COUNTING PERFECT POLYNOMIALS

U. CANER CENGIZ, PAUL POLLACK, AND ENRIQUE TREVIÑO

Abstract. Let $A \in \mathbf{F}_2[T]$. We say A is *perfect* if A coincides with the sum of all of its divisors in $\mathbf{F}_2[T]$. We prove that the number of perfect polynomials A with $|A| \le x$ is $O_\epsilon(x^{1/12+\epsilon})$ for all $\epsilon > 0$, where $|A| = 2^{\deg A}$. We also prove that every perfect polynomial A with $1 < |A| \le 1.6 \times 10^{60}$ is divisible by T or $T+1$; that is, there are no small "odd" perfect polynomials.

1. Introduction

For each nonzero $A \in \mathbf{F}_2[T]$, let $\sigma(A) = \sum_{D|A} D$, where D runs over all of the divisors of A in $\mathbf{F}_2[T]$. We call A perfect if $\sigma(A) = A$. For example, $T(T+1)$ is perfect, because

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

The study of perfect polynomials was initiated by Canaday [1] in his doctoral work under Leonard Carlitz.[1] In the case when A splits over $\mathbf{F}_2$ — meaning that all of its roots in $\overline{\mathbf{F}_2}$ lie in $\mathbf{F}_2$ — Canaday discovered the following concrete characterization of when A is perfect:

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

For non-splitting perfect polynomials the situation is less clear. Canaday discovered 11 examples whose irreducible factorizations are exhibited in Table 1.

One immediately striking feature of Canaday's list is that all the polynomials appearing have a root in $\mathbf{F}_2$. Are there perfect polynomials ($\neq 1$) without such a root? Almost 80 years later we can do no better than echo Canaday's assessment: "it seems plausible that none of this type exist, but this is not proved." Let us agree to call A *even* if A has a root in $\mathbf{F}_2$ and to call A *odd* otherwise.[2] Then, in analogy with the integer case, Canaday's conjecture becomes:

Canaday's conjecture. *There are no odd perfect polynomials, other than $A = 1$.*

From now on, when we refer to an *odd perfect polynomial*, we will mean an odd perfect polynomial $\neq 1$. With this convention, Canaday's conjecture is that there are no odd perfect polynomials.

Various constraints are known on the multiplicative structure of any odd perfect polynomial. The following basic result can be considered the analogue of the classical Euler-form for odd perfect numbers:

2010 *Mathematics Subject Classification.* 11T55 (primary), and 11T06 (secondary).

Key words and phrases. perfect polynomial; one-ring; sum-of-divisors.

[1]Canaday did not name these polynomials *perfect*. He used the term *one-ring* for a perfect polynomial. The term *perfect polynomial* was first used by Beard, O'Connell and West in [7].

[2]These terms originated in several papers of Gallardo and Rahavandrainy (see [3, 4]).

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	$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
	$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1)$

TABLE 1. Known nonsplitting perfect polynomials over $\mathbf{F}_2$.

Theorem B. *An odd perfect polynomial is a square.*

The proof of Theorem B is straightforward: if P^e is a unitary divisor of some odd perfect polynomial,[3] then both P and $\sigma(P^e)$ are odd. In particular, both P and $\sigma(P^e) = 1 + P + \cdots + P^e$ have constant term 1; this implies that e is even.

In [5], Gallardo and Rahavandrainy proved that an odd perfect polynomial has at least five distinct irreducible factors. In [3], they showed that an odd perfect polynomial that is a product of squares of distinct irreducibles has at least 10 distinct irreducible factors. Therefore, using Theorem B, we have:

Theorem C. *If A is an odd perfect polynomial, then the number of irreducible factors of A, counted with multiplicity, is at least 12.*

In the classical setting, Hornfeck & Wirsing showed [6] that there are $O_\epsilon(x^\epsilon)$ perfect numbers $\le x$. We have not been able to do as well in the polynomial case. By combining the method of Hornfeck–Wirsing with the result of Theorem C, we prove:

Theorem 1.1. *The number of perfect polynomials of norm $\le x$ is $O_\epsilon(x^{\frac{1}{12}+\epsilon})$ for every $\epsilon > 0$.*

Here and throughout, the *norm of* A, abbreviated $|A|$, denotes the size of the quotient $\mathbf{F}_2[T]/(A)$. That is, $|A| = 2^{\deg A}$ for each nonzero polynomial A.

