INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Olivier Rahavandrainy

Familles de polynômes unitairement parfaits sur $\mathbb{F}_2$

Volume 359, issue 2 (2021), p. 123-130.

<https://doi.org/10.5802/crmath.149>

Les Comptes Rendus. Mathématique *sont membres du Centre Mersenne pour l'édition scientifique ouverte*
www.centre-mersenne.org

Comptes Rendus
Mathématique
2021, 359, nº 2, p. 123-130
https://doi.org/10.5802/crmath.149

Algèbre / *Algebra*

Familles de polynômes unitairement parfaits sur $\mathbb{F}_2$

Some families of unitary perfect polynomials over $\mathbb{F}_2$

Olivier Rahavandrainy[a]

[a] Univ Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique
Courriel : olivier.rahavandrainy@univ-brest.fr

Résumé. Nous caractérisons les polynômes binaires unitairement parfaits, connus jusqu'ici, apparemment de façon « empirique ». La méthode que nous avons trouvée a permis et permettrait d'en découvrir d'autres.

Abstract. We characterize all the known unitary perfect binary polynomials by precising their admissible families. Our method allows us to find other ones.

Manuscrit reçu le 10 août 2020, révisé le 9 novembre 2020, accepté le 12 novembre 2020.

1. Introduction

On travaille sur le corps premier à deux éléments $\mathbb{F}_2$. Avant tout, nous voudrions donner les quelques définitions suivantes, inspirées de certaines notions sur les entiers naturels (voir [7, 8] et [9] pour plus d'explications).

On dit qu'un polynôme non nul sur $\mathbb{F}_2$ (appelé aussi polynôme *binaire*) est *pair* s'il a un facteur linéaire et *impair* si non. Un polynôme de Mersenne (irréductible) est un polynôme (irréductible) de la forme $1 + x^a(x+1)^b$, où a et b sont deux entiers naturels non nuls. Un diviseur d d'un polynôme A sur $\mathbb{F}_2$ est *unitaire* si $\mathrm{pgcd}(d, \frac{A}{d}) = 1$. On note $\omega(A)$ (resp. $\sigma(A)$, $\sigma^*(A)$) le nombre de diviseurs irréductibles distincts (resp. la somme de tous les diviseurs (unitaires)) de A. Les fonctions σ et σ^* sont multiplicatives (voir la Définition 2). On dit que A est (*unitairement*) *parfait* si $\sigma(A) = A$ (resp. $\sigma^*(A) = A$). Un polynôme (unitairement) parfait est *indécomposable* s'il ne peut pas se factoriser en deux polynômes non constants, premiers entre eux et (unitairement) parfaits.

Cette notion de « perfection » est introduite par E. F. Canaday [3] en 1941. J. T. B. Beard Jr. *et al.* l'ont étendue dans diverses directions [1, 2]. Nous nous y sommes intéressés depuis quelque temps, avec plus ou moins de succès (voir [4–6] et des références qui y sont mentionnées).

Dans toute la suite, $\mathbb{N}$ (resp. $\mathbb{N}^*$) désigne l'ensemble des entiers naturels (resp. des entiers naturels non nuls). On note, pour $S \in \mathbb{F}_2[x]$:

- $val_x(S)$ (resp. $val_{x+1}(S)$) la valuation de S, en x (resp. en $x+1$),

- $\overline{S}$: le polynôme obtenu de S, en remplaçant x par $x+1$,
- $S^{abc} := 1 + x^a(x+1)^b S^c$, pour S impair (on a : $\overline{S^{abc}} = \overline{S}^{bac}$),
- $S^*(x) := x^{\deg(S)} \cdot S(\frac{1}{x})$, le polynôme réciproque de S, si $S(0) = 1$.

