International Electronic Journal of Algebra
Volume 28 (2020) 1-8
DOI: 10.24330/ieja.768086

MASON-STOTHERS THEOREM AND PERFECT BINARY POLYNOMIALS

Luis H. Gallardo

Received: 16 February 2019; Revised: 10 December 2019; Accepted: 14 March 2020
Communicated by Abdullah Harmancı

Abstract. We prove that there is no perfect binary polynomial R that is the sum of two appropriate powers, besides, possibly $R = P+1$ with P irreducible. The proofs follow from analogue results involving the ABC-theorem for polynomials and a classical identity.

Mathematics Subject Classification (2020): 11T55, 11T06
Keywords: Polynomial ABC-theorem, binary polynomial, perfect polynomial

1. Introduction

A perfect number n is a positive integer such that the sum of all its divisors including 1 and n equals $2n$. For example, $n = 6$ and $n = 28$ are perfect numbers. It is conjectured that there is an infinity of perfect numbers and that all of them are even. Deep computations have resulted in more known examples. However, essentially, we only know two main theoretical results about them, namely (a) all even perfect numbers have exactly two prime divisors, more precisely, the even perfect numbers are exactly the integers of the form $2^{p-1}(2^p - 1)$ with $2^p - 1$ prime, and (b) all, if any exist, odd perfect numbers are products of powers of primes p^{4k+1} by perfect squares. Beginning with E. F. Canaday (see [2]), the first doctoral student of Leonard Carlitz, the study of an analogous problem over polynomials instead of numbers, started in 1941. More precisely, let $A \in \mathbb{F}_2[x]$ be a binary polynomial. We say that A is perfect if and only if A equals the sum of all its divisors including 1 and A. We also say that a binary polynomial $B \in \mathbb{F}_2[x]$ is *even* if $B(1) = 0$ or $B(0) = 0$, and we say that a polynomial that is not even is *odd*. In other words, B odd means that $B(0) = 1$ and $B(1) = 1$. Canaday found the infinite family of even perfect polynomials $(x(x+1))^{2^n-1}$ where $n = 0, 1, 2, \ldots$ and called them "trivial". He also found a list of 11 non-trivial perfect polynomials, that we call *sporadic* (see Proposition 2.1 below), all of them even, of degrees between 5 and 20. He says furthermore, that it seems plausible that no odd perfect polynomial can exist but that this is not proved. No new perfect

polynomial has been discovered since besides the efforts of Beard et al.[1], Gallardo and Rahavandrainy [6,7,8,9,10], Cengiz et al.[3]. On the other hand, the polynomial ABC-theorem, i.e., Mason-Stothers theorem (see [11, pp. 194-195]), is a nice result about polynomials (see Lemma 2.4 below for details) that essentially says that if one has two coprime polynomials in one variable over a field K, besides the case where both these polynomials are p-th powers, where p is the characteristic of the field K, the degree of the product of all prime (irreducible) polynomials that divide their sum cannot be too small in terms of the degrees of both polynomials.

In the present paper, by considering possible perfect polynomials that are (essentially) sums of two powers, (generalizing the "trivial" family described above) we extend the number of cases for which we know that perfect binary polynomials cannot exist and, moreover, we propose a conjecture that seems non-trivial.

More precisely, we prove in Theorem 1.1 that we cannot build odd perfect polynomials by adding to a polynomial that splits in $\mathbb{F}_2$ (e.g., a "trivial" perfect polynomial) any power of another polynomial. While our result in Theorem 1.2 characterizes the even perfect polynomials of the form $P+1$, where P is irreducible, as the only perfect polynomials that are sums of two appropriate powers of binary polynomials.

Our first result is

Theorem 1.1. *There is no odd perfect binary polynomial R of the form $R = x^k(x+1)^l + M^t$ in which $M \in \mathbb{F}_2[x]$, $t > 1$ is an integer, k, l are non-negative integers, and k, l are not both even.*

Our second result is

Theorem 1.2. *Assume that a perfect binary polynomial R satisfies the condition:*

$$R^m = P^k + S^n \tag{1}$$

in which P is a prime (irreducible) binary polynomial, S a binary polynomial, not divisible by P and n, k, m are non-negative integers with $m \geq 1$, $k \geq 1$ such that P^k and S^n are not both squares in $\mathbb{F}_2[x]$, and one has either $n = 0$ and $\deg(R) \leq \deg(P)$, or $n \neq 0$ and

$$\frac{1}{m} + \frac{1}{n} \leq \frac{1}{2}, \tag{2}$$

$$\deg(R) \geq \deg(P), \tag{3}$$

and

$$\gcd(m, n\deg(S)) = 1. \tag{4}$$

Then

$$R = P + 1. \tag{5}$$

Moreover, R is even perfect.