The key ingredient in the proof of Theorem 1.1 is a polynomial analogue of a lemma of Hornfeck–Wirsing [6], which we prove in §3 (see Lemma 3.1 below). The statement of the lemma suggests an algorithm that can be used to search for perfect polynomials. In §6 we describe this algorithm and report on computations that prove the following two theorems.

Theorem 1.2. *There are no odd perfect polynomials of degree ≤ 200, i.e., there are no odd perfect polynomials of norm $\le 2^{200} \approx 1.6 \times 10^{60}$.*

Theorem 1.3. *If A is a non-splitting perfect polynomial of degree ≤ 200, then A is one of Canaday's polynomials in Table 1.*

[3]Recall that A is said to be a *unitary divisor* of M if $M = AB$ with $\gcd(A, B) = 1$; in this case, we also write $A \parallel M$.

2. Facts from elementary prime number theory in $\mathbf{F}_2[T]$

We begin by defining a normalized prime counting function for $\mathbf{F}_2[T]$ by

$$\Pi(x) = \#\{A \in \mathbf{F}_2[T] : |A| \le x, A \text{ irreducible}\}.$$

The following lemma is a well-known consequence of a formula of Gauss. See, e.g., Exercises 3.26 and 3.27 in [8].

Lemma 2.1. *For each positive integer d, the number $\pi_2(d)$ of irreducibles $A \in \mathbf{F}_2[T]$ of degree d satisfies*

$$\frac{2^d}{d} - 2\frac{2^{d/2}}{d} \le \pi_2(d) \le \frac{2^d}{d}.$$

From this we can quickly deduce the following analogue of Chebyshev's estimates in classical prime number theory.

Lemma 2.2 (Chebyshev's prime counting bounds for $\mathbf{F}_2[T]$)**.**

$$\Pi(x) \asymp x/\log x \quad \textit{for } x \ge 2.$$

Remark. Lemma 2.2, while sufficient for the present purposes, is quite crude. For more precise results, see for instance [10] and the references therein.

Proof. First note that $\Pi(x) = \sum_{d \le \log_2 x} \pi_2(d)$. Using the upper bound in Lemma 2.1, and noting that the function $t \mapsto 2^t/t$ is increasing for $t \ge 2$, we see that

$$\Pi(x) \le \sum_{d \le \log_2 x} \frac{2^d}{d} \le 2 + \int_2^{\log_2 x + 1} \frac{2^t}{t} \mathrm{d}t \le 2 + \int_2^{2x} \frac{1}{\log u} \mathrm{d}u \ll \frac{x}{\log x}.$$

The proof for the lower bound is similar. □

Lemma 2.3. *Suppose $x \ge 10$ and suppose y is such that*

$$\prod_{\substack{|P| \le y \\ P \text{ irreducible}}} |P| \le x.$$

Then $y \le c_1 \log x$ for an absolute constant $c_1 \ge 1$.

Proof. If $y \le 2$ then the result is trivial. Otherwise we write the above inequality in the form $\sum_{|P| \le y,\ P \text{ irreducible}} \log |P| \le \log x$. For each positive integer d, Lemma 2.1 implies that the number of irreducibles of degree d is $\gg 2^d/d$ (with an absolute implied constant), and so reorganizing the irreducibles according to their degree we find that

$$\log x \ge \sum_{|P| \le y,\ P \text{ irreducible}} \log |P| \gg \sum_{\substack{2^d \le y \\ d \ge 1}} d\frac{2^d}{d} = \sum_{\substack{2^d \le y \\ d \ge 1}} 2^d \gg y.$$

This proves the claim, modulo the hypothesis that $c_1 \ge 1$. But we can clearly increase c_1 if necessary without affecting the truth of the lemma. □

Lemma 2.4. *Suppose $x \ge 10$. If the product of r irreducible polynomials in $\mathbf{F}_2[T]$ has norm $\le x$ then $r \le c_2 \log x/\log\log x$ where c_2 is an absolute constant.*

Proof. Let c_1 be the constant of Lemma 2.3, so that the product of the irreducibles of norm not exceeding $2c_1 \log x$ exceeds x. Letting r' be the number of terms in that product we must have $r \le r'$. But $r' = \Pi(2c_1 \log x) \le c_2 \log x/\log\log x$, say, by Lemma 2.2. □

3. The method of Hornfeck & Wirsing and our fundamental lemma

In this section we adapt the method of Hornfeck & Wirsing [6] to the polynomial setting.

