On a Conjecture of Beard, O'Connell and West Concerning Perfect Polynomials

Luis Gallardo

Department of Mathematics
University of Brest

Paul Pollack [1,*]

Department of Mathematics
Dartmouth College

Olivier Rahavandrainy

Department of Mathematics
University of Brest

Abstract

Following Beard, O'Connell and West (1977) we call a polynomial over a finite field $\mathbf{F}_q$ *perfect* if it coincides with the sum of its monic divisors. The study of perfect polynomials was initiated in 1941 by Carlitz's doctoral student Canaday in the case $q = 2$, who proposed the still unresolved conjecture that every perfect polynomial over $\mathbf{F}_2$ has a root in $\mathbf{F}_2$. Beard, et al. later proposed the analogous hypothesis for all finite fields. Counterexamples to this general conjecture were found by Link (in the cases $q = 11, 17$) and Gallardo & Rahavandrainy (in the case $q = 4$). Here we show that the Beard-O'Connell-West conjecture fails in all cases except possibly when q is prime. When $q = p$ is prime, utilizing a construction of Link we exhibit a counterexample whenever $p \equiv 11$ or $17 \pmod{24}$. On the basis of a polynomial analog of Schinzel's Hypothesis H, we argue that if there is a single perfect polynomial over the finite field $\mathbf{F}_q$ with no linear factor, then there are infinitely many. Lastly, we prove without any hypothesis that there are infinitely many perfect polynomials over $\mathbf{F}_{11}$ with no linear factor.

Key words: Perfect polynomials, Beard-O'Connell-West Conjecture, Hypothesis H
1991 MSC: 11T06, 11T55

Preprint submitted to Elsevier *24 June 2007*

1 Introduction and Statement of Results

For polynomials with coefficients in a fixed finite field, we denote by $\sigma(\cdot)$ the polynomial analog of the usual sum of divisors function, which we define by

$$\sigma(A) := \sum_{\substack{D \mid A \\ D \text{ monic}}} D.$$

This yields an $\mathbf{F}_q[T]$-valued function which is multiplicative and whose value on powers of monic primes is given by the familiar geometric series. We call a polynomial A *perfect* if A is the sum of all its monic divisors, i.e., if $\sigma(A) = A$. For example, $T(T+1)$ is perfect over $\mathbf{F}_2$ because modulo 2,

$$\sigma(T(T+1)) = \sigma(T)\sigma(T+1) = (T+1)((T+1)+1) = T(T+1). \quad (1)$$

The study of perfect polynomials was begun by Canaday [1], who treated only the case $q = 2$. For polynomials which split into linear factors over $\mathbf{F}_2$ he gave the following criterion, which may be considered an analog of the classical Euler-form for even perfect numbers:

Proposition 1 *If A splits over $\mathbf{F}_2$, then A is perfect if and only if $A = (T(T+1))^{2^n-1}$ for some positive integer n.*

Our example (1) is of course the case $n = 1$.

The distribution of non-splitting perfect polynomials is far more mysterious. Canaday discovered 11 examples of such, which are displayed in Table 1. A striking feature of Canaday's list is that all the polynomials which appear have a root over $\mathbf{F}_2$. Are there perfect polynomials without such a root? Sixty years later we can do no better than echo Canaday's assessment: "it is plausible that none of this type exist, but this is not proved."

Let us agree to call a polynomial over $\mathbf{F}_2$ *even* if it possesses a root over $\mathbf{F}_2$ and *odd* otherwise. This is more sensible than it may appear at first glance: indeed, with the usual definition of the absolute value of a polynomial over a finite field, viz. $|A| := q^{\deg A}$, the even polynomials are exactly those with a divisor of absolute value 2. In complete analogy with the integer case, Canaday's conjecture now assumes the following tantalizing form:

* Corresponding author. Address: 6188 Kemeny Hall, Dartmouth College, Hanover, New Hampshire 03755. Phone: (603) 646-2415. Fax: (603) 646-1312.

Email addresses: `Luis.Gallardo@univ-brest.fr` (Luis Gallardo), `Paul.Pollack@dartmouth.edu` (Paul Pollack), `Olivier.Rahavandrainy@univ-brest.fr` (Olivier Rahavandrainy).

1 Supported by an NSF Graduate Research Fellowship.

Table 1
Canaday's list of nonsplitting perfect polynomials over $\mathbf{F}_2$.

