On the largest irreducible factor of an odd perfect polynomial over $\mathbb{F}_2$

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

hexagon:2611.00030v1

Abstract

A polynomial $A \in \mathbb{F}_2[x]$ is perfect if it equals the sum $\sigma(A)$ of all its divisors, and odd if it is coprime to $x^2 + x$. Canaday conjectured in 1941 that 1 is the only odd perfect polynomial. Known necessary conditions on a counterexample bound its number of distinct irreducible factors ($\omega \geq 5$, Gallardo and Rahavandrainy), its number of irreducible factors counted with multiplicity and its degree ($\Omega \geq 12$ and $\deg A > 200$, Cengiz, Pollack and Treviño), and, when all exponents equal 2, the degree of its smallest irreducible factor (at least 40, Gallardo). We bound a different invariant: every odd perfect polynomial $A \neq 1$ has an irreducible factor of degree at least 20. The proof reduces the question, for each D, to a finite system: if all irreducible factors of A have degree at most D, the exponents of A belong to an explicit finite set, through the cyclotomic factorisation of $\sigma(P^h)$ and the multiplicative order of P modulo the factors of $\sigma(P^h)$. An iterated sieve on the resulting production relations empties for every $D \leq 19$. The computation was carried out twice, by two independent programs, with identical results; the second program is attached as an ancillary file. As a cross-check of the method, the same programs reproduce, by the orbit argument of Gallardo and Rahavandrainy, the exclusion of every prime of degree at most 30 as the smallest factor of a special perfect polynomial, in agreement with the published bounds.

1 Introduction

For $A \in \mathbb{F}_2[x]$ let $\sigma(A)$ be the sum of all the divisors of A (all divisors are monic over $\mathbb{F}_2$). The function σ is multiplicative, and $\sigma(P^h) = 1 + P + \cdots + P^h = (P^{h+1} + 1)/(P + 1)$ for P irreducible. The polynomial A is *perfect* if $\sigma(A) = A$, and *odd* if neither x nor $x + 1$ divides it. Perfect polynomials divisible by x or $x + 1$ are plentiful: $(x^2 + x)^{2^n - 1}$ is perfect for every $n \geq 1$, and eleven further ones are known [1, 2]. The odd case is open.

Conjecture (Canaday [1]). *The only odd perfect polynomial over* $\mathbb{F}_2$ *is* 1.

Let $A \neq 1$ be odd and perfect. The following necessary conditions are known.

- A is a square [1].
- A has at least 5 distinct irreducible factors [4, 5].
- A has at least 12 irreducible factors counted with multiplicity (see [2]), and $\deg A > 200$ [2, Theorem 1.2].
- If A is *special*, that is, $A = S^2$ with S squarefree, then A has at least 10 distinct irreducible factors, each of them of even degree and congruent to 1 modulo $x^2 + x + 1$ [4, Lemma 5.3 and Theorem 5.5]; its irreducible factor of smallest degree has degree at least 30 [4, Theorem 5.5], and in fact at least 40 [3, Theorem 1.2]. Further conditions on the special case are given in [6].

None of these conditions bounds the degree of the *largest* irreducible factor of A in general: a counterexample of very large degree all of whose irreducible factors have small degree is not excluded by them. We exclude it below degree 20.

Theorem 1. *Every odd perfect polynomial $A \neq 1$ over $\mathbb{F}_2$ has an irreducible factor of degree at least 20.*

For $D \geq 2$ let S_D be the set of irreducible polynomials of $\mathbb{F}_2[x]$ of degree between 2 and D, and let E_D be the set of odd perfect polynomials $A \neq 1$ all of whose irreducible factors lie in S_D. Theorem 1 is the statement $E_{19} = \emptyset$. It is obtained in two steps.