Lemma 3.1 (Fundamental lemma)**.** *Let M be a polynomial which is not perfect, and let $k \geq 2$ be a fixed positive integer. Let $x \geq 10$. Then there exists a constant C_k depending only on k, as well as a set $\mathcal{S}$ depending only on M, k and x, of cardinality bounded by $x^{C_k/\log\log x}$, with the following property: if A is a perfect polynomial of norm $\leq x$ for which*

(a) *M is a unitary divisor of A: i.e., $A = MN$ with $\gcd(M, N) = 1$, and*
(b) *$N = A/M$ is k-free, i.e., $P^k \nmid N$ for any irreducible polynomial P,*

then A has a decomposition of the form $M'N'$, where

(i) *M' is an element of $\mathcal{S}$,*
(ii) *M' and N' are unitary divisors of A,*
(iii) *both factors M' and N' are perfect,*
(iv) *N' is k-free,*
(v) *M is a unitary divisor of M'.*

Proof. Let A be a perfect polynomial with the properties of the lemma. Since M is not perfect, $M \neq \sigma(M)$ and since M and $\sigma(M)$ share the same degree, it must be that $\sigma(M) \nmid M$. It follows that there is an irreducible polynomial P_1 which divides $\sigma(M)$ to a higher power than that to which it divides M. Referring to the equation

$$MN = A = \sigma(A) = \sigma(M)\sigma(N)$$

we see that P_1 divides N. Say $P_1^{\alpha_1} \parallel N$, where by the k-free hypothesis on N necessarily $1 \leq \alpha_1 \leq k-1$. Now define

$$M_2 = MP_1^{\alpha_1} \quad \text{and} \quad N_2 = N/P_1^{\alpha_1}.$$

If M_2 is perfect then we stop here. Otherwise we see that A has the decomposition $A = M_2N_2$ with M_2 a non-perfect unitary divisor of A and N_2 a k-free polynomial. But then we can repeat the above argument: if P_2 is chosen as an irreducible dividing $\sigma(M_2)$ to a higher power than that to which it divides M_2, we find that $P_2^{\alpha_2} \parallel N$ for some $1 \leq \alpha_2 \leq k-1$. We then set

$$M_3 := M_2P_2^{\alpha_2} \quad \text{and} \quad N_3 := N_2/P_2^{\alpha_2}.$$

If M_3 is perfect, then we stop, otherwise we continue in the same way until we reach a perfect M_r.

Let us check that if at this point we set $M' := M_r$ and $N' := N_r$, then M' and N' have the five properties listed in the conclusion of the lemma. Properties (ii), (iv), (v) are straightforward to verify: indeed, M_i and N_i have the corresponding properties at every step of the algorithm. To see (iii) note that

$$1 = \frac{\sigma(A)}{A} = \frac{\sigma(M'N')}{M'N'} = \frac{\sigma(M')}{M'}\frac{\sigma(N')}{N'}.$$

Since M' is perfect, the first factor in the final expression is 1, and so its cofactor is also 1: that is, N' is also perfect.

It remains to check property (i), i.e., that M' can be chosen to belong to a small set $\mathcal{S}$ (depending only on M, k and x). This comes from a detailed analysis of our algorithm: observe that P_1 can be chosen to depend only on M (e.g., we can take the irreducible divisor of M of largest degree which comes last lexicographically).

There are $k-1$ possibilities for α_1, and after α_1 is determined, we know M_2. But then M_2 is either perfect, and so we terminate the algorithm, or we choose an irreducible P_2 as described above (which can be chosen to depend only on P_1 and α_1). But then once we know α_2, we know M_3, and so we know whether to terminate the algorithm or to continue (picking an irreducible P_3, which can be chosen to depend only on M, α_1 and α_2). If we continue in this way we find that M_r is determined completely by M and the sequence of exponents $\alpha_1, \dots, \alpha_{r-1}$.

Let us now estimate the number of possibilities for this sequence. Every α_i belongs to the $(k-1)$-element set $\{1, 2, \dots, k-1\}$. Moreover, the polynomial N has norm $\leq x$ but is divisible by the $r-1$ distinct irreducibles $P_1, \dots, P_{r-1}$. Lemma 2.4 implies that the length of the sequence $\alpha_1, \dots, \alpha_{r-1}$ is bounded by $c_2 \log x / \log\log x$. Piecing this together, we find that the number of possibilities for the exponent sequence (and hence for M', as argued above) is

$$\ll (\log x / \log\log x) \cdot (k-1)^{c_2 \log x / \log\log x}.$$

(To see this bound, think of first choosing the length of the exponent sequence and then its elements.) This upper bound is at most $x^{C_k / \log\log x}$ if C_k is chosen appropriately. □

4. Bounding the number of indecomposable perfect polynomials

Definition. The nonconstant perfect polynomial A is called *indecomposable* if A has no nontrivial factorization as a product of two relatively prime perfect polynomials. Here *nontrivial* means that neither factor is 1.

