ISSN 2075-9827 e-ISSN 2313-0210
Carpathian Math. Publ. 2023, **15** (2), 507–513
doi:10.15330/cmp.15.2.507-513

https://journals.pnu.edu.ua/index.php/cmp
Карпатські матем. публ. 2023, Т.15, №2, С.507–513

On the index of special perfect polynomials

Gallardo L.H.

We give a lower bound of the degree and the number of distinct prime divisors of the index of special perfect polynomials. More precisely, we prove that $\omega(d) \geq 9$, and $\deg(d) \geq 258$, where $d := \gcd(Q^2, \sigma(Q^2))$ is the index of the special perfect polynomial $A := p_1^2 Q^2$, in which p_1 is irreducible and has minimal degree. This means that $\sigma(A) = A$ in the polynomial ring $\mathbb{F}_2[x]$. The function σ is a natural analogue of the usual sums of divisors function over the integers. The index considered is an analogue of the index of an odd perfect number, for which a lower bound of 135 is known. Our work use elementary properties of the polynomials as well as results of the paper [J. Théor. Nombres Bordeaux 2007, **19** (1), 165–174].

Key words and phrases: cyclotomic polynomial, characteristic 2, special perfect polynomial, factorization.

Laboratoire de Mathématiques de Bretagne Atlantique, University of Western Brittany, 6 Av. Le Gorgeu, F-29238 Brest, France
E-mail: `luis.gallardo@univ-brest.fr`

Introduction

A perfect number is a positive integer n that the sum of all its divisors, say $\sigma(n)$, equals $2n$. More generally, a multiperfect number is a positive integer m such that the quotient of $\sigma(m)$ by m is still a positive integer. Namely

$$\frac{\sigma(m)}{m} \in \mathbb{Z}. \tag{1}$$

It is known that all perfect numbers n, even or odd, have the following form

$$n = P^k Q^2, \tag{2}$$

where P is a prime number, and k, Q are positive integers such that $P \nmid Q$. More precisely, if n is even, $k = 1$, $P = 2^p - 1$, with p an odd prime number, and $Q = 2^{\frac{p-1}{2}}$, while if n is odd, $k \equiv 1 \pmod 4$ and also $P \equiv 1 \pmod 4$. Besides $n = 1$ no other odd multiperfect number is known.

Let n be a perfect number. Using (2), by the multiplicative property of σ, one has

$$2P^k Q^2 = \sigma\left(P^k\right)\sigma\left(Q^2\right).$$

One sees that this equality can be also written as

$$\frac{\sigma\left(Q^2\right)}{Q^2} = \frac{P^k}{\sigma\left(P^k\right)/2}, \tag{3}$$

УДК 511.6
2020 *Mathematics Subject Classification:* 11T55, 11T06, 11A07, 11A25.

and that the right hand side fraction in (3) is in lowest terms, i.e. gcd $\left(P^k, \sigma(P^k)/2\right) = 1$.

It is then natural to define the index d of n as

$$d := \gcd\left(Q^2, \sigma(Q^2)\right), \tag{4}$$

so that from (3) one has

$$\sigma(Q^2) = d \cdot P^k \quad \text{and} \quad Q^2 = d \cdot \sigma(P^k)/2.$$

In 1937, R. Steuerwald [9] proved that there is no odd perfect numbers n of the form $n := P^k p_1^2 \cdots p_m^2$, where $P \equiv 1 \pmod 4$ and the p_j are distinct odd prime numbers, and $k = 1 \pmod 4$. In other words, when Q is square-free.

In this paper, we deal with an analogue of the index d in (4) for special perfect polynomials in $\mathbb{F}_2[x]$, that has exactly the same form. More precisely, A in $\mathbb{F}_2[x]$ is special perfect if it is a product of squares of irreducible (*prime*) polynomials, such that

$$\frac{\sigma(A)}{A} \in \mathbb{F}_2[x] \tag{5}$$

the natural analogue of (1) in $\mathbb{Z}$.

Since $\deg(A) = \deg\left(\sigma(A)\right)$ in $\mathbb{F}_2[x]$, (5) just says that A satisfies

$$\sigma(A) = A.$$

Thus, a special perfect polynomial in $\mathbb{F}_2[x]$ is just a product of squares of prime polynomials that is *fixed* by the function $\sigma : \mathbb{F}_2[x] \mapsto \mathbb{F}_2[x]$, the *mutatis mutandi* analogue, of the usual sums of divisors function σ.