Degree	**Factorization into Irreducibles**
5	$T(T+1)^2(T^2+T+1)$
	$T^2(T+1)(T^2+T+1)$
11	$T(T+1)^2(T^2+T+1)^2(T^4+T+1)$
	$T^2(T+1)(T^2+T+1)^2(T^4+T+1)$
	$T^3(T+1)^4(T^4+T^3+1)$
	$T^4(T+1)^3(T^4+T^3+T^2+T+1)$
15	$T^3(T+1)^6(T^3+T+1)(T^3+T^2+1)$
	$T^6(T+1)^3(T^3+T+1)(T^3+T^2+1)$
16	$T^4(T+1)^4(T^4+T^3+1)(T^4+T^3+T^2+T+1)$
20	$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
	$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1)$

Conjecture 2 *There are no odd perfect polynomials.*

The study of perfect polynomials over arbitrary finite fields was taken up 35 years later by Beard, O'Connell and West ([2], [3]). There one finds proposed the following bold extension of Canaday's conjecture:

Conjecture 3 *If A is a perfect polynomial over $\mathbf{F}_q$, then A has a linear factor over $\mathbf{F}_q$.*

Link, a master's student of Beard's, showed that this conjecture is too optimistic by exhibiting explicit counterexamples for $q = 11$ and $q = 17$ ([4], [5]). Counterexamples for $q = 4$ appear in a paper of Gallardo & Rahavandrainy [6].

Here we show that the Beard-O'Connell-West conjecture fails in all cases except possibly when q is prime:

Theorem 4 *If $\mathbf{F}_q$ is a nontrivial extension of its prime field $\mathbf{F}_p$, then there is always a perfect polynomial over $\mathbf{F}_q$ with no linear factor.*

The remaining cases appear much more subtle. Here we note that the Link's construction of a counterexample for $p = 11$ generalizes to an infinite class of primes:

Theorem 5 *Let p be any prime for which*

$$\left(\frac{-2}{p}\right) = 1 \quad \textit{while} \quad \left(\frac{-3}{p}\right) = -1.$$

Then $A := \prod_{\alpha \in \mathbf{F}_p} \left((T+\alpha)^2 - 3/8\right)^2$ is perfect yet without linear factors.

Remark 6 *The primes obeying the conditions of the theorem are exactly the primes $p \equiv 11$ or $17 \pmod{24}$, the first few of which are 11, 17, 41, 59, 83, 89, 107, 113, ... By the prime number theorem for arithmetic progressions (or Chebotarev's density theorem), these constitute asymptotically $\frac{1}{4}$ of all primes; in particular, the conjecture of Beard, O'Connell and West fails for infinitely many primes.*

As we noted above, the case $p = 2$ (Canaday's conjecture) remains open. However, assuming a plausible hypothesis on the distribution of prime polynomials, it is easy to prove that if there is a single odd perfect polynomial, then there are infinitely many. The hypothesis we need is the following, which is a partial polynomial analogue of Schinzel's Hypothesis H:

Conjecture 7 *Let $f_1(T), \ldots, f_k(T)$ be irreducible polynomials over $\mathbf{F}_q$. Assume that there is no irreducible polynomial $\pi \in \mathbf{F}_q[T]$ for which the map $\mathbf{F}_q[T] \to \mathbf{F}_q[T]/\pi$ given by*

$$g \mapsto f_1(g) f_2(g) \cdots f_k(g) \pmod{\pi}$$

is identically zero. Then there are infinitely many monic polynomials $g(T)$ for which the specializations $f_1(g(T)), \ldots, f_k(g(T))$ are all irreducible.

Recently progress has been made on this conjecture by the second author [7], who shows that its conclusion holds whenever q is sufficiently large, depending only on k and the degrees of the f_i. Here we prove:

Theorem 8 *Assume Conjecture 7. If there is a single perfect polynomial over $\mathbf{F}_q$ without linear factors, then there are infinitely many.*

If a counterexample to the Beard-O'Connell-West conjecture is known for a specific $\mathbf{F}_q$ (for example, if p satisfies the condition of Theorem 5), then we can often obtain infinitely many counterexamples without the need for Conjecture 7. We illustrate by bootstrapping Link's counterexample in the case $p = 11$ to obtain the following unconditional result:

Theorem 9 *There are infinitely many perfect polynomials over $\mathbf{F}_{11}$ with no linear factor.*

2 Proof of Theorem 4

We begin with the following construction of special irreducible trinomials taken from Cohen [8, Lemma 2]:

Lemma 10 *For any $\beta \in \mathbf{F}_q$, the polynomial $T^p - \alpha T - \beta$ is irreducible in $\mathbf{F}_q$ if and only if*

$$\alpha = A^{p-1} \quad \textit{for some} \quad A \in \mathbf{F}_q \quad \textit{and} \quad \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(\beta/A^p) \neq 0.$$

Here p denotes the characteristic of $\mathbf{F}_q$.