Our strategy in the proof of Theorem 1.1 is to understand the distribution of indecomposable perfects and to piece this information together to get a picture of the distribution of all perfects. The first half of this is plan is implemented in this section; the latter half in §5.

We begin with some consequences of our fundamental lemma (Lemma 3.1).

Recall that a polynomial is called *k-full* if every irreducible in its prime decomposition appears to at least the kth power.

Lemma 4.1. *Let $k \geq 2$. The number of k-full polynomials of norm $\leq x$ is $O(x^{1/k})$. The implied constant depends on k.*

Proof. We mimic the usual proof of the analogous bound in the rational setting. Suppose A is k-full. We claim that $A = Q_1^k Q_2^{k+1} \cdots Q_k^{2k-1}$ for some nonzero polynomials $Q_1, Q_2, \dots Q_k$. Indeed, suppose P is an irreducible divisor of A and $P^r \parallel A$. We may write $r = km + i$ for some nonnegative integer m and some integer i satisfying $0 \leq i \leq k-1$. Since A is k-full, $r \geq k$, and so $m \geq 1$. Therefore $r = (k+i) + (m-1)k$, and $P^r = P^{k+i}(P^{m-1})^k = U_1^{k+i} U_2^k$. The claim follows.

Now let us count how many possible $Q_1^k Q_2^{k+1} \dots Q_k^{2k-1}$ we can have under the constraint that the norm stays $\leq x$. Let $U = Q_2^{k+1} Q_3^{k+2} \cdots Q_k^{2k-1}$. Once U is fixed, Q_1 is constrained to have norm $\leq (x/U)^{1/k}$, so that there are at most $2(x/U)^{1/k}$ possibilities for Q_1. Therefore, the number of k-full polynomials of norm $\leq x$ is bounded by

$$2x^{1/k} \sum_{|Q_2^{k+1} Q_3^{k+2} \cdots Q_k^{2k-1}| \leq x} \frac{1}{\left|Q_2^{k+1} Q_3^{k+2} \cdots Q_k^{2k-1}\right|^{\frac{1}{k}}} \leq 2x^{1/k} \prod_{i=1}^{k-1} \sum_{Q} \frac{1}{|Q|^{\frac{k+i}{k}}},$$

where the final sums on Q are over all nonzero polynomials in $\mathbf{F}_2[T]$. Grouping terms of the same degree,

$$\sum_Q \frac{1}{|Q|^{\frac{k+i}{k}}} = \sum_{d\geq 0} 2^d \cdot \frac{1}{(2^d)^{\frac{k+i}{k}}}.$$

The sum on d is a convergent geometric series (for each i) and the result follows. □

Lemma 4.2. *For each $k \geq 2$ the number of indecomposable perfect polynomials of norm $\leq x$ which are not k-free is $O(x^{1/k+\epsilon})$ for any fixed $\epsilon > 0$. The implied constant here may depend on k and ϵ.*

Proof. If A is any nonzero polynomial over $\mathbf{F}_2$, then A has a unique decomposition $A = MN$, where M is k-full, N is k-free and $\gcd(M, N) = 1$. We apply this observation with A an indecomposable perfect polynomial which is not k-free; then by hypothesis $M \neq 1$.

We now fix a k-full $M \neq 1$ with $|M| \leq x$ and estimate the number of indecomposable perfect A of norm $\leq x$ having M as their k-full part. For this to be the case, it is necessary and sufficient that $A = MN$ where

(i) M and N are coprime,
(ii) N is k-free,
(iii) MN is perfect,
(iv) MN is indecomposable,
(v) MN has norm $\leq x$.

Suppose first that M is itself perfect. From (i) and (iii) we find that then N is also perfect. But then the indecomposability of $A = MN$ (i.e., property (iv)) forces $N = 1$. Thus if M is perfect, there is only one choice for N, and so also only one choice for A.

Now suppose that M is not perfect. Then the hypotheses of Lemma 3.1 are satisfied for $A = MN$, and the lemma provides a decomposition

$$A = M'N', \quad \text{where} \quad M \parallel M' \parallel A, \quad \text{and} \quad M', N' \quad \text{are both perfect,}$$

and where M' is restricted to a set of size at most $x^{C_k/\log\log x}$. This is a factorization of A into coprime perfect polynomials, so that by (iv) either $M' = 1$ or $N' = 1$. But $M \mid M'$ and $M \neq 1$, so that we must have $N' = 1$. Hence $A = M'$, and so A itself is restricted to a set of size at most $x^{C_k/\log\log x}$.