The index d of a special perfect polynomial $A \in \mathbb{F}_2[x]$, written as

$$A = p_1^2 \cdot Q^2, \tag{6}$$

where p_1 is a prime divisor of *minimal* degree of A, is defined by

$$d := \gcd\left(Q^2, \sigma(Q^2)\right). \tag{7}$$

We have no analogue on $\mathbb{F}_2[x]$ of the result of R. Steuerwald (see, however, [3]). This shows that the particular problem of characterizing the special perfect polynomials appears (contrary to R. Steuerwald's result over the integers) difficult to resolve.

More details about the index follow.

First of all, we describe the binary perfect polynomials in $\mathbb{F}_2[x]$. This ring is the polynomial ring *close* to the ring of integers $\mathbb{Z}$. In other words, we can do arithmetic in it, and generally, the translated arithmetic problems in $\mathbb{F}_2[x]$, that come from $\mathbb{Z}$, are easier to work, since there are more tools available for polynomials than for integers. For example, the formal derivation $(P \mapsto P')$, whose kernel in $\mathbb{F}_2[x]$ are the squares, is a really useful tool, not available in $\mathbb{Z}$.

In order to better understand the notion of index translated to $\mathbb{F}_2[x]$ (see (7)) we introduce some definitions and a notation.

A binary polynomial B is *odd* if $B(0) = B(1) = 1$, otherwise B is *even*. A *minimal* prime of an odd polynomial A is a prime divisor P of A that has minimal degree. Analogously, a *maximal* prime of an odd polynomial A is a prime divisor P of A that has maximal degree. A prime divisor of A that is neither minimal, nor maximal is a *medium* prime [3]. We let $\omega(A)$ denote the number of distinct prime factors of A over $\mathbb{F}_2$.

Consider the function $\sigma\colon \mathbb{F}_2[x] \mapsto \mathbb{F}_2[x]$ defined over a polynomial $A \in \mathbb{F}_2[x]$ by $\sigma(A) = \sum_{D|A} D \in \mathbb{F}_2[x]$, i.e. by the sum of all divisors of A, including 1 and A. The function σ is *multiplicative*, i.e. for coprime binary polynomials X, Y one has, as over the integers $\mathbb{Z}$, $\sigma(XY) = \sigma(X)\sigma(Y)$. This function σ is more natural, but also more complex, than the usual sum of divisor function $\sigma_1(A) = \sum_{D|A} 2^{\deg(A)}$. We consider this function σ as the natural analogue on $\mathbb{F}_2[x]$ of the usual sum of divisors function over the integers $\mathbb{Z}$. For instance, some divisors D of A can sum up to 0, while a sum over D of $2^{\deg D}$ is always greater than 0. We recall that a *binary perfect* polynomial A is defined by the equality $\sigma(A) = A$, i.e. $\sigma(A)/A$ belongs to the ring $\mathbb{F}_2[x]$. We can also say that A is a *fixed* point of the function σ (see [1–7]). By our analogy between $\mathbb{F}_2[x]$ and $\mathbb{Z}$, this corresponds to a multiperfect number n in the ring of integers, i.e. a positive integer n with the property that $\sigma(n)/n$ belong to the ring $\mathbb{Z}$ (a slightly more general property than the study of the perfect numbers, i.e. the usual case when $\sigma(n)/n = 2$). E.F. Canaday, the first PhD student of Leonard Carlitz, started the work [1] on binary perfect polynomials in 1941. His paper resumes most of his PhD dissertation.

We know that a perfect polynomial A must have an even number of minimal primes (see [3, Lemma 2.3]). No analogue result is known for the parity of the number of medium or maximal primes dividing a perfect polynomial. No odd perfect polynomial A is known besides the trivial perfect $A = 1$. The only general result known about odd perfect polynomials A is that A must be a square [1] (this explains why the divisor P^k of n in (2) has no analogue in (6)). More generally, R. Lidl and H. Niederreiter [8], and R.G. Swan [10], give the most classic results about polynomials over finite fields. We recall that the third cyclotomic polynomial is defined by

$$\Phi_3(x) = x^2 + x + 1.$$

Our main result is as follows.