Theorem 2. *Let $D \geq 2$ and $T_D = \{t > 1 : \ t \mid 2^m - 1$ for some $m \leq D\}$. Every $A \in E_D$ is of the form $A = \prod_{P \in T} P^{h_P}$ with $T \subseteq S_D$ and $h_P + 1 \in T_D$ for every $P \in T$. In particular E_D is finite.*

Theorem 3. *$E_D = \emptyset$ for every $D \leq 19$.*

Theorem 2 is proved in Section 2. Theorem 3 is a finite computation, described in Section 3; only the case $D = 19$ is needed, since $E_D \subseteq E_{19}$ for $D \leq 19$. Section 4 applies the same programs to the special case, as a check against the published results. Section 5 describes the two independent computations.

Combined with $\omega(A) \geq 5$ and with the fact that A is a square, Theorem 1 only gives $\deg A \geq 2(20 + 2 + 3 + 3 + 4) = 64$, which is weaker than $\deg A > 200$. The two statements bound different invariants and neither implies the other.

2 Notation and the finiteness of E_D

Throughout, P denotes an irreducible polynomial of degree at least 2; such a P satisfies $P(0) = P(1) = 1$. We write $N(k)$ for the number of irreducible polynomials of degree k over $\mathbb{F}_2$, $\Phi_n(Y) \in \mathbb{F}_2[Y]$ for the reduction modulo 2 of the n-th cyclotomic polynomial, φ for Euler's function, $\mathrm{ord}_t(2)$ for the multiplicative order of 2 modulo an odd integer t, and $v_R(B)$ for the exponent of the irreducible R in B. A polynomial is *D-smooth* if all its irreducible factors have degree at most D.

Lemma 4 (Canaday [1])**.** *If $A \neq 1$ is odd and perfect, every exponent $h_P = v_P(A)$ is even.*

Proof. For $P \mid A$ we have $P(0) = 1$, hence $\sigma(P^{h_P})(0) = h_P + 1$ in $\mathbb{F}_2$. Since A is odd, $A(0) = 1$, and $1 = \sigma(A)(0) = \prod_{P \mid A}(h_P + 1)$ in $\mathbb{F}_2$. Every $h_P + 1$ is therefore odd. □

Lemma 5. *Let P be irreducible of degree at least 2, $h \geq 2$ even, and $t = h + 1$.*

(i) $\sigma(P^h) = \prod_{d \mid t,\, d>1} \Phi_d(P)$, and the factors $\Phi_d(P)$ are pairwise coprime.

(ii) If $d > 1$ is odd and Q is an irreducible factor of $\Phi_d(P)$, then $Q \neq P$, and the multiplicative order of P modulo Q equals d. In particular $d \mid 2^{\deg Q} - 1$.

(iii) If $d > 1$ is odd, $\Phi_d(P)$ is divisible neither by x nor by $x + 1$.

Proof. (i) In $\mathbb{F}_2[Y]$ one has $(Y^t - 1)/(Y - 1) = \prod_{d \mid t,\, d>1} \Phi_d(Y)$. Since t is odd, $Y^t - 1$ is separable, so the $\Phi_d(Y)$ are squarefree and pairwise coprime; a Bézout relation $U\Phi_d + V\Phi_e = 1$ in $\mathbb{F}_2[Y]$ remains one after the substitution $Y = P$. (ii) For $d \geq 2$ the constant term of the cyclotomic polynomial Φ_d is 1, so $\Phi_d(P) \equiv 1 \pmod P$ and $Q \neq P$. In the field $\mathbb{F}_2[x]/(Q)$ the class of P is a root of Φ_d; as $Y^d - 1$ is separable, the roots of Φ_d are exactly the elements of order d, and d divides the order $2^{\deg Q} - 1$ of the multiplicative group. (iii) Since $P(0) = P(1) = 1$, both values $\Phi_d(P)(0)$ and $\Phi_d(P)(1)$ equal $\Phi_d(1)$ reduced modulo 2. Now $\Phi_d(1)$ is a prime q if d is a power of q, and 1 otherwise; d being odd, $\Phi_d(1)$ is odd. □

Lemma 6. *Let $A \in E_D$ and $P \mid A$. Then h_P+1 divides 2^m-1 for some $m \le D$; in particular $h_P \le 2^D-2$.*