On considère :

$$
\begin{aligned}
&M_1 := 1 + x + x^2,\ M_2 := 1 + x + x^3,\ M_3 := \overline{M_2} = 1 + x^2 + x^3,\\
&M_4 := 1 + x + x^2 + x^3 + x^4, M_5 := \overline{M_4} = 1 + x^3 + x^4,\\
&M_6 := 1 + x^3 + x^5,\ M_7 := 1 + x^3 + x^7,\ M_8 := 1 + x^6 + x^7,\\
&M_9 := \overline{M_6},\ M_{10} := \overline{M_7},\ M_{11} := \overline{M_8},\\
&M_{12} := x^9 + x + 1, M_{13} := \overline{M_{12}} = x^9 + x^8 + 1,\\
&T_1 := x^2(x+1)M_1, T_2 := \overline{T_1},\\
&T_3 := x^4(x+1)^3 M_4, T_4 := \overline{T_3},\ T_5 := x^4(x+1)^4 M_4 \overline{M_4} = \overline{T_5},\\
&T_6 := x^6(x+1)^3 M_2 \overline{M_2}, T_7 := \overline{T_6},\\
&T_8 := x^4(x+1)^6 M_2 \overline{M_2} M_4 \text{ et } T_9 := \overline{T_8},\\
&T_{10} := x^2(x+1)\left(x^4 + x + 1\right) {M_1}^2,\ T_{11} := \overline{T_{10}},\\
&S_1 := {M_1}^{111} = \overline{S_1},\ S_2 := {M_1}^{221},\ S_3 := {M_1}^{134},\ S_4 := {M_1}^{311},\ S_5 := {M_1}^{131},\\
&S_6 := {M_1}^{314},\ S_7 := {M_1}^{113},\ S_8 := {M_1}^{331},\ S_9 := {M_1}^{115},\ S_{10} := {M_1}^{411},\\
&S_{11} := {M_1}^{121},\ S_{12} := {M_1}^{212},\ S_{13} := {M_1}^{141},\ S_{14} := {M_1}^{211},\ S_{15} := {M_1}^{122},\\
&\mathscr{F}_1 := \{M_1, \ldots, M_{13}\},\ \mathscr{F}_2 := \{S_1, \ldots, S_{15}\},\ \mathscr{F} := \mathscr{F}_1 \cup \mathscr{F}_2.
\end{aligned}
$$

Voici les résultats connus pour les polynômes parfaits pairs sur $\mathbb{F}_2$. D'abord, il y a les « triviaux », de la forme $(x^2+x)^{2^n-1}$, où n est un entier naturel. Il y a aussi neuf autres, $T_1, \ldots, T_9$, qui sont les seuls pairs de la forme $x^a(x+1)^b \prod_j {P_j}^{2^{n_j}-1}$, où les P_j sont des polynômes de Mersenne [7, Théorème 1.1]. Et enfin, les deux derniers, T_{10}, T_{11}, qui sont les seuls de la forme $x^a(x+1)^b M^{2h}\sigma(M^{2h})$, où M est un polynôme de Mersenne [8, Théorème 1.4]. De plus, T_{10} et T_{11} sont divisibles par le polynôme x^4+x+1 (qui n'est pas de Mersenne). Les polynômes parfaits impairs, s'ils existent, sont des carrés.

Les polynômes unitairement parfaits connus sont décrits, de façon « empirique » (en apparence), dans [2, pages 13-14]. Ils appartiennent à une vingtaine de « classes d'équivalence » (*cf.* Remarque 6) dont les représentants seront notés : $E_1, \ldots, E_{21}$. Nous en avons caractérisé quelques uns [7, Théorème 1.3]. Nous voudrions poursuivre cette démarche, pour tous ces polynômes. Pour cela, nous élaborons une méthode que nous avons commencé à utiliser dans [10]. Nous y avons introduit la notion de *famille admissible*. Nous avons ainsi construit la famille $\mathscr{F}$ ci-dessus. Les diviseurs irréductibles et impairs de ces polynômes sont des polynômes de Mersenne (les M_i) ou les S_j cités ci-dessus (des polynômes de la forme $1 + x^a(x+1)^b M^c$, où M est un polynôme de Mersenne), sauf pour deux d'entre eux : E_{18} et E_{21} (de degrés 58 et 86). En effet, $V_1 = {M_4}^{112}$ et $V_2 = \overline{V_1} = {M_5}^{112}$ divisent E_{18}, $V_3 = {M_2}^{321}$, $V_4 = \overline{V_3}$, $V_5 = 1 + x(x+1)^2 S_{11}$ et $V_6 = \overline{V_5}$ divisent E_{21}, $V_1, \ldots, V_6 \notin \mathscr{F}$.