Theorem 1. *Let $A = p_1^2 \cdots p_m^2 \in \mathbb{F}_2[x]$ be a special perfect polynomial, i.e. $\sigma(A) = A$, with $\omega(A) = m$, $d_k := \deg(p_k)$ for all $k = 1, \ldots, m$ and $d_1 \leq \cdots \leq d_m$. In particular, p_1 is minimal, and p_m is maximal. Put $Q := p_2^2 \cdots p_m^2$, and let $d := \gcd\left(Q^2, \sigma(Q^2)\right)$ be the index of A. Let m_1, m_2 and m_3 be the number of minimal, medium and maximal prime divisors of A, respectively.*

Then the following hold.

(a) *We have that d is not a square in $\mathbb{F}_2[x]$.*

(b) *We have that d is not square-free.*

(c) *There exist two divisors a, b of A such that $\gcd(a, b) = 1$, $Q = ab$, and $d = a^2 b$. Moreover, $a = \gcd\left(\sigma(Q^2)/Q, Q\right)$, $a \neq 1$ and $b \neq 1$.*

(d) *We have $\omega(d) \geq 9$ and $\deg(d) \geq 258$.*

1 Tools

The following lemma is useful.

Lemma 1 ([3, Lemma 2.3])**.** *Let q be a power of 2. Let $A \in \mathbb{F}_q[x]$ be a perfect polynomial. Let $p_1, \ldots, p_r$ be the list of all monic minimal primes of A. Then the integer r is even.*

Parts (a) and (b) of the following lemma follow from [3, Lemma 4.2], while part (c) is [3, Corollary 4.4].

Lemma 2. *Let $P \in \mathbb{F}_2[x]$ be a maximal prime of a special perfect polynomial $A = p_1^2 \cdots p_m^2 \in \mathbb{F}_2[x]$, with $\omega(A) = m$, $d_k := \deg(p_k)$, for all $k = 1, \ldots, m$, and $d_1 \leq \cdots \leq d_m$. In particular, p_1 is minimal, and p_m is maximal. Then there exists a unique pair (i,j), $i,j \in \{1, \ldots, m\}$, such that the following hold.*

(a) *We have $p_j \neq P$, $d_1 < d_i < d_j = \deg(p_j) = \deg(P) = d_m$. In other words, p_j is maximal while p_i is medium.*

(b) *We have $P \mid p_i^2 + p_i + 1$ and $P \mid p_j^2 + p_j + 1$, so that $P = p_i + p_j + 1$. In particular, P cannot divide $\Phi_3(Q_1)$ and $\Phi_3(Q_2)$ for any two distinct maximal divisors Q_1, Q_2 of A.*

(c) *Let m_2 be the number of medium primes that divide A, and m_3 the number of maximal primes that divide A. Then*
$$m_2 \geq m_3 \geq 3.$$

The following lemma is useful for the proof of part (d) of the Theorem 1. It also appears, without proof, in [1, Theorem 21].

Lemma 3 ([3, Lemma 5.3 (b)])**.** *Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Let $P \in \mathbb{F}_2[x]$ be a prime divisor of A. Then $\deg(P)$ is even.*

The most important numerical result [3, Theorem 5.5], known about these special perfect polynomials, follows.

Lemma 4. (a) *Any special perfect polynomial A have $\omega(A) \geq 10$.*

(b) *For any prime divisor P of A we have $\deg(P) \geq 30$.*

2 Proof of Theorem 1

Observe that $A = p_1^2 Q^2$. Since $A = \sigma(A)$ and σ is multiplicative, one has

$$p_1^2 Q^2 = \sigma(A) = (p_1^2 + p_1 + 1)\sigma(Q^2) = \Phi_3(p_1)\sigma(Q^2).$$

Thus

$$\frac{\sigma\left(Q^2\right)}{Q^2} = \frac{p_1^2}{\Phi_3(p_1)}.$$

Clearly, $\gcd(p_1^2, \Phi_3(p_1)) = 1$, i.e. the fraction in the right hand side of the above equality is in lower terms.

By definition of the index d, we have

$$\sigma(Q^2) = dp_1^2,$$

and

$$Q^2 = d\Phi_3(p_1). \tag{8}$$

Let us differentiate both sides of (8) relative to x, we obtain

$$0 = d'\Phi_3(p_1) + d\Phi_3'(p_1) = d'\Phi_3(p_1) + dp_1',$$

since both Q^2 and $p_1^2 + 1 = (p_1 + 1)^2$ are squares in $\mathbb{F}_2[x]$.