PROOF OF THEOREM 4. Since the trace is a linear map from $\mathbf{F}_q$ down to $\mathbf{F}_p$, and $\mathbf{F}_q$ is a nontrivial extension of $\mathbf{F}_p$, the kernel of the trace map is necessarily nonzero. Thus we can fix $A \in \mathbf{F}_q$ so that the trace of A^{-1} vanishes. After fixing A in this way, choose $\beta \in \mathbf{F}_q$ so that

$$\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(\beta/A^p) \neq 0;$$

this is possible since the left hand side can be written as a polynomial in β of degree q/p, so cannot vanish on all of $\mathbf{F}_q$. We claim that the p polynomials

$$x^p - A^{p-1}x - (\beta + \gamma), \quad \gamma = 0, 1, 2, \ldots, p-1$$

are each irreducible over $\mathbf{F}_q$. By Lemma 10 it suffices to check that $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}((\beta + \gamma)/A^p)$ is nonvanishing for each γ. But this is easy: by the $\mathbf{F}_p$-linearity of the trace,

$$\begin{aligned}\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}((\beta+\gamma)/A^p) &= \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(\beta/A^p) + \gamma \cdot \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(1/A^p) \\ &= \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(\beta/A^p) + \gamma \cdot \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(1/A) = \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(\beta/A^p),\end{aligned}$$

and this is nonzero by the choice of β. To complete the proof we set $A := \prod_{\gamma \in \mathbf{F}_p}(x^p - A^{p-1}x - \beta - \gamma)$ and observe that

$$\sigma(A) = \prod_{\gamma \in \mathbf{F}_p}(x^p - A^{p-1}x - \beta - \gamma + 1) = A.$$

Thus A is perfect over $\mathbf{F}_q$ with no linear factors.

3 Proof of Theorem 5

PROOF. Our construction generalizes Link's treatment of the case $p = 11$. We begin by observing that over any field of characteristic $\neq 2$ in which -2

is a square, we have the polynomial identity

$$
\begin{aligned}
1+(T^2-3/8)+(T^2-3/8)^2 &= (T^2+T\sqrt{-2}-7/8)(T^2-T\sqrt{-2}-7/8)\\
&= ((T+\frac{1}{2}\sqrt{-2})^2-3/8)((T-\frac{1}{2}\sqrt{-2})^2-3/8).
\end{aligned}
$$

Our condition that -3 is not a square implies that also $3/8=(-3)(-2)^{-3}$ is not a square. It follows that $T^2-3/8$ as well as the two polynomial factors appearing on the right hand side are all irreducible. But then with $A := \prod_{\alpha\in\mathbf{F}_p}((T+\alpha)^2-3/8)^2$, we have

$$
\begin{aligned}
\sigma(A) &= \prod_{\alpha\in\mathbf{F}_p}\sigma\left(\left((T+\alpha)^2-\frac{3}{8}\right)^2\right)\\
&= \prod_{\alpha\in\mathbf{F}_p}\left(1+\left((T+\alpha)^2-\frac{3}{8}\right)+\left((T+\alpha)^2-\frac{3}{8}\right)^2\right)\\
&= \prod_{\alpha\in\mathbf{F}_p}\left((T+\alpha+\frac{1}{2}\sqrt{-2})^2-\frac{3}{8}\right)\prod_{\alpha\in\mathbf{F}_p}\left((T+\alpha-\frac{1}{2}\sqrt{-2})^2-\frac{3}{8}\right)\\
&= \prod_{\alpha'\in\mathbf{F}_p}\left((T+\alpha')^2-\frac{3}{8}\right)\prod_{\alpha'\in\mathbf{F}_p}\left((T+\alpha')^2-\frac{3}{8}\right)=A,
\end{aligned}
$$

so A is perfect. Moreover, by construction A is composed of p irreducible quadratic factors, so is a counterexample to the conjecture of Beard, O'Connell and West.

