-1)^l}{(x^p - x)^l} (l!). \end{aligned}$$

Since  $l! \not\equiv 0 \pmod{p}$  we are done.  $\square$

In conclusion, the sum  $B_{(l)}$  of the distinct divisors of  $B$  having degrees equal to  $l$  is also of interest. Here, at the suggestion of S. MULAY we have considered the generating function  $f(y) = \prod_{i=0}^{p-1} \frac{1}{1-(x-i)y}$ , which has coefficients  $B_{(l)}$  for  $B = B(N, 0)$  and  $l \leq N - 1 < p$ . From the general coefficient  $P_t(x)$  of  $y^t$  in  $f(y)$ , one discovers that the elementary symmetric functions  $\alpha_j(x)$  in the polynomials  $x - i$  taken  $j$  at the time satisfy  $\alpha_1(x) = \cdots = \alpha_{p-2}(x) = 0$ ,  $\alpha_{p-1}(x) = -1$  and  $\alpha_p(x) = x^p - x$ . Hence  $B_{(l)} = 0$  for  $1 \leq l \leq p - 2$ .

It remains to be seen whether further study of the level divisors of polynomials might eventually yield a (conjectured [3]) characterization of those which are bi-unitary perfect.

### References

- [1] J. T. B. BEARD, JR., J. R. O'CONNELL and K. I. WEST, Perfect polynomials over  $GF(q)$ , *Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8), **62** (1977), 283-291.
- [2] J. T. B. BEARD, JR., A. T. BULLOCK and M. S. HARBIN, Infinitely many perfect and unitary perfect polynomials over  $GF(q)$ , *Atti. Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8), **63** (1977), 294-303.
- [3] J. T. B. BEARD, JR., Bi-unitary perfect polynomials over  $GF(q)$ , *Annali di Matematica pura ed applicata (IV)* CIL (1987), 61-68.
- [4] C. BERGE, Principles of Combinatorics, *New York*, 1971.
- [5] E. F. CANADAY, The sum of the divisors of a polynomial, *Duke Math. J.* **7** (1941), 721-737.

TENNESSEE TECHNOLOGICAL UNIVERSITY  
COOKEVILLE, TENNESSEE 38505, USA

(December 30, 1986)