Our conjecture is

Conjecture 1.3. *The only even perfect binary polynomials $R \in \mathbb{F}_2[x]$ such that $R+1$ is prime are*

$$R_0(x) := x^2 + x, R_1(x) := x^5 + x^2 \text{ and } R_2(x) := x^5 + x^4 + x^2 + x. \tag{6}$$

Remark 1.4. Clearly $R_0(x)$ satisfies the conjecture. It is not difficult to check that of the 11 known sporadic perfect binary polynomials (see Proposition 2.1), $R_1(x)$ and $R_2(x) = R_1(x+1)$ are the only that satisfy the conjecture. While for any, say T, of the trivial even perfect binary polynomials, with $\deg(T) > 2$, $T+1$ is always reducible (indeed, it has x^2+x+1 as a prime factor). Moreover, from computations in [3] it is known that the conjecture holds when $\deg(R) \leq 200$.

For information on the analogue of the conjecture over the integers, the reader may check [4] as well as [5].

In Section 2, one finds the necessary tools (Lemma 2.5 and Lemma 2.7) that essentially prove our main results. However, for clarity, both theorems are proved in Section 3.

2. Tools

The list of all known sporadic perfect binary polynomials (see [1,2,3]) is:

Proposition 2.1. *Let* $P_2 := x^2+x+1, P_{3a} := x^3+x+1, P_{3b} := P_{3a}(x+1) = x^3+x^2+1, P_{4a} := x^4+x^3+1, P_{4b} := P_{4a}(x+1) = x^4+x^3+x^2+x+1, P_{4c} := x^4+x+1$.

The 11 known sporadic perfect polynomials over $\mathbb{F}_2[x]$ are

(a) *degree 5:* $x(x+1)^2P_2, x^2(x+1)P_2$,
(b) *degree 11:* $x(x+1)^2P_2^2P_{4c}, x^2(x+1)P_2^2P_{4c}, x^3(x+1)^4P_{4a}, x^4(x+1)^3P_{4b}$,
(c) *degree 15:* $x^3(x+1)^6P_{3a}P_{3b}, x^6(x+1)^3P_{3a}P_{3b}$,
(d) *degree 16:* $x^4(x+1)^4P_{4a}P_{4b}$,
(e) *degree 20:* $x^4(x+1)^6P_{3a}P_{3b}P_{4b}, x^6(x+1)^4P_{3a}P_{3b}P_{4a}$.

A simple, but important property of binary polynomials is

Lemma 2.2. *Let B be a binary polynomial. Then there exist unique binary polynomials B_1 and B_2 such that*

$$B = B_1^2 + xB_2^2.$$

Proof. Observe that $f\colon \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ defined by $f(t) = t^2$ is one to one since $f(t) = f(u)$ implies $0 = t^2 - u^2 = (t-u)^2$, so that $t = u$. Thus, in order to define B_1 and B_2, it is only necessary to define B_1^2 and B_2^2 as appropriate squares in $\mathbb{F}_2[x]$. Observe also that the formal derivative $M^{'}$ of any binary polynomial M is a square in $\mathbb{F}_2[x]$ and that the formal derivative of a square in $\mathbb{F}_2[x]$ is equal to 0. Put $B_2^2 := B^{'}$, the formal derivative of B. Put also $B_1^2 := (xB)^{'}$. This proves the existence and uniqueness of both B_1 and B_2. □

The following classical lemma (see [2]) is useful.

Lemma 2.3. *If A is an odd perfect binary polynomial then A is a square in $\mathbb{F}_2[x]$.*

The following lemma is the ABC theorem for binary polynomials. The proof is the same as Lang's proof of Mason-Stothers theorem [11, Theorem 7.1], which works in any characteristic.

Lemma 2.4. *Let a, b, c be relatively prime polynomials in $\mathbb{F}_2[x]$ such that $a+b=c$ and a, b, c are not simultaneously squares in $\mathbb{F}_2[x]$. Then*

$$\max(\deg(a), \deg(b), \deg(c)) < \deg(\mathrm{rad}(abc)), \tag{7}$$

where $\mathrm{rad}(abc)$ *is the product of all distinct prime divisors of abc in $\mathbb{F}_2[x]$.*

Lemma 2.5. *Let k, l be non-negative integers not both even and let $t > 1$ be an integer. Then there are no polynomials $L, M \in \mathbb{F}_2[x]$ such that L is odd and*

$$L^2 + x^k(x+1)^l = M^t. \tag{8}$$

Proof. Assume, on the contrary, the existence of two polynomials L and $M \in \mathbb{F}_2[x]$ satisfying (8). Put $A := L^2, B := x^k(x+1)^l, C := M^t$. Since M^t cannot be a square we have $t = 2t_1 + 1$ and only two cases to consider.

Case 1. We have that k, l are not both odd, say $k := 2k_1$, and $l := 2l_1 + 1$, since we can always change x by $x+1$ if necessary in (8).