4 Proof of Theorem 8

PROOF. Let A be a perfect polynomial over $\mathbf{F}_q$ without linear factors and write $A=\prod_{i=1}^{k}P_i(T)^{e_i}$, where the P_i are distinct monic irreducibles of degree ≥ 2. For any prime polynomial π of $\mathbf{F}_q[T]$, the map

$$g\mapsto P_1(g)P_2(g)\cdots P_k(g)\pmod{\pi}$$

is not identically zero, since $g=0$ is sent to a nonzero residue class. So by Conjecture 7, there are infinitely many monic polynomials $g(T)$ for which $P_1(g(T)),\ldots,P_k(g(T))$ are each irreducible.

Since A is perfect, we have

$$A=\prod_{i=1}^{k}(1+P_i(T)+P_i(T)^2+\cdots+P_i(T)^{e_i}).$$

Since the substitution $T \mapsto g(T)$ induces an endomorphism of $\mathbf{F}_q[T]$, we have

$$A(g(T)) = \prod_{i=1}^{k} (1 + P_i(g(T)) + P_i(g(T))^2 + \cdots + P_i(g(T))^{e_i}). \qquad (2)$$

By the choice of g, the $P_i(g(T))$ are all irreducible; moreover, since the P_i are distinct and g is transcendental over $\mathbf{F}_q$, the $P_i(g(T))$ are also distinct. It follows that the right hand side of (2) is exactly $\sigma(\prod P_i(g(T))^{e_i}) = \sigma(A(g(T)))$, and comparing with the left hand side we see that $A(g(T))$ is perfect. Moreover, none of the prime factors $P_i(g(T))$ of $A(g(T))$ is linear, so we obtain in this manner infinitely many counterexamples to the Beard-O'Connell-West conjecture.

It seems plausible that we can strengthen the conclusion of Conjecture 7 to read that there are $\gg_{f_1,\ldots,f_k,\epsilon} x^{1-\epsilon}$ such g with absolute value not exceeding x, as $x \to \infty$. Under this additional assumption, the above argument shows that if a single counterexample to the Beard-O'Connell-West conjecture exists over $\mathbf{F}_q$, then the number of counterexamples of absolute value $\leq x$ is at least x^δ for some small positive δ and all large x. By contrast, in the classical setting Hornfeck & Wirsing [9] have shown that there are only $O_\epsilon(x^\epsilon)$ perfect numbers $\leq x$ for every $\epsilon > 0$.

Another nonanalogy is worth pointing out: the above proof also shows that if an odd perfect polynomial with k distinct prime factors exists, then (under Hypothesis H) infinitely many such odd perfect polynomials exist. This is perhaps surprising in light of Dickson's classical result [10] that for each k there are only finitely many odd perfect numbers with k distinct prime factors.

5 Proof of Theorem 9

Let A denote Link's counterexample to Beard's conjecture for $p = 11$, so that

$$A := \prod_{\alpha \in \mathbf{F}_{11}} \left((T+\alpha)^2 + 1\right)^2.$$

Lemma 11 *Let $f(T)$ be an irreducible quadratic polynomial over $\mathbf{F}_p$, where p is prime. Then the substitution $T \mapsto T^p + T$ leaves f irreducible.*

PROOF. Let $\beta \in \mathbf{F}_{p^2}$ be a root of $f(T)$. The irreducibility of $f(T^p + T)$ over $\mathbf{F}_p$ is equivalent to the irreducibility of $T^p + T - \beta$ over $\mathbf{F}_{p^2}$. By Lemma 10, we have this property if and only if

$$-1 = A^{p-1} \quad \text{for some} \quad A \in \mathbf{F}_{p^2} \quad \text{and} \quad \mathrm{Tr}_{\mathbf{F}_{p^2}/\mathbf{F}_p}(\beta/A^p) = 1. \tag{3}$$

Fix a generator g of $\mathbf{F}_p^\times$ and set $A := \sqrt{g} \in \mathbf{F}_{p^2}$. Then $A^{p-1} = A^p/A = -\sqrt{g}/\sqrt{g} = -1$. So to complete the proof it suffices to verify the nonvanishing condition on the trace appearing in (3). But

$$\mathrm{Tr}_{\mathbf{F}_p^2/\mathbf{F}_p}(\beta/A^p) = \beta/A^p + \beta^p/A^{p^2} = -\beta/A + \beta^p/A = A^{-1}(\beta^p - \beta),$$

which is nonzero since otherwise β belongs to $\mathbf{F}_p$, contradicting the irreducibility of f.