Proof. By Lemma 4, $t = h_P+1 \ge 3$ is odd. Since σ is multiplicative, $\sigma(P^{h_P})$ divides $\sigma(A) = A$ and is therefore D-smooth. By Lemma 5(i), $\Phi_t(P)$ divides $\sigma(P^{h_P})$; it has degree $\varphi(t)\deg P \ge 2$, hence an irreducible factor Q with $\deg Q \le D$, and Lemma 5(ii) gives $t \mid 2^{\deg Q}-1$. □

Proof of Theorem 2. The irreducible factors of $A \in E_D$ lie in S_D by definition, and $h_P+1 \in T_D$ by Lemma 6. Both sets are finite. □

Remark 7. Lemma 4 is what makes E_D finite. In the even case, $\sigma(x^{2^n-1}) = (x+1)^{2^n-1}$, and the exponents of the perfect polynomials $(x^2+x)^{2^n-1}$ are unbounded.

The next lemma discards most pairs (P,h) without any polynomial computation.

Lemma 8. *Let P be irreducible of degree $p \ge 2$, let $t > 1$ be odd, $m = \mathrm{ord}_t(2)$, and*

$$B(t,D) = \sum_{j\ge 1,\ jm\le D} jm\, N(jm).$$

If $\Phi_t(P)$ is D-smooth, then $\varphi(t)\,p \le B(t,D)+\varepsilon$, where $\varepsilon = p-1$ if $m \le p-1$ and $\varepsilon = 0$ otherwise.

Proof. By Lemma 5(ii), every irreducible factor Q of $\Phi_t(P)$ satisfies $t \mid 2^{\deg Q}-1$, that is, $m \mid \deg Q$. Write $\Phi_t(P) = \prod_Q Q^{k_Q}$. If $k_Q \ge 2$, then $Q^{k_Q} \mid P^t-1$, and Q^{k_Q-1} divides the derivative $tP^{t-1}P' = P^{t-1}P'$; as $Q \ne P$, $Q^{k_Q-1} \mid P'$. The polynomials Q^{k_Q-1} being pairwise coprime, their product divides P', which is non-zero because P is separable; hence $\sum_Q (k_Q-1)\deg Q \le p-1$. A repeated factor has degree divisible by m and at most $p-1$, so there is none when $m > p-1$. Finally $\varphi(t)p = \deg \Phi_t(P) = \sum_Q \deg Q + \sum_Q (k_Q-1)\deg Q$, where the first sum runs over distinct irreducibles of degrees divisible by m and at most D, and is therefore at most $B(t,D)$. □

Remark 9. If $t = 2^D-1$ is prime, then $m = D$ and $B(t,D) = D\,N(D) = 2^D-2$, whereas $\varphi(t)p = (2^D-2)p$. Lemma 8 therefore discards the exponent $h = 2^D-2$ for every P; for $D = 13$ this concerns $\sigma(P^{8190})$, of degree $8190\deg P$.

3 The sieve and Theorem 3

Fix D. A pair (P,h) with $P \in S_D$ and $h+1 \in T_D$ is *admissible* if $\sigma(P^h)$ is D-smooth; it is then odd, by Lemma 5(iii). Its *production* is the factorisation $\sigma(P^h) = \prod_R R^{e_R(P,h)}$, computed factor by factor through Lemma 5(i). We say that (P,h) *produces* R if $e_R(P,h) > 0$. Since $\Phi_d(P) \equiv 1 \pmod P$, a pair never produces its own prime.

A polynomial $A = \prod_{P\in T} P^{h_P}$ is perfect if and only if $\sum_{P\in T} e_R(P,h_P) = v_R(A)$ for every irreducible R. Starting from all primes of S_D and all admissible pairs, we iterate the following three rules until nothing changes:

(R1) a pair dies if its prime is dead or if it produces a dead prime;

(R2) a prime dies if no living pair has it as first coordinate;

(R3) a prime dies if no living pair produces it.