Since $M \in \mathbb{F}_2[x]$, Lemma 2.2 implies the existence of unique binary polynomials $M_1, M_2 \in \mathbb{F}_2[x]$ such that

$$M = M_1^2 + xM_2^2. \tag{9}$$

Thus we can write (8) in the form

$$T^2 + xV^2 = (M^{t_1}M_1)^2 + x(M^{t_1}M_2)^2, \tag{10}$$

where

$$T := L + x^{k_1}(x+1)^{l_1} \text{ and } V := x^{k_1}(x+1)^{l_1}. \tag{11}$$

It follows from the uniqueness of T and V in (10) (guaranteed by Lemma 2.2 again) and by (11) that

$$x^{k_1}(x+1)^{l_1} = M^{t_1}M_2, \tag{12}$$

which is a contradiction since M is odd, so that it cannot have roots in $\mathbb{F}_2$.

Case 2. We have that k, l are both odd. We obtain the same contradiction as before, since we get the same V on the left hand side of (10). This finishes the proof of the Lemma. □

Remark 2.6. We first found a proof of Lemma 2.5 using the ABC theorem, however our present proof above, based on the classical Lemma 2.2 is much shorter.

Lemma 2.7. *Assume that a non-constant binary polynomial R satisfies the condition:*

$$R^m = P^k + S^n \tag{13}$$

in which P is a prime (irreducible) binary polynomial, S a binary polynomial, not divisible by P and n, k, m are non-negative integers with $m \geq 1$, $k \geq 1$ such that P^k and S^n are not both squares in $\mathbb{F}_2[x]$, and one has either $n = 0$ and $\deg(R) \leq \deg(P)$, or $n \neq 0$ and

$$\frac{1}{m} + \frac{1}{n} \leq \frac{1}{2}, \tag{14}$$

$$\deg(R) \geq \deg(P), \tag{15}$$

and

$$\gcd(m, n\deg(S)) = 1. \tag{16}$$

Then

$$R = P + 1. \tag{17}$$

Proof. Put $A := R^m, B := P^k$ and $C = S^n$. Put also

$$\alpha := \max(\deg(A), \deg(B), \deg(C)), \beta := \deg(\mathrm{rad}(ABC)).$$

Case 1. We have $\deg(A) = \deg(B)$. Assume first that $n = 0$, so that $C = 1$. Clearly, $\gcd(A, B) = 1$. One has $\alpha = \deg(A) = \deg(B) = m\deg(R) = k\deg(P)$, $\beta = \deg(\mathrm{rad}(A)\mathrm{rad}(B)) = \deg(\mathrm{rad}(R)P) = \deg(\mathrm{rad}(R)) + \deg(P) \leq \deg(R) + \deg(P)$ so that $\beta \leq \frac{k}{m}\deg(P) + \deg(P)$. By Lemma 2.4 one has $\beta > \alpha$ thus $k\deg(P) < \frac{k}{m}\deg(P) + \deg(P)$. In other words, one has

$$1 < \frac{1}{m} + \frac{1}{k}. \tag{18}$$

It follows from (18) that $k < 2$ or $m < 2$. If $m > 1$ then (18) implies that $k = 1$, so that (13) becomes

$$P = R^m + 1. \tag{19}$$

But P is prime, so that it is not a square, i.e., $m > 1$ is odd. Thus $R^m+1 = (R+1)T$ for some non-constant binary polynomial T. Thus (19) contradicts the primality of P. Therefore, $m = 1$. Thus the hypothesis $\deg(R) \leq \deg(P)$ and $k \geq 1$ together with

$$\deg(R) = m \deg(R) = k \deg(P), \tag{20}$$

proves that $k = 1$, i.e., we get the conclusion that $R = P + 1$.

Assume now that $n \neq 0$. From $\deg(A) = \deg(B)$ and (13) one gets that $\deg(C) < \deg(A)$ and

$$m \deg(R) = k \deg(P). \tag{21}$$

Thus, $\alpha = \deg(A) = m \deg(R) = k \deg(P)$, while $\beta = \deg(\mathrm{rad}(A)\mathrm{rad}(B)\mathrm{rad}(C)) = \deg(\mathrm{rad}(R) \deg(P)\mathrm{rad}(S)) = \deg(\mathrm{rad}(R)) + \deg(P) + \deg(\mathrm{rad}(S)) \leq \deg(R) + \deg(P) + \deg(S)$. From Lemma 2.4 one gets

$$m \deg(R) < \deg(R) + \frac{m}{k} \deg(R) + \frac{m}{n} \deg(R). \tag{22}$$

In other words,

$$1 < \frac{1}{m} + \frac{1}{k} + \frac{1}{n}. \tag{23}$$

Putting together (23) and the hypothesis (14), we obtain $\frac{1}{2} < \frac{1}{k}$, i.e.,

$$k = 1. \tag{24}$$

If follows from (24) and (21) that

$$m \deg(R) = \deg(P). \tag{25}$$

Finally, (25) together with hypothesis (15) gives

$$m = 1. \tag{26}$$

But (26) contradicts hypothesis (14), so that $n \neq 0$ cannot happen in Case 1.