Putting together the two cases and using Lemma 4.1, we see that the number of possibilities for A is certainly bounded by

$$\sum_{\substack{|M|\leq x \\ M \text{ } k\text{-full}}} (1 + x^{C_k/\log\log x}) \ll x^{1/k} + x^{1/k + C_k/\log\log x} \ll x^{1/k+\epsilon}$$

for any $\epsilon > 0$. □

Lemma 4.3. *Let $k \geq 2$ be an integer and let $\epsilon > 0$. The number of indecomposable perfect polynomials of norm $\leq x$ with at least k irreducible factors, counted with multiplicity, is $O(x^{1/k+\epsilon})$. As before, the implied constant here may depend on both k and ϵ.*

Proof. By Lemma 4.2 we may add the assumption that the polynomials to be counted here are k-free. Let A be a polynomial satisfying all of the above hypotheses. Since A has norm not exceeding x and A has at least k irreducible factors

(counted with multiplicity), A has an irreducible factor P of norm at most $x^{1/k}$. Since A is k-free, there are only $O(1)$ possibilities for the exponent to which P occurs in A. Collecting these observations, we see that A has a unitary prime power divisor P^α from a set of size $\ll x^{1/k}$. For each possibility for P^α, we count the number of k-free indecomposable, perfect polynomials of norm $\leq x$ which possess P^α as a unitary divisor.

For this, apply Lemma 3.1 with $M = P^\alpha$. If A with $|A| \leq x$ is k-free, perfect, indecomposable and possesses P^α as unitary prime divisor, we obtain a factorization

$$A = M'N', \quad \text{where} \quad P^\alpha \parallel M' \parallel A, \quad \text{and} \quad M', N' \quad \text{are both perfect;}$$

moreover, there are at most $x^{C_k/\log\log x}$ possibilities for M'. As in Lemma 4.2, A being indecomposable implies that $N' = 1$ and hence that $A = M'$, so that there are only $x^{C_k/\log\log x}$ possibilities for A.

Summing over the $\ll x^{1/k}$ possibilities for P^α, we obtain $\ll x^{C_k/\log\log x + 1/k}$ polynomials A as described in the lemma statement. □

The preceding results imply a very satisfactory bound on the number of indecomposable *even* perfect polynomials:

Corollary 4.4 (Bound on the number of indecomposable even perfects)**.** *The number of indecomposable even perfect polynomials of norm $\leq x$ is $O_\epsilon(x^\epsilon)$ for any $\epsilon > 0$.*

Proof. Fix $k \geq 2$ with $\frac{1}{k} < \epsilon$. By Lemma 4.3 there are $O_\epsilon(x^\epsilon)$ indecomposable perfect polynomials with at least k irreducible factors, counted with multiplicity. So we may restrict our attention to A with fewer than k irreducible factors. Since A is even, A has a unitary divisor M among

$$T,\ T^2,\ \ldots,\ T^{k-1} \quad \text{or} \quad (T+1),\ (T+1)^2,\ \ldots,\ (T+1)^{k-1},$$

and the quotient of A by this unitary divisor is k-free. Running through the $O(k)$ possibilities for M, we find from the indecomposability of A and Lemma 3.1 that the number of possibilities for A is $O(kx^{C_k/\log\log x}) = O_\epsilon(x^\epsilon)$. □

Unfortunately, bounding the count of indecomposable odd perfect polynomials is not so simple, and this accounts for the imperfection in our Theorem 1.1. We introduce the following hypothesis, for each $k = 1, 2, 3, \ldots$:

Hypothesis O_k. *For each $\epsilon > 0$, all but $O_\epsilon(x^\epsilon)$ odd perfect polynomials over $\mathbf{F}_2$ of norm $\leq x$ have at least k irreducible factors, counted with multiplicity.*

Theorem C shows that Hypothesis O_{12} holds; in fact, the phrase "all but ..." in the statement of the Hypothesis can be replaced simply by "all." From Lemma 4.3 we deduce immediately the following result:

Corollary 4.5 (Bound on the number of odd indecomposables)**.** *Under Hypothesis O_k, the number of indecomposable odd perfect polynomials of norm $\leq x$ is $O_{k,\epsilon}(x^{1/k+\epsilon})$. In particular, this number is unconditionally $O_\epsilon(x^{1/12+\epsilon})$.*