En plus de ces polynômes connus, nous avons découvert 28 autres nouvelles classes (voir la Section 3.1), dont les représentants sont notés B_j, $1 \le j \le 28$, $25 \le \deg(B_j) \le 95$. Nous pouvons dire que la méthode choisie permettrait de construire, à partir d'une famille admissible fixée, des polynômes unitairement parfaits. Inspiré de ces idées, nous pouvons énoncer la Conjecture 16.

Nous obtenons, par le Théorème 1, la caractérisation voulue, avec la famille $\mathscr{F}$. L'analogue de cette méthode pour les polynômes parfaits, n'a pas permis d'en découvrir de nouveaux [10]. On pose : $\mathscr{U}_1 := \{E_1, \ldots, E_{17}, E_{19}, E_{20}\}$ et $\mathscr{U}_2 := \{B_1, \ldots, B_{28}\}$.

Théorème 1. *Soit*

$$A = x^a(x+1)^b \prod_{i=1}^{13} {M_i}^{c_i} \cdot \prod_{j=1}^{15} {S_j}^{d_j} = x^a(x+1)^b\, A_1, \quad où \quad a,b,c_i,d_j \in \mathbb{N},\ a,b \geq 1 \quad et \quad A_1 \neq 1.$$

Alors, A est (indecomposable et) unitairement parfait sur $\mathbb{F}_2$ *si et seulement si*

$$A \in \left\{ B^{2^n}, \overline{B}^{2^n} : n \in \mathbb{N} \right\},\ où\ B \in \mathscr{U}_1 \cup \mathscr{U}_2.$$

2. Preuve du Théorème 1

Il reste la « nécessité », car la suffisance est obtenue par des vérifications directes (utilisant `Maple`). On pose, pour u, v, u_i, v_j impairs et $n, m, n_i, m_j \in \mathbb{N}$:

$$a = 2^n u,\ b = 2^m v, \quad c_i = 2^{n_i} u_i, \quad d_j = 2^{m_j} v_j. \tag{1}$$

On se ramène au cas : $a = val_x(A) \leq val_{x+1}(A) = b$, quitte à remplacer A par $\overline{A}$ (Lemme 5).

On note $I := \{i : i \leq 13,\ c_i \neq 0\}$ et $J := \{j : j \leq 15,\ d_j \neq 0\}$.

2.1. *Préliminaires*

Les définitions et résultats suivants sont connus, cités ou prouvés dans [10].

Définition 2. *Une application non nulle* f, *de* $\mathbb{F}_2[x] \setminus \{0\}$ *vers* $\mathbb{F}_2[x]$, *est* multiplicative *si* $f(A_1A_2) = f(A_1)f(A_2)$, *pour tous* $A_1, A_2 \in \mathbb{F}_2[x] \setminus \{0\}$, *premiers entre eux.*

Lemme 3. *Il n'existe pas de polynôme impair, unitairement parfait et non constant sur* $\mathbb{F}_2$.

Lemme 4. *Si u est impair, alors* $\sigma^*(P^u) = (1+P) \cdot \sigma(P^{u-1})$.

Lemme 5.

(i) *A est unitairement parfait si et seulement si* $\overline{A}$ *l'est.*
(ii) *A est unitairement parfait si et seulement si pour tout* $r \in \mathbb{N}$, A^{2^r} *l'est.*

Remarque 6. Le Lemme 5 permet de classifier des familles de polynômes unitairement parfaits, en précisant un représentant B de chaque « classe d'équivalence » : le seul tel que $B' \neq 0$ et $val_x(B) \leq val_{x+1}(B)$.

