hexagon:2611.00025v1

The invariant c_M of Gallardo and Rahavandrainy at Mersenne prime exponents, and the case $p = 7$

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

Abstract

A Mersenne prime polynomial is an irreducible polynomial over $\mathbb{F}_2$ of the form $x^a(x+1)^b+1$ with $a, b \geq 1$. Gallardo and Rahavandrainy conjectured that, apart from two exceptions, $\sigma(M^{2h})$ always has an irreducible factor which is not a Mersenne prime. For a prime $p \geq 5$ they proved it for every M outside an exceptional set $\Sigma_p = \Sigma_p^1 \cup \cdots \cup \Sigma_p^4$, defined through an integer c_M and an odd integer m_M read off the leading coefficients of $\sigma(\sigma(M^{p-1}))$, and later they proved it for every Mersenne prime number $p \geq 31$; their method does not reach $p = 7$. We compute c_M exactly when $p = 2^d - 1$ is a Mersenne prime number: $c_M = d + 1$ if $\deg M \neq d$, and $c_M = d$ if $\deg M = d$. Consequently Σ_p^1 consists of the Mersenne primes of degree d or $d+1$, Σ_p^2 is empty, and Σ_p^3, Σ_p^4 are described by $m_M = \deg M - d - 1$ and $m_M = \deg M - d$ respectively. For $p = 7$ this reduces the conjecture to the Mersenne primes M with $m_M \in \{\deg M - 4, \deg M - 3\}$. A direct computation shows that $\sigma(M^6)$ has a non-Mersenne irreducible factor for every Mersenne prime M of degree at most 500, and that $m_M \leq 17$ in that range. Hence the conjecture holds whenever 7 divides $2h+1$ and $\deg M \leq 500$, and a counterexample with $7 \mid 2h+1$ would need $m_M \geq \deg M - 4 > 496$. A script attached as an ancillary file checks these computations, and reproduces the table of exceptional sets of Gallardo and Rahavandrainy.

1 Introduction

For $A \in \mathbb{F}_2[x]$ let $\sigma(A)$ be the sum of the divisors of A. A *Mersenne prime* is an irreducible polynomial $M = x^a(x+1)^b + 1$ with $a, b \geq 1$; we write $\mathcal{M}$ for the set of Mersenne primes. Mersenne primes play a central role in the classification of even perfect polynomials over $\mathbb{F}_2$ [1], where the following statement is a recurring obstacle.

Conjecture 1 (Gallardo–Rahavandrainy [2, Conjecture 1.2])**.** Let $h \geq 1$ and $M \in \mathcal{M}$, with $M \notin \{1+x+x^3, 1+x^2+x^3\}$ or $h \geq 2$. Then $\sigma(M^{2h})$ is divisible by an irreducible polynomial which is not a Mersenne prime.

If p is a prime dividing $2h+1$, then $\sigma(M^{p-1}) = (M^p - 1)/(M - 1)$ divides $\sigma(M^{2h})$, so it suffices to treat $2h + 1 = p$ prime. Put

$$S = \sigma(M^{p-1}) = \Phi_p(M), \qquad U = \sigma(S), \qquad W = U + S + 1,$$

where Φ_p is the p-th cyclotomic polynomial. Following [2], let $\alpha_l(F)$ be the coefficient of $x^{\deg F - l}$ in F,

$$c_M = (p-1)\deg M - \deg W = \deg S - \deg W,$$

and, when $\deg W$ is even, let m_M be the least odd l with $\alpha_l(W) = 1$. With $n = \deg M$, the exceptional sets of [2] are

$$\begin{aligned}
\Sigma_p^1 &= \{M \in \mathcal{M} : \ c_M = n\},\\
\Sigma_p^2 &= \{M \in \mathcal{M} : \ c_M = n+1, \ c_M \text{ odd}\},\\
\Sigma_p^3 &= \{M \in \mathcal{M} : \ c_M + m_M = n, \ c_M \text{ even}\},\\
\Sigma_p^4 &= \{M \in \mathcal{M} : \ c_M + m_M = n+1, \ c_M \text{ even}, \ m_M \geq 3\},
\end{aligned}$$

and $\Sigma_p = \Sigma_p^1 \cup \Sigma_p^2 \cup \Sigma_p^3 \cup \Sigma_p^4$. Gallardo and Rahavandrainy proved that for $p \geq 5$ prime and $M \notin \Sigma_p$, $\Phi_p(M)$ has a non-Mersenne irreducible factor [2, Theorem 1.1], and tabulated the sizes of the Σ_p^j for small p [2, Table 1]. In [1, Proposition 1.1] they settled the conjecture whenever $2h+1$ has a prime divisor in an explicit set which contains every Mersenne prime number other than 7, and every prime p with $\mathrm{ord}_p(2) \equiv 0 \pmod 8$; for a Mersenne prime number $p \geq 31$ this is [1, Lemma 4.17]. The case $p = 7$ is left open there.