In other words we have

$$d'\Phi_3(p_1) = dp_1'. \tag{9}$$

In order to prove (a), it follows from (9), and from $d' = 0$ that

$$0 = dp_1',$$

i.e. one has $p_1' = 0$. Thus, the prime p_1 is also a square, what is impossible. This proves part (a).

In order to prove (b), assume, to the contrary, that d is square-free. In other words, we have

$$\gcd\left(d, d'\right) = 1.$$

From (9) we obtain that

$$d \mid \Phi_3(p_1). \tag{10}$$

In particular $\deg(d) \leq 2d_1$. This implies that $\omega(d) \leq 2$, since any possible prime divisor of d has degree $\geq d_1$.

Therefore, either $d = p_k$ for some k or $d = p_i p_j$ for some $i \neq j$.

If $d = p_k$, put $\Phi_3(p_1) = dR$. Putting this into equation (8), we get that R is a square, say, $R = S^2$. We have then

$$\Phi_3(p_1) = p_k S^2. \tag{11}$$

Taking degrees in (11), we obtain

$$2d_1 = d_k + 2\deg(S). \tag{12}$$

We have $d_k \geq d_1$. It follows then from (12) that $\deg(S) \leq d_1/2$. This is impossible since the degree of any divisor of A is $\geq d_1$. Thus d is not prime.

We consider now the other possible case, i.e. we take $d = p_i p_j$ for some $i \neq j$. Since both d_i and d_j are at least equal to d_1, we conclude that p_j and p_i are minimal primes. In particular,

$$\deg(d) = 2d_1 = \deg\left(\Phi_3(p_1)\right).$$

But, as observed in (10), d divides $\Phi_3(p_1)$. It follows that $d = \Phi_3(p_1)$. Thus, (8) implies that

$$d = Q. \tag{13}$$

But $\omega(Q) = \omega\left(Q^2\right) = \omega(A) - 1$, since $A = p_1^2 Q^2$. It is known [3], that $\omega(A) \geq 10$ (see also Lemma 4). Therefore, it follows from (13) that

$$\omega(d) \geq 9.$$

But this is impossible since $d = p_i p_j$. This proves part (b).

In order to prove (c), write $d = a^2 b$ with b square-free, or $b = 1$. Since d is not a square, we have $b \neq 1$. Since d is not square-free, we have that $a \neq 1$. Since d divides A, the exponents of the primes dividing d are in $\{1, 2\}$, thus $\gcd(a, b) = 1$. Indeed if $\gcd(a, b) \neq 1$ then we must have $p_j^3 || A$ for some j, and this is impossible.

Observe that $K := \Phi_3(p_1)$ has degree $2d_1$, so that either K is a prime or K is a product of two (minimal) primes. Write (8) as follows

$$\left(\frac{Q}{a}\right)^2 = bK. \tag{14}$$

Since b and K are square-free, it follows from (14) that $K = b$. Thus, we obtain $Q = ab$ from (14) again. From $d = a^2 b$ and $Q = ab$ we have then

$$d = aQ. \tag{15}$$

But, by definition of d, and since Q divides d, we have

$$a^2 b = d = \gcd\left(Q^2, \sigma(Q^2)\right) = Q \gcd\left(Q, \sigma(Q^2)/Q\right) = ab \gcd\left(Q, \sigma(Q^2)/Q\right).$$

In other words, this means that $a = \gcd\left(Q, \sigma\left(Q^2\right)/Q\right)$. This finishes the proof of (c).

In order to prove (d), observe first that $m_1 \geq 2$, since by Lemma 1, m_1 is even.