Définition 7. *Une famille* $\mathscr{G}$ *de polynômes impairs et irréductibles est admissible si elle satisfait au moins à l'une des trois conditions suivantes :*

(i) *pour tout* $T \in \mathscr{G}$, $T^* \in \mathscr{G}$ *ou* $\overline{T} \in \mathscr{G}$,
(ii) *il existe* $h \in \mathbb{N}^*$ *tel que* $\sigma(x^{2h})$ *ou* $\sigma((x+1)^{2h})$ *se factorise dans* $\mathscr{G}$,
(iii) *pour tout* $T \in \mathscr{G}$, $1+T$ *ou* $\sigma(T^{2h})$ *se factorise dans* $\mathscr{G} \cup \{x, x+1\}$, *pour un* $h \in \mathbb{N}^*$.

Corollaire 8. *Si A est unitairement parfait et non scindé, alors ses diviseurs premiers et impairs forment une famille admissible.*

Lemme 9. *La famille* $\mathscr{F} = \mathscr{F}_1 \cup \mathscr{F}_2$ *est admissible.*

2.2. *Comparaison entre $\sigma^*(A)$ et A*

Nous allons préciser les exposants des diviseurs de $\sigma^*(A)$, afin de comparer ce dernier avec A. Nous conservons les notations de (1). Nous pouvons écrire (par la multiplicativité de σ^*) :

$$\begin{aligned}
\sigma^*(A) &= \sigma^*\left(x^a\right)\sigma^*\left((x+1)^b\right)\prod_{i=1}^{13}\sigma^*\left({M_i}^{c_i}\right)\prod_{j=1}^{15}\sigma^*\left({S_j}^{d_j}\right),\\
\sigma^*\left(x^a\right) &= (x+1)^{2^n}\cdot\left[\sigma\left(x^{u-1}\right)\right]^{2^n}, \sigma^*\left((x+1)^b\right) = x^{2^m}\cdot\left[\sigma\left((x+1)^{u-1}\right)\right]^{2^m},\\
\sigma^*\left({M_i}^{c_i}\right) &= (1+M_i)^{2^{n_i}}\left[\sigma\left({M_i}^{u_i-1}\right)\right]^{2^{n_i}}, \sigma^*\left({S_j}^{d_j}\right) = (1+S_j)^{2^{m_j}}\left[\sigma\left({S_j}^{v_j-1}\right)\right]^{2^{m_j}}.
\end{aligned} \tag{2}$$

Nous voudrions connaître tous les $S \in \{x, x+1\}\cup\mathscr{F}$ et les $h\in\mathbb{N}^*$ tels que $\sigma(S^{2h})$ se factorisent dans $\mathscr{F}$. La réponse est donnée par les trois prochains Lemmes 10, 11, 12 et le Corollaire 13, qui sont déjà prouvés dans [10]. On pose :

$$\sigma^*(A) = x^\alpha(x+1)^\beta\prod_{i=1}^{13}{M_i}^{\gamma_i}\prod_{j=1}^{15}{S_j}^{\delta_j},\ \text{où}\ \alpha,\beta,\gamma_i,\ \delta_j\in\mathbb{N}. \tag{3}$$

Lemme 10. *Si $\sigma(x^{2h})$ et $\sigma((x+1)^{2h})$ se factorisent dans $\mathscr{F}$, alors $h\in\{1,2,3,4,5,6,7\}$. Dans ce cas,*

$$\begin{aligned}
&\sigma\left(x^2\right) = \sigma\left((x+1)^2\right) = M_1, \sigma\left(x^4\right) = M_4, \sigma\left((x+1)^4\right) = M_5,\\
&\sigma\left(x^6\right) = \sigma\left((x+1)^6\right) = M_2M_3, \sigma\left(x^8\right) = M_1S_4, \sigma\left((x+1)^8\right) = M_1S_5,\\
&\sigma\left(x^{10}\right) = V_3, \sigma\left((x+1)^{10}\right) = V_4,\\
&\sigma\left(x^{12}\right) = S_3, \sigma\left((x+1)^{12}\right) = S_6, \sigma\left(x^{14}\right) = \sigma\left((x+1)^{14}\right) = M_1M_4M_5S_1.
\end{aligned}$$