Our main result computes c_M when p is a Mersenne prime number.

Theorem 2. *Let $d \geq 3$ be such that $p = 2^d - 1$ is prime, and let M be a Mersenne prime of degree n. Then*

$$c_M = \begin{cases} d+1 & \text{if } n \neq d, \\ d & \text{if } n = d. \end{cases}$$

Corollary 3. *Under the hypotheses of Theorem 2,*

- *Σ_p^1 is the set of Mersenne primes of degree d or $d+1$;*
- *$\Sigma_p^2 = \emptyset$;*
- *$\Sigma_p^3 = \{M \in \mathcal{M} : \ \deg M \neq d, \ m_M = \deg M - d - 1\}$ and $\Sigma_p^4 = \{M \in \mathcal{M} : \ \deg M \neq d, \ m_M = \deg M - d, \ m_M \geq 3\}$.*

For $p \geq 31$ the conjecture is already known [1], and Corollary 3 only describes the exceptional sets of [2, Theorem 1.1]. For $p = 7$ it gives the following reduction, which we complete by a computation in Section 3.

Corollary 4. *Let $M \in \mathcal{M}$. If $\sigma(M^6)$ has no irreducible factor other than Mersenne primes, then either $\deg M \in \{3, 4\}$, or $m_M \in \{\deg M - 4, \ \deg M - 3\}$.*

Proposition 5. *For every Mersenne prime M with $\deg M \leq 500$, $\sigma(M^6)$ has an irreducible factor which is not a Mersenne prime. In that range $m_M \leq 17$, and Σ_7 consists of the four Mersenne primes of degree 3 and 4 (in Σ_7^1), the two of degree 6 in Σ_7^4, and two of degree 7 in Σ_7^3.*

Consequently, Conjecture 1 holds for every h with $7 \mid 2h+1$ and every M of degree at most 500; beyond, a counterexample with $7 \mid 2h+1$ would need $m_M \geq \deg M - 4 > 496$.

2 Proof of Theorem 2

We work in the field $\mathbb{F}_2((1/x))$ of Laurent series in $1/x$, where every non-zero polynomial F is invertible and $F^{-1} = x^{-\deg F}(1 + O(x^{-1}))$.

Lemma 6. *Let $S = P_1 \cdots P_k$ be a product of distinct irreducible polynomials, $r = \min_i \deg P_i \geq 2$, κ the number of i with $\deg P_i = r$, and $T = \sigma(S) + S$. In T/S, the coefficient of x^{-j} vanishes for $j < r$ and equals $\kappa \bmod 2$ for $j = r$. If no P_i has degree $r+1$, the coefficient of x^{-r-1} equals $\sum_{\deg P_i = r} a_i \bmod 2$, where a_i is the coefficient of x^{r-1} in P_i. In particular $\deg T = \deg S - r$ when κ is odd.*

Proof. As S is squarefree, $\sigma(S) = \prod_i (1 + P_i)$ and $T/S = \prod_i (1 + P_i^{-1}) - 1 = \sum_{\emptyset \neq I} \prod_{i \in I} P_i^{-1}$. A product over $|I| \geq 2$ has valuation at least $2r \geq r+2$. A single P_i^{-1} with $\deg P_i \geq r+2$ starts at x^{-r-2}, and for $\deg P_i = r$ one has $P_i^{-1} = x^{-r}(1 + a_i x^{-1} + O(x^{-2}))$. Finally $T = S \cdot (T/S)$. $\square$

Proof of Theorem 2. Since $p = 2^d - 1$ is prime, d is prime, hence odd as $d \geq 3$, and $\mathrm{ord}_p(2) = d$. Recall that $S = \Phi_p(M)$ is squarefree [2, Lemma 2.3].

Degrees of the factors. Let γ be a root of S in an algebraic closure of $\mathbb{F}_2$. Then $M(\gamma)^p = 1$, and $M(\gamma) \neq 1$ since $\Phi_p(1) = p$ is odd. So $M(\gamma)$ has multiplicative order p in $\mathbb{F}_2(\gamma)^\times$, and $d = \mathrm{ord}_p(2)$ divides $[\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. Every irreducible factor of S has degree divisible by d; in particular there is none of degree $d+1$.

The factors of degree d. As d is prime, the elements of $\mathbb{F}_{2^d} \setminus \mathbb{F}_2$ are exactly the roots of the $N = (2^d - 2)/d$ irreducible polynomials of degree d, each root once. Let $\beta \in \mathbb{F}_{2^d} \setminus \mathbb{F}_2$ with $M(\beta) \neq 0$. Then $M(\beta) \neq 1$, for otherwise $\beta^a(\beta+1)^b = 0$; and $M(\beta)^p = 1$ since $\mathbb{F}_{2^d}^\times$ has order p. As p is prime, $M(\beta)$ is a root of Φ_p, that is, $S(\beta) = 0$. If $M(\beta) = 0$, then $S(\beta) = \Phi_p(0) = 1$. Hence the irreducible factors of degree d of S are the irreducible polynomials of degree d other than M (this is [1, Corollary 4.4]), and their number is $\kappa = N$ if $n \neq d$, $\kappa = N - 1$ if $n = d$. By Fermat's little theorem d divides $2^{d-1} - 1$, so $N = 2(2^{d-1} - 1)/d$ is even.