5. Bounding the number of perfect polynomials

Lemma 5.1. *Every perfect polynomial A has a factorization as a product of pairwise relatively prime indecomposable perfect polynomials. We allow the empty factorization when $A = 1$.*

Proof. The lemma is true when $A = 1$. If it fails for some nonconstant perfect polynomial, choose a counterexample A whose degree is as small as possible. Then A is not indecomposable itself, so that $A = MN$ for some coprime perfect polynomials M and N with $1 \le \deg M, \deg N < \deg A$. But then both M and N can be written as a product of pairwise coprime indecomposable perfect polynomials. Concatenating their factorizations yields a decomposition of A into pairwise coprime indecomposables. This contradicts the choice of A. □

We now prove Theorem 1.1 in a slightly more general guise.

Theorem 5.2. *Suppose Hypothesis O_k. Then there are $O_{k,\epsilon}(x^{1/k+\epsilon})$ perfect polynomials of norm $\le x$. In particular, unconditionally there are $O_\epsilon(x^{1/12+\epsilon})$ perfect polynomials of norm $\le x$.*

Proof. Let $\mathcal{S}$ be the set of indecomposable perfect polynomials and let $S(x)$ be the corresponding counting function, i.e., the number of elements of $\mathcal{S}$ with norm bounded by x. By Corollaries 4.4 and 4.5, we have $S(x) = O(x^{1/k+\epsilon/2})$ under Hypothesis O_k. Then partial summation yields

$$\sum_{A\in\mathcal{S}} \frac{1}{|A|^{1/k+\epsilon}} = \int_1^\infty S(t)(1/k+\epsilon)\frac{1}{t^{1+1/k+\epsilon}}\,\mathrm{d}t \ll \int_1^\infty \frac{1}{t^{1+\epsilon/2}}\,\mathrm{d}t < \infty.$$

Consequently, if $\mathcal{T}$ denotes the set of all perfect polynomials,

$$\sum_{M\in\mathcal{T}} \frac{1}{|M|^{1/k+\epsilon}} \le \prod_{A\in\mathcal{S}} \left(1 + \frac{1}{|A|^{1/k+\epsilon}}\right) \le \exp\left(\sum_{A\in\mathcal{S}} \frac{1}{|A|^{1/k+\epsilon}}\right) < \infty.$$

To see the first of these inequalities, expand out the product and recall that by Lemma 5.1 every perfect polynomial (element of $\mathcal{T}$) can be written as a product of distinct indecomposables (elements of $\mathcal{S}$).

The convergence of $\sum_{M\in\mathcal{T}} |M|^{-1/k-\epsilon}$ easily implies that the counting function $T(x)$ of the perfect polynomials satisfies $T(x) = O(x^{1/k+\epsilon})$. Indeed, since $1 \le x/|M|$ for any polynomial M of norm $\le x$, we have

$$T(x) = \sum_{\substack{M\in\mathcal{T}\\ |M|\le x}} 1 \le \sum_{M\in\mathcal{T}} (x/|M|)^{\frac{1}{k}+\epsilon} \ll_{k,\epsilon} x^{\frac{1}{k}+\epsilon}.$$ □

Remark. As explained on [2, p. 247], if there is a single odd perfect polynomial, then a plausible polynomial analogue of the Bateman–Horn conjecture from rational number theory implies that the number of odd perfect polynomials of norm not exceeding x is $\gg x^\delta$, for some constant $\delta > 0$. So — subject to this conjecture — proving that the counting function of perfect polynomials is $O_\epsilon(x^\epsilon)$, for all $\epsilon > 0$, is equivalent to showing that there are no odd perfect polynomials at all!

6. An algorithm for finding perfect polynomials inspired by the Hornfeck–Wirsing work

The proof of Lemma 3.1 suggests the following algorithm to search for indecomposable perfect polynomials below a given bound.

H.-W. Algorithm. Given a polynomial B and a stopping bound H, with $\deg B \le H$, the following algorithm (a) outputs only perfect polynomials A of degree $\le H$ having B as a unitary divisor, and (b) outputs every such A that is indecomposable.

(i) Check if $\sigma(B) = B$. If yes, then output B and break.
(ii) Compute $D = \sigma(B)/\gcd(B, \sigma(B))$.
(iii) If $\gcd(B, D) \neq 1$, break.
(iv) Let P be an irreducible factor of D of largest degree.
(v) Recursively call the algorithm with inputs BP^k and stopping bound H, for all positive integers k with $\deg(BP^k) \leq H$.