Lemme 11. *Si $M\in\mathscr{F}_1$ et $h\in\mathbb{N}^*$ tels que $\sigma(M^{2h})$ se factorise dans $\mathscr{F}$, alors ($M=M_1$ et $h\in\{1,2,3,7\}$) ou ($M\in\{M_2,M_3\}$ et $h=1$). On obtient : $\sigma({M_2}^2) = M_1M_5$, $\sigma({M_3}^2) = M_1M_4$ et $\sigma({M_1}^2) = S_1$, $\sigma({M_1}^4) = S_8$, $\sigma({M_1}^6) = M_2M_3S_2$, $\sigma({M_1}^{14}) = M_4M_5S_1S_7S_8$.*

Lemme 12. *Si $S\in\mathscr{F}_2$ et $h\in\mathbb{N}^*$ tels que $\sigma(S^{2h})$ se factorise dans $\mathscr{F}$, alors $h=1$ et $S\in\{S_1,S_2\}$. On a : $\sigma({S_1}^2) = M_4M_5$ et $\sigma({S_2}^2) = S_1S_7$.*

Corollaire 13.

(1) *Si M_i et S_j divisent $\sigma^*(A)$, alors $i\le 5$ et $j\le 8$.*
(2) *Pour tout $j\in\{2,\dots,6\}$, ${S_j}^2$ ne divise pas $\sigma^*(A)$.*

Pour $w\in\mathbb{N}^*$, on considère la fonction indicatrice χ_w du singleton $\{w\}$:

$$\chi_w(w) = 1,\ \chi_w(t) = 0\ \text{si}\ t\neq w.$$

En conservant les notations de (1) et (3), on pose :

$$\begin{aligned}
&M_i = 1+x^{a_i}(x+1)^{b_i}\in\mathscr{F}_1, && S_j = 1+x^{\alpha_j}(x+1)^{\beta_j}{M_1}^{\lambda_j}\in\mathscr{F}_2,\\
&\xi_1 = \chi_3(u)+\chi_9(u)+\chi_{15}(u), && \xi_2 = \chi_3(v)+\chi_9(v)+\chi_{15}(v),\\
&\xi_3 = \chi_5(u)+\chi_{15}(u), && \xi_4 = \chi_5(v)+\chi_{15}(v).
\end{aligned}$$

Les égalités dans (2) impliquent immédiatement le

Lemme 14. *Les entiers α, β, γ_i et δ_j vérifient :*

$$\alpha = 2^m + \sum_{i\in I} a_i\cdot 2^{n_i} + \sum_{j\in J} \alpha_j\cdot 2^{m_j}, \quad \beta = 2^n + \sum_{i\in I} b_i\cdot 2^{n_i} + \sum_{j\in J} \beta_j\cdot 2^{m_j},$$
$$\gamma_1 = \xi_1\cdot 2^n + \xi_2\cdot 2^m + \chi_3(u_2)\cdot 2^{n_2} + \chi_3(u_3)\cdot 2^{n_3} + \sum_{j\in J} \lambda_j\cdot 2^{m_j},$$
$$\gamma_2 = \gamma_3 = \chi_7(u)\cdot 2^n + \chi_7(v)\cdot 2^m + \chi_7(u_1)\cdot 2^{n_1},$$
$$\gamma_4 = \xi_3\cdot 2^n + \chi_{15}(v)\cdot 2^m + \chi_{15}(u_1)\cdot 2^{n_1} + \chi_3(u_3)\cdot 2^{n_3} + \chi_{15}(v_1)\cdot 2^{m_1},$$
$$\gamma_5 = \chi_{15}(u)\cdot 2^n + \xi_4\cdot 2^m + \chi_{15}(u_1)\cdot 2^{n_1} + \chi_3(u_2)\cdot 2^{n_2} + \chi_{15}(v_1)\cdot 2^{m_1},$$
$$\delta_1 = \chi_{15}(u)\cdot 2^n + \chi_{15}(v)\cdot 2^m + \big(\chi_3(u_1) + \chi_{15}(u_1)\big)\cdot 2^{n_1},$$
$$\delta_2 = \chi_7(u_1)\cdot 2^{n_1}, \quad \delta_3 = \chi_{13}(u)\cdot 2^n, \quad \delta_4 = \chi_9(u)\cdot 2^n, \quad \delta_5 = \chi_9(v)\cdot 2^m,$$
$$\delta_6 = \chi_{13}(v)\cdot 2^m, \quad \delta_7 = \delta_8 = \chi_{15}(u_1)\cdot 2^{n_1}.$$