By Lemma 2 (c) we have that $m_2 \geq m_3 \geq 3$. By Lemma 4 (b) we have $d_1 \geq 30$. Since by Lemma 3, all d_j are even, by definition of medium prime, we have $d_i \geq 32$ for any medium prime p_i, and $d_j \geq 34$ for any maximal prime p_j. This implies that

$$\deg(A) \geq 2(m_1 d_1 + m_2 d_2 + m_3 d_3) \geq 2(2d_1 + 3d_2 + 3d_3),$$

Thus

$$\deg(A) \geq 2(60 + 96 + 102) = 516.$$

Now, from $A = p_1^2 Q^2$ we have $\deg(Q) = \deg(A)/2 - \deg(p_1) \geq 258 - d_1$. But by (15) $d = aQ$ and a, as a divisor of A, has degree $\deg(a) \geq d_1$. Therefore

$$\deg(d) = \deg(a) + \deg(Q) \geq d_1 + (258 - d_1) = 258.$$

Still from $A = p_1^2 Q^2$ we have $\omega(Q) = \omega(A) - 1$. From (15) $d = aQ$, so that $\omega(d) \geq \omega(Q)$. But $\omega(A) \geq 10$ by Lemma 4 (a). Thus

$$\omega(d) \geq \omega(Q) \geq \omega(A) - 1 \geq 10 - 1 = 9.$$

This finishes the proof of the theorem.

References

[1] Canaday E.F. *The sum of the divisors of a polynomial*. Duke Math. J. 1941, **8** (4), 721–737. doi:10.1215/S0012-7094-41-00861-X

[2] Cengiz U.C., Pollack P., Treviño E. *Counting perfect polynomials*. Finite Fields Appl. 2017, **47**, 242–255. doi:10.1016/j.ffa.2017.05.006

[3] Gallardo L.H., Rahavandrainy O. *Odd perfect polynomials over* $\mathbb{F}_2$. J. Théor. Nombres Bordeaux 2007, **19** (1), 165–174. doi:10.5802/jtnb.579

[4] Gallardo L.H., Rahavandrainy O. *There is no odd perfect polynomial over* $\mathbb{F}_2$ *with four prime factors*. Port. Math. 2009, **66** (2), 131–145. doi:10.4171/pm/1836

[5] Gallardo L.H., Rahavandrainy O. *On even (unitary) perfect polynomials over* $\mathbb{F}_2$. Finite Fields Appl. 2012, **18** (5), 920–932. doi:10.1016/j.ffa.2012.06.004

[6] Gallardo L.H., Rahavandrainy O. *Characterization of sporadic perfect polynomials over* $\mathbb{F}_2$. Funct. Approx. Comment. Math. 2016, **55** (1), 7–21. doi:10.7169/facm/2016.55.1.1

[7] Gallardo L.H., Rahavandrainy O. *On Mersenne polynomials over* $\mathbb{F}_2$. Finite Fields Appl. 2019, **59**, 284–296. doi:10.1016/j.ffa.2019.06.006

[8] Lidl R., Niederreiter H. Finite Fields. In: Doran R., Ismail M., Lam T.-Y., Lutwak E. (Eds.) Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1996.

[9] Steuerwald R. *Verschärfung einer notwedingen Bedingung für die Existenz einer ungeraden volkommenen Zahl*. Sitzungsber. Bayer. Akad. Wiss., Math.-Naturwiss. Abt. 1937, **2**, 69–72.

[10] Swan R.G. *Factorization of polynomials over finite fields*. Pacific J. Math. 1962, **12** (3), 1099–1106.

Received 05.11.2021

Ґаллардо Л.Х. *Про індекс спеціальних досконалих поліномів* // Карпатські матем. публ. — 2023. — Т.15, №2. — С. 507–513.

У статті ми подаємо нижню оцінку степеня та кількості різних простих дільників індексу спеціальних досконалих поліномів. Точніше, ми доводимо, що $\omega(d) \geq 9$ та $\deg(d) \geq 258$, де $d := \gcd(Q^2, \sigma(Q^2))$ є індексом спеціального досконалого полінома $A := p_1^2 Q^2$, в якому p_1 є незвідним та має мінімальний степінь. Це означає, що $\sigma(A) = A$ у поліноміальному кільці $\mathbb{F}_2[x]$. Функція σ є природним аналогом функції, що обчислює суму дільників над полем цілих чисел. Розглянутий індекс є аналогом індекса непарного досконалого числа, для якого нижня межа 135 є відомою. У нашій роботі використано елементарні властивості поліномів, а також результати статті [J. Théor. Nombres Bordeaux 2007, **19** (1), 165–174].

Ключові слова і фрази: многочлен поділу кола, характеристика 2, спеціальний досконалий многочлен, факторизація.