Since each irreducible factor of A is quadratic, Lemma 11 implies that the substitution $T \mapsto T^{11} + T$ takes A to another perfect polynomial, say $\tilde{A}$ (cf. the proof of Theorem 8). We now show how from $\tilde{A}$ one can obtain an infinite family of perfect polynomials over $\mathbf{F}_{11}$ without linear factors.

Recall that if $f(T) \in \mathbf{F}_q[T]$ is an irreducible polynomial not a constant multiple of T, then by the *order of f* we mean the order of any of its roots in the multiplicative group of its splitting field, or equivalently, the order of T in the unit group $(\mathbf{F}_q[T]/f)^\times$. The next lemma is contained in the classical researches of Serret and Dickson; a modern reference is [11, Theorem 3.3.5].

Lemma 12 *Let $f(T) \in \mathbf{F}_q[T]$ be an irreducible polynomial of degree m and order e. Suppose that l is an odd prime for which*

$$l \textit{ divides } e \quad \textit{but} \quad l \textit{ does not divide } (q^m - 1)/e. \tag{4}$$

Then the substitution $T \mapsto T^{l^k}$ leaves f irreducible for every $k = 1, 2, 3, \ldots$.

From the data in Table 2, we observe that Lemma 12 can be simultaneously applied to each of the irreducible factors of $\tilde{A}$ with the same prime $l = 15797$ (or with $l = 1806113$). Then each of the substitutions $T \mapsto T^{l^k}$ takes $\tilde{A}$ to another perfect polynomial.

Summarizing, we have shown that each of the composite substitutions

$$T \mapsto T^{11} + T \quad \text{followed by} \quad T \mapsto T^{15797^k}$$

takes A to a perfect polynomial over $\mathbf{F}_{11}$ without linear factors. This completes the proof of Theorem 9.

Table 2
Data needed for the proof of Theorem 9. Note that $11^2 - 1 = 2^3 \cdot 3 \cdot 5$ while $11^{22} - 1 = 2^3 \cdot 3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$.

Polynomial	**Order after substitution** $T \mapsto T^{11} + T$
$T^2 + 1$	$2^2 \cdot 15797 \cdot 1806113$
$(T+1)^2 + 1$	$2^3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+2)^2 + 1$	$3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+3)^2 + 1$	$2^3 \cdot 3 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+4)^2 + 1$	$2^3 \cdot 3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+5)^2 + 1$	$2^2 \cdot 3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+6)^2 + 1$	$2^2 \cdot 3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+7)^2 + 1$	$2^3 \cdot 3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+8)^2 + 1$	$2^3 \cdot 3 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+9)^2 + 1$	$2 \cdot 3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$
$(T+10)^2 + 1$	$2^3 \cdot 5 \cdot 23 \cdot 89 \cdot 199 \cdot 15797 \cdot 58367 \cdot 1806113$

Acknowledgements

We thank Felipe Voloch for enlightening e-mail correspondence related to Theorem 8.

References

[1] E. F. Canaday, The sum of the divisors of a polynomial, Duke Math. J. 8 (1941) 721–737.

[2] J. R. O'Connell, Perfect polynomials over GF(p), Master's thesis, Univ. Texas at Arlington (1974).

[3] J. T. B. Beard, Jr., J. R. O'Connell, Jr., K. I. West, Perfect polynomials over GF(q), Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 62 (1977) 283–291.

[4] M. L. Link, Iterated sums of polynomial divisors over GF(p), Master's thesis, Tennessee Technological University (1995).

[5] J. T. B. Beard, Jr., M. L. Link, Iterated sums of polynomial divisors, Libertas Math. 17 (1997) 111–124.

[6] L. Gallardo, O. Rahavandrainy, On perfect polynomials over $\mathbf{F}_4$, Port. Math. (N.S.) 62 (1) (2005) 109–122.

[7] P. Pollack, An explicit approach to Hypothesis H for polynomials over a finite field, In Proceedings of the Anatomy of Integers Conference, Montréal, March 2006, to appear.

[8] S. D. Cohen, The reducibility theorem for linearised polynomials over finite fields, Bull. Austral. Math. Soc. 40 (3) (1989) 407–412.

[9] B. Hornfeck, E. Wirsing, Über die Häufigkeit vollkommener Zahlen, Math. Ann. 133 (1957) 431–438.

[10] L. E. Dickson, Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors, Amer. J. Math. 35 (4) (1913) 413–422.

[11] R. Lidl and H. Niederreiter, Finite fields, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. With a foreword by P. M. Cohn.