To see that the algorithm works, suppose A is an indecomposable perfect polynomial with $B \parallel A$. Write $A = BC$, so that $\gcd(B, C) = 1$. Then

$$BC = A = \sigma(A) = \sigma(B)\sigma(C);$$

hence, $\sigma(B) \mid BC$, and

$$D = \frac{\sigma(B)}{\gcd(B, \sigma(B))} \mid C.$$

Suppose that $D = 1$. Then B is perfect, and the algorithm outputs B and breaks. Note that this output is perfect, has B as a unitary divisor, and that if there is any indecomposable perfect polynomial having B as a unitary divisor, then it is B itself.

Suppose we do not break in (i) and continue on to (ii), (iii). If D has an irreducible factor in common with B, then this irreducible is a common factor of B and C, contradicting that $\gcd(B, C) = 1$. So again we can stop, this time because no solution exists.

In the remaining case, take any irreducible factor P of D. (We specified above that P is chosen of largest degree for definiteness and to speed up the algorithm.) If P^e is the highest power of P dividing C, then A has the unitary divisor BP^e. Thus, we restart the algorithm with the inputs listed in step (v).

The algorithm is recursive, but guaranteed to terminate, since we are only searching for solutions up to height H.

Proof of Theorem 1.2. Since odd perfect polynomials are necessarily squares, we run a modified version of the algorithm, where instead of recursing over BP^k with $\deg(BP^k) \leq H$, we recurse over BP^{2k} with $\deg(BP^{2k}) \leq H$. We ran this modified algorithm with $H = 200$ for all odd square polynomials $B \neq 1$ of degree ≤ 40 (we did this by squaring each odd polynomial of degree in the interval $[1, 20]$). There was no output. The computation took roughly 6 hours with `PARI/GP` [9] running on a Core i7-6600U machine.

To see why this implies Theorem 1.2, assume for the sake of contradiction that there is an odd perfect polynomial A of degree $d \leq 200$. Since A has at least five distinct irreducible factors, A has a nonconstant unitary divisor B of degree $\leq \frac{200}{5} = 40$. Moreover, since A is an odd square, so is B. Since the algorithm produced no output, there are no odd perfect polynomials of degree $d \leq 200$. □

The proof of Theorem 1.3 is similar. We begin by recalling two easy (known) results. The proofs are reproduced for the convenience of the reader.

Lemma 6.1. *Let $A \in \mathbf{F}_2[T]$. Then:*

(i) *The polynomial $A(T)$ is perfect if and only if $A(T + 1)$ is perfect.*
(ii) *If $A(T)$ is perfect, then T divides $A \iff T + 1$ divides A.*

Proof. First, note that the map $T \mapsto T+1$ induces an automorphism of $\mathbf{F}_2[T]$, which we will denote here with a tilde. Factor $A = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$. Then the prime factorization of $\tilde{A}$ takes the form $\tilde{P}_1^{\alpha_1} \cdots \tilde{P}_k^{\alpha_k}$; thus,

$$\widetilde{\sigma(A)} = \prod_{i=1}^{k} \widetilde{(1 + P_i + \cdots + P_i^{\alpha_i})} = \prod_{i=1}^{k} (1 + \tilde{P}_i + \cdots + \tilde{P}_i^{\alpha_i}) = \sigma(\tilde{A}).$$

Part (i) of the lemma follows immediately. To prove (ii), suppose that A is perfect and $T \mid A$. Let $A = T^\alpha \prod_{i=1}^{r} P_i^{\alpha_i}$ be its prime factorization. For the sake of contradiction, suppose that $T+1 \nmid A$. Then $P_i(0) = P_i(1) = 1$ for all $i = 1, 2, \ldots, r$. Now $\sigma(P_i^{\alpha_i}) = 1 + P_i + P_i^2 + \ldots + P_i^{\alpha_i}$, so that $\sigma(P_i^{\alpha_i})(1) = \alpha_i + 1$. Since $T+1 \nmid A = \sigma(A)$, each α_i is even. But then each $\sigma(P_i^{\alpha_i})(0) = 1$, and hence $T \nmid \sigma(P_i^{\alpha_i})$. Since also $T \nmid \sigma(T^\alpha)$, it follows that $T \nmid \sigma(A)$, contradicting that $T \mid A = \sigma(A)$. Hence, if $T \mid A$, then $T+1 \mid A$. This proves the forward implication in (ii). The backward implication follows from the forward one, by first applying the tilde automorphism interchanging T and $T+1$. □

Proof of Theorem 1.3. We ran the (unmodified) algorithm with $B = T$, T^2, …, T^{100} and $H = 200$. The computation took 3 days, and the eventual output consisted of the six splitting perfect polynomials of degrees in $[1, 200]$, together with the list of 11 non-splitting perfect polynomials found by Canaday. We denote this set of 17 output values by $\mathcal{E}$.