Case $n = d$. Then κ is odd, the smallest degree of a factor is d, and Lemma 6 gives $\deg T = \deg S - d$, where $T = \sigma(S) + S = W + 1$.

Case $n \neq d$. Then $\kappa = N$ is even and the coefficient of x^{-d} in T/S vanishes. The coefficient of x^{-d-1} is the sum of the coefficients of x^{d-1} of all irreducible polynomials of degree d, that is, the sum of their roots, which is $\sum_{\beta \in \mathbb{F}_{2^d}} \beta - (0+1) = 1$. Hence $\deg T = \deg S - d - 1$.

In both cases $\deg T \geq 1$, so $\deg W = \deg T$ and $c_M = \deg S - \deg W$ has the stated value. □

Proof of Corollary 3. If $n = d$, then $c_M = d = n$ is odd: $M \in \Sigma_p^1$, and M lies in none of the other sets, which require $c_M = n + 1$ or c_M even. If $n \neq d$, then $c_M = d + 1$ is even, $M \in \Sigma_p^1$ if and only if $n = d + 1$, $M \notin \Sigma_p^2$, and the conditions defining Σ_p^3 and Σ_p^4 become $m_M = n - d - 1$ and $m_M = n - d$, $m_M \geq 3$. □

Proof of Corollary 4. Apply [2, Theorem 1.1] with $p = 7$, $d = 3$, and Corollary 3. □

Remark 7. The two Mersenne primes of degree 3 are the exceptions of Conjecture 1 for $h = 1$; for $p = 7$ they lie in Σ_7^1. The method of [1] uses an irreducible factor of degree $\mathrm{ord}_p(2)$ of $\Phi_p(M)$ which is not a Mersenne prime; for $p = 7$ both irreducible polynomials of degree 3 are Mersenne primes, which is why that case stays open.

3 The case $p = 7$

Proof of Proposition 5. For each pair (a, b) with $a, b \geq 1$ and $a + b \leq 500$ such that $M = x^a(x+1)^b + 1$ is irreducible, we factored $S = \Phi_7(M)$, which has degree $6 \deg M$, computed U, W, c_M and m_M, and checked that some irreducible factor P of S is not a Mersenne prime, that is, $P + 1$ is not of the form $x^i(x+1)^j$. Table 1 gives the largest value of m_M and the degrees at which it is first reached, and the members of Σ_7 found. □

Mersenne primes M with $2 \leq \deg M \leq 500$	1203
largest m_M	17
first degree with $m_M = 3, 5, 7, 9, 11, 13, 15, 17$	2, 7, 5, 44, 84, 177, 201, 425
Σ_7^1	$\deg M \in \{3, 4\}$ (four polynomials)
Σ_7^3	$x^3(x+1)^4 + 1$, $x^4(x+1)^3 + 1$
Σ_7^4	$x(x+1)^5 + 1$, $x^5(x+1) + 1$

Table 1: The computation of Proposition 5 ($p = 7$).

The members of $\Sigma_7^3 \cup \Sigma_7^4$ of degree between 5 and 100 agree with the counts 2 and 2 of [2, Table 1]. In the range computed m_M grows very slowly; Corollary 4 shows that a bound $m_M < \deg M - 4$ for all Mersenne primes of degree larger than 500 would settle Conjecture 1 for every h with $7 \mid 2h + 1$.

4 Verification

The ancillary file `VERIFY_mersenne7.py` (Python 3 with `python-flint`) checks: Theorem 2 for $p = 7$ ($\deg M \leq 40$), $p = 31$ ($\deg M \leq 24$), $p = 127$ ($\deg M \leq 12$) and $p = 8191$ ($\deg M \leq 3$), together with the two facts used in its proof and the parity of κ; Corollary 3 on the same data; all thirteen rows of [2, Table 1], which it reproduces exactly; and Proposition 5. Every factorisation used for Theorem 2 and Proposition 5 is accepted only if its product is the polynomial and every factor passes a Rabin irreducibility test. The default run takes less than a minute; `python3 VERIFY_mersenne7.py full` takes less than half an hour.

Acknowledgements. Technical assistance: Claude (Anthropic).

References

[1] L. H. Gallardo and O. Rahavandrainy, *All even (unitary) perfect polynomials over $\mathbb{F}_2$ with only Mersenne primes as odd divisors*, Kragujevac J. Math. **49** (2025), no. 4, 639–652.

[2] L. H. Gallardo and O. Rahavandrainy, *Factorization of cyclotomic polynomial values at Mersenne prime polynomials*, Mat. Vesnik, published online 2025, doi:10.57016/MV-HMLV9f07; arXiv:2106.10008.