Corollaire 15. *Si A est unitairement parfait, alors :*

(i) $a = 2^n u, b = 2^m v$ *où* $n, m \in \mathbb{N}$ *et* $u, v \in \{1,3,5,7,9,11,13,15\}$.
(ii) $I \subset \{1,\dots,5\}$ *et* $J \subset \{1,\dots,8\}$.
(iii) $c_1 = 2^{n_1} u_1$ *où* $u_1 \in \{0,1,3,5,7,15\}$.
(iv) $c_i = 2^{n_i} u_i$ *, avec* $u_i \in \{0,1,3\}$ *si* $i \in \{2,3\}$, $u_i \in \{0,1\}$ *si* $i \in \{4,5\}$.
(v) $d_j = 2^{m_j} v_j$ *où* $v_1 \in \{0,1,3\}$, $v_j \in \{0,1\}$ *si* $j \in \{2,\dots,8\}$.
(vi) $c_2 = c_3$ *et* $n, m, m_1, n_i \in \{0,1,2,3\}$, *pour tout* $i \le 5$.
(vii) $d_2, d_7, d_8 \in \{0, 2^{n_1}\}, d_3, d_4 \in \{0, 2^n\}$ *et* $d_5, d_6 \in \{0, 2^m\}$.

Preuve. Comme $\sigma^*(A) = A$, on a : $a = \alpha$, $b = \beta, c_i = \gamma_i$ et $d_j = \delta_j$.

Les points (i) à (v) résultent immédiatement des lemmes et corollaire ci-dessus.

(vi) : $c_2 = \gamma_2 = \gamma_3 = c_3$. D'après la Remarque 6, $\operatorname{pgcd}(a, b, (c_i)_{i\in I}, (d_j)_{j\in J})$ est impair, c'est-à-dire : l'un des $n, m, (n_i)_{i\in I}, (m_j)_{j\in J}$, au moins, est nul. On applique le Lemme 14.

- Si $n = 0$, alors de l'égalité : $u = a = \alpha$, on déduit que $2^m \le u \le 15$ et 2^{n_i}, $2^{m_j} \le u \le 15$ si $u_i, v_j \ne 0$.
- Si $m = 0$, alors $v = b = \beta$ et donc : 2^m, 2^{n_i}, $2^{m_j} \le 15$ si $u_i, v_j \ne 0$.
- De même, si $n_1 = 0$, alors $2^n, 2^m, 2^{n_2}, 2^{n_3}, 2^{m_j} \le u_1 \le 15$ si $u_2, u_3, v_j \ne 0$.
- Démarches analogues si ($n_2 = 0$ ou $n_3 = 0$ ou $m_1 = 0$).

(vii) résulte du fait que $d_j = \delta_j$, pour tout $j \in J$. □

2.3. *La preuve*

D'après la Remarque 6, B n'est pas un carré, ou encore, son polynôme dérivé B' est non nul. Par le Corollaire 15, on voit que $I \subset \{1,\dots,5\}$, $J \subset \{1,\dots,8\}$ et que l'on se restreint à un nombre fini de valeurs de $a, b, n, m, c_i, u_i, d_j, v_j$. On pourrait ainsi faire des calculs en `Maple`. Dans un premier temps, nous dressons la liste des 8-uplets $[n, u, m, v, n_1, u_1, n_2, u_2]$ tels que $a \ge 1, a \le b$ et $c_2 = \gamma_2$ (voir les Lemme 14 et Corollaire 15). On obtient (au bout d'une minute) 27468 tels 8-uplets. Ensuite, on applique les conditions : $d_j = \delta_j$. Au bout de 12 mn, cela donne 62292 18-uplets de la forme $[n, u, m, v, n_1, u_1, n_2, u_2, d_1, \dots, d_8, m_1, v_1]$. Après, les conditions : $a = \alpha$, $b = \beta$ et $B' \ne 0$ ne fournissent que 175 polynômes (moins de 4 mn). Parmi ces derniers, on trouve très vite ceux qui sont tels que $\sigma^*(B) + B = 0$. Ils sont 47. On obtient le Théorème 1.