Now we explain why this implies Theorem 1.3. By Theorem 1.2, there are no odd perfect polynomials of degree in $[1, 200]$, so all non-splitting perfect polynomials in that range are even.

By Lemma 6.1(ii), an even perfect polynomial is divisible by $T(T+1)$. Hence, the seeds $T, T^2, T^3, \ldots$ eventually capture all indecomposable even perfect polynomials. Using a tilde to denote the automorphism of $\mathbf{F}_2[T]$ swapping T and $T+1$, we have from Lemma 6.1(i) that A is perfect if and only if $\tilde{A}$ is perfect. Now either A or $\tilde{A}$ is such that their largest-degree divisor of the form $T^\alpha(T+1)^\beta$ has $\alpha \le \beta$; if we assume that $\deg A \le 200$, then $\alpha \le 100$.

Thus, if A is indecomposable, even, and perfect of degree at most 200, then either A or $\tilde{A}$ will be found by starting with one of the seeds $T, T^2, \ldots, T^{100}$. Hence, $\mathcal{E} \cup \tilde{\mathcal{E}}$ (with the obvious meaning for $\tilde{\mathcal{E}}$) contains all indecomposable perfect polynomials of degree ≤ 200. It is easily checked that $\tilde{\mathcal{E}} = \mathcal{E}$. Hence, $\mathcal{E} \cup \tilde{\mathcal{E}} = \mathcal{E}$, and so all indecomposable, non-splitting perfect polynomials of degree ≤ 200 are already on Canaday's list.

We finish the proof by observing that there are no non-indecomposable perfect polynomials of degree in $[1, 200]$: By Lemma 5.1, every perfect polynomial factors into pairwise coprime indecomposable perfects. But all nonconstant perfect polynomials of degree ≤ 200 are even, and hence share the factor $T(T+1)$. This forces every nonconstant perfect polynomial of degree ≤ 200 to be indecomposable. □

Remark. Source code for the programs used in the proofs of Theorems 1.2 and 1.3 is available from the second author upon request.

Acknowledgements

The first and third author would like to thank the Richter Scholar Summer Research Program at Lake Forest College for financial support. The second author is partially supported by NSF award DMS-1402268. The third author would also

like to thank the I2M Math Laboratory of Aix-Marseille Université for hosting the author while working on the paper.

References

[1] E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. J. **8** (1941), 721–737. MR 0005509

[2] L. H. Gallardo, P. Pollack, and O. Rahavandrainy, *On a conjecture of Beard, O'Connell and West concerning perfect polynomials*, Finite Fields Appl. **14** (2008), 242–249. MR 2381490

[3] L. H. Gallardo and O. Rahavandrainy, *Odd perfect polynomials over* $\mathbb{F}_2$, J. Théor. Nombres Bordeaux **19** (2007), 165–174. MR 2332059

[4] ———, *Perfect polynomials over* $\mathbb{F}_4$ *with less than five prime factors*, Port. Math. **64** (2007), 21–38. MR 2298110

[5] ———, *There is no odd perfect polynomial over* $\mathbb{F}_2$ *with four prime factors*, Port. Math. **66** (2009), 131–145. MR 2522765

[6] B. Hornfeck and E. Wirsing, *Über die Häufigkeit vollkommener Zahlen*, Math. Ann. **133** (1957), 431–438. MR 0090600

[7] J. T. B. Beard, Jr., J. R. O'Connell, Jr., and K. I. West, *Perfect polynomials over* GF(q), Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **62** (1977), 283–291. MR 497649

[8] R. Lidl and H. Niederreiter. *Finite fields*. Second edition. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge, 1997. xiv+755 pp. MR 1429394

[9] PARI/GP, version `2.7.5`. `http://pari.math.u-bordeaux.fr/`, Bordeaux, 2015.

[10] P. Pollack, *Revisiting Gauss's analogue of the prime number theorem for polynomials over a finite field*, Finite Fields Appl. **16** (2010), 290–299. MR 2646339

Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, IL 60045, USA

E-mail address: `cengizuc@mx.lakeforest.edu`

Department of Mathematics, University of Georgia, Athens, GA 30602, USA

E-mail address: `pollack@uga.edu`

Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, IL 60045, USA

E-mail address: `trevino@lakeforest.edu`