Case 2. One has $\deg(A) > \deg(B)$. This implies, from (13), that $\deg(A) = \deg(C)$, i.e.,

$$m \deg(R) = n \deg(S). \tag{27}$$

Assume first that $n \neq 0$. Then from (27) and condition (16) we get $m = 1$. But this contradicts condition (14). Therefore, we must have $n = 0$. But this implies $C = 1$, so that we get $m \deg(R) = 0$ from (27). This is a contradiction and thus Case 2 does not happen.

Case 3. One has $\deg(A) < \deg(B)$. This implies, from (13), that $\deg(B) = \deg(C)$, i.e.,

$$k \deg(P) = n \deg(S). \tag{28}$$

Assume first that $n = 0$. Then $C = 1$ so that (28) implies $k \deg(P) = 0$. This is a contradiction. We have therefore $n \neq 0$. One has by (28) $\alpha = \deg(B) = k \deg(P)$, β is computed as before, i.e., $\beta = \deg((\mathrm{rad}(A)\mathrm{rad}(B)\mathrm{rad}(C)) = \deg(\mathrm{rad}(R) \deg(P)\mathrm{rad}(S))$ $= \deg(\mathrm{rad}(R)) + \deg(P) + \deg(\mathrm{rad}(S)) \leq \deg(R) + \deg(P) + \deg(S)$. Since $\beta > \alpha$ by Lemma 2.4, we get from (28)

$$k \deg(P) < \frac{k}{m} \deg(P) + \deg(P) + \frac{k}{n} \deg(P). \tag{29}$$

It follows from (29) that indeed

$$k < \frac{1}{1 - \frac{1}{m} - \frac{1}{n}}. \tag{30}$$

Now hypothesis (14), together with (30), implies that

$$k < 2, \tag{31}$$

so that $k = 1$. We now put together (31), $\deg(A) < \deg(B)$ and hypothesis (15) to obtain

$$m \deg(R) < \deg(P) \leq \deg(R), \tag{32}$$

i.e., $m < 1$. This is a contradiction. Therefore, Case 3 does not happen. This finishes the proof of the Lemma. □

3. Proofs of Theorem 1.1 and Theorem 1.2

Proof of Theorem 1.1:

Proof. Assume, on the contrary, that R is an odd perfect polynomial that satisfies the conditions of the theorem. It follows from Lemma 2.3 that there exists an $L \in \mathbb{F}_2[x]$ such that $R = L^2$. Thus Lemma 2.5 gives a contradiction. The result follows. □

Proof of Theorem 1.2:

Proof. By Lemma 2.7, one has $R = P + 1$. Since R is perfect we cannot have $\deg(P) = 1$, thus $\deg(P) \geq 2$ so that P is odd. It follows that R is even perfect. □

Acknowledgement. We are grateful to the three referees for careful reading and detailed suggestions that resulted in an improved paper. Particular thanks to the referee that pointed out the importance of the uniqueness in Lemma 2.2. Thanks also to Reinhardt Euler for useful comments.

References

[1] 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. Nat., 62(8) (1977), 283-291.

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

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

[4] L. H. Gallardo, *Question: Even perfect numbers n with $n+1$ prime*, https://mathoverflow.net/questions/62797/even-perfect-numbers-n-with-n1-prime.

[5] L. H. Gallardo, Sequence A189373 in The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org, 2017.

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

[7] L. H. Gallardo and O. Rahavandrainy, *Even perfect polynomials over $\mathbb{F}_2$ with four prime factors*, Int. J. Pure Appl. Math., 52(2) (2009), 301-314.

[8] L. H. Gallardo and O. Rahavandrainy, *There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors*, Port. Math., 66(2) (2009), 131-145.

[9] L. H. Gallardo and O. Rahavandrainy, *Characterization of sporadic perfect polynomials over $\mathbb{F}_2$*, Funct. Approx. Comment. Math., 55(1) (2016), 7-21.

[10] L. H. Gallardo, P. Pollack and O. Rahavandrainy, *On a conjecture of Beard, O'Connell and West concerning perfect polynomials*, Finite Fields Appl., 14(1) (2008), 242-249.

[11] S. Lang, Algebra, 2nd ed., Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

Luis H. Gallardo
Univ Brest, UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique
6, Av. Le Gorgeu
C.S. 93837, Cedex 3
F-29238 Brest, France
e-mail: Luis.Gallardo@univ-brest.fr