Proposition 10. *Let $A \in E_D$. No prime dividing A and no pair $(P, v_P(A))$ with $P \mid A$ is ever killed. In particular, if the sieve empties, then $E_D = \emptyset$.*

Proof. For $P \mid A$ the pair (P, h_P) is admissible: $h_P + 1 \in T_D$ by Lemma 6, and $\sigma(P^{h_P})$ divides $\sigma(A) = A$, so it is D-smooth and all the primes it produces divide A. Assume that, before some iteration, all these primes and pairs are alive. Rule (R1) spares (P, h_P), since the primes it produces divide A. Rule (R2) spares P, which carries the pair (P, h_P). For (R3), comparing exponents of P in $\sigma(A) = A$ gives $\sum_{Q|A} e_P(Q, h_Q) = h_P > 0$ with $e_P(P, h_P) = 0$, so some $Q \mid A$, $Q \neq P$, produces P through a living pair. As $A \neq 1$, the sieve does not empty. □

Had the sieve not emptied, an exhaustive search over the surviving primes and exponents would have been needed; it never was.

Proof of Theorem 3. For each $D \leq 19$ the admissible pairs were computed and the sieve was run to its fixed point. It empties in every case. Table 1 gives the counts. □

D	$\lvert S_D\rvert$	pairs	iter.	D	$\lvert S_D\rvert$	pairs	iter.
2	1	0	1	11	410	164	4
3	3	0	1	12	745	418	4
4	6	4	2	13	1375	550	4
5	12	4	2	14	2536	1086	5
6	21	10	3	15	4718	1682	5
7	39	12	3	16	8798	3668	5
8	69	39	3	17	16508	5598	5
9	125	55	3	18	31040	12277	6
10	224	118	4	19	58634	19351	6

Table 1: The sieve of Section 3: number of primes in S_D, number of admissible pairs, and number of iterations until the sieve is empty.

Proof of Theorem 1. If every irreducible factor of an odd perfect $A \neq 1$ had degree at most 19, then A would lie in E_{19}, which is empty by Theorem 3. □

4 A cross-check: the special case

Let A be special, $A = \prod_{P \in T} P^2$ with T a finite set of irreducibles. Then $\sigma(P^2) = \Phi_3(P) = P^2 + P + 1$ is the only function involved, and $\sigma(A) = A$ implies that every irreducible factor of $\Phi_3(P)$, for $P \in T$, belongs to T. Every $P \in T$ has even degree and satisfies $P \equiv 1 \pmod{x^2 + x + 1}$ [4, Lemma 5.3]. (The parity of the degree also follows from Lemma 5: P divides $A = \sigma(A)$ and $\Phi_3(P) \equiv 1 \pmod{P}$, so P divides some $\Phi_3(Q)$, and then $3 \mid 2^{\deg P} - 1$.)

Let $P \in T$ be of smallest degree d. Define $O_0 = \{P\}$ and let O_k be the set of irreducible factors of the polynomials $\Phi_3(R)$, $R \in O_{k-1}$. All the O_k are contained in T, so every element of every O_k has even degree at least d and is congruent to 1 modulo $x^2 + x + 1$. This is the argument of [4, Corollary 5.4]. We say that P *survives to depth* k if the elements of $O_1, \ldots, O_k$ satisfy these three conditions.

Running this test on every irreducible P of even degree $d \leq 30$ with $P \equiv 1 \pmod{x^2+x+1}$ gives Table 2. The column "rough" counts the P for which $\Phi_3(P)$ has no irreducible factor of degree less than d. No P survives to depth 4. For $d = 2$ the only candidate, $x^2 + x + 1$, is not congruent to 1, and odd degrees do not occur.

Corollary 11. *No irreducible polynomial of degree at most* 30 *is the factor of smallest degree of a special perfect polynomial.*

d	$P \equiv 1$	rough	survivors to depth $1, 2, 3, \ldots$
4	1	1	0
6	3	2	2, 0
8	10	4	4, 0
10	33	11	8, 2, 0
12	111	24	20, 6, 0
14	387	82	75, 4, 0
16	1360	338	317, 29, 0
18	4842	894	843, 62, 0
20	17459	2897	2696, 186, 0
22	63519	9915	9335, 526, 0
24	232950	33464	31694, 1721, 12, 0
26	860265	110419	105161, 5155, 8, 0
28	3195465	380186	363023, 16803, 32, 0
30	11930067	1322127	1266736, 53693, 128, 0

Table 2: The orbit test of Section 4, for every irreducible P of degree d congruent to 1 modulo $x^2 + x + 1$.

This is contained in the published results: [4, Theorem 5.5] covers the degrees up to 28, and [3, Theorem 1.2 and Lemma 2.6] extends the bound to 40. We record it only as an independent check, by a different procedure, of the degrees $d \leq 30$. With the three conditions above, depth 3 does not suffice from $d = 24$ on. For $d = 28$ and $d = 30$ the first of the two computations of Section 5 tested depth 4 directly; the intermediate counts in Table 2 come from the second.

5 The computations

Polynomials over $\mathbb{F}_2$ are encoded as integers, bit i being the coefficient of x^i; all computations are exact. Theorem 3 and Table 2 were obtained twice.

First computation (July 2026). A self-contained Python engine generated the irreducible polynomials by trial division, computed the admissible pairs through Lemmas 5 and 8 with a weaker form of the latter, and decided smoothness by a chain of gcds with $x^{2^k} - x$ followed by equal-degree splitting, every factor being checked against the list of irreducibles. The orbit test used the same arithmetic, with the factorisations of the deep levels done by the FLINT library and re-checked by exact reconstruction and a Rabin irreducibility test. For $D \in \{6, 10, 13\}$ an end-to-end reimplementation on FLINT primitives gave the same pairs and productions.

Second computation (October 2026). The ancillary file `VERIFY_canaday.py` redoes everything with different algorithms: the irreducibles, and in the special case the candidates P and the rough check, come from a Rabin test and a product-of-gcds test written in vectorised integer arithmetic; smoothness of $\Phi_t(P)$ is decided by the criterion that a squarefree h is D-smooth if and only if it divides $\prod_{D/2 \leq i \leq D}(x^{2^i} - x)$; smooth polynomials are factored by FLINT, and the factorisation is accepted only if its product is the polynomial and every factor belongs to the list of irreducibles. The factorisations of the orbit test are accepted only after exact reconstruction and a Rabin test of every factor. The script also checks Lemma 6 by computing $\sigma(P^h)$ directly for all even $h \leq 2^D - 2$, $D \leq 6$, checks that Lemma 8 does not change the admissible pairs for $D \leq 12$, and recovers by brute force the perfect polynomials of degree at most 16 (twelve of them, none odd). Every count in Tables 1 and 2 is printed by the script and compared with the tables; the two computations agree on all of them.

Running `python3 VERIFY_canaday.py` takes less than a minute and covers $D \leq 13$ and $d \leq 22$; `python3 VERIFY_canaday.py full` covers the whole of both tables (about two hours on one core). The script needs Python 3 with `numpy` and `python-flint`.

Acknowledgements. Technical assistance: Claude (Anthropic).

References

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

[2] U. C. Cengiz, P. Pollack and E. Treviño, *Counting perfect polynomials*, Finite Fields Appl. **47** (2017), 242–255.

[3] L. H. Gallardo, *On the equation* $\prod_P \Phi_3(P) = \prod_P P^2$ *over* $\mathbb{F}_2[x]$, Gulf J. Math. **12** (2022), no. 2, 39–48.

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

[5] L. H. Gallardo and O. Rahavandrainy, *There is no odd perfect polynomial over* $\mathbb{F}_2$ *with four prime factors*, Port. Math. **66** (2009), 131–145.

[6] O. Rahavandrainy, *On special perfect polynomials over* $\mathbb{F}_2$, arXiv:2606.08640, 2026.