3. Annexe

3.1. *Les polynômes* $B_1, \ldots, B_7, B_{13}, B_{25}, \ldots, B_{28}$

Chaque polynôme

$$B_j = x^a (x+1)^b \prod_{i=1}^{5} {M_i}^{c_i} \cdot \prod_{j=1}^{8} {S_j}^{d_j}$$

est tel que $a \leq b$.

Il est représenté sous la forme du 15-uplet : $(a, b, c_1, \ldots, c_5, d_1, \ldots, d_8)$.

On se contente d'en donner seulement une douzaine.

On voit que $\omega(B_j)$ est le nombre de colonnes non nulles, dans la ligne de B_j.

B	a	b	c_1	c_2	c_3	c_4	c_5	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	degré
B_1	5	6	3	0	0	1	0	1	0	0	0	0	0	0	0	25
B_2	5	9	2	0	0	1	0	0	0	0	0	1	0	0	0	28
B_3	6	7	3	1	1	0	0	1	0	0	0	0	0	0	0	29
B_4	6	9	4	0	0	0	0	0	0	0	0	1	0	0	0	29
B_5	7	9	2	1	1	0	0	0	0	0	0	1	0	0	0	32
B_6	5	9	3	0	0	1	0	1	0	0	0	1	0	0	0	34
B_7	7	9	3	1	1	0	0	1	0	0	0	1	0	0	0	38
B_{13}	9	9	6	0	0	0	0	2	0	0	1	1	0	0	0	50
B_{25}	13	14	7	3	3	1	1	0	1	1	0	0	0	0	0	85
B_{26}	13	13	12	0	0	0	0	4	0	1	0	0	1	0	0	90
B_{27}	14	18	7	3	3	1	1	0	1	0	0	2	0	0	0	90
B_{28}	13	18	12	0	0	0	0	4	0	1	0	2	0	0	0	95

3.2. *Deux autres exemples*

Pour $u \in \{11, 17\}$, on va construire une famille admissible $\mathcal{G}_u$ et puis, à partir de $\mathcal{G}_u$, une famille de polynômes unitairement parfaits contenant, cette fois, les deux polynômes « exceptionnels » E_{18} et E_{21} évoqués dans l'Introduction. La plupart des calculs sont obtenus par `Maple`. En principe, on devrait traiter tous les cas $v \leq u$, avec v impair, mais, pour alléger les démarches, on se contentera d'en considérer deux : $(u = 11, v \in \{9, 11\})$ et $(u = 17, v \in \{15, 17\})$.

3.2.1. *Cas* $u = 11,\ v \in \{9, 11\}$

(1) Factorisation de $\sigma(x^{u-1})$:

$$\sigma\left(x^{10}\right) = 1 + x + \cdots + x^{10} = 1 + x(x+1){M_4}^2 = {M_4}^{112} = V_1.$$

On pose : $V_2 = \overline{V_1} = {M_5}^{112} = \sigma((x+1)^{10})$ et on a : $\{V_1, V_2\} \subset \mathcal{G}_u$.

(2) Les diviseurs impairs et irréductibles de $1 + V_j$, $j \in \{1, 2\}$: M_4, M_5. Donc,

$$\{M_4, M_5, V_1, V_2\} \subset \mathcal{G}_u.$$

(3) Factorisation de $\sigma((x+1)^{v-1})$, pour $v \in \{9, 11\}$: $\sigma((x+1)^8) = M_1 S_5$, $\sigma((x+1)^{10}) = V_2$. Donc, $\{M_1, M_4, M_5, V_1, V_2, S_5, S_4 = \overline{S_5}\} \subset \mathcal{G}_u$. On peut prendre

$$\mathcal{G}_u = \{M_1, M_4, M_5, V_1, V_2, S_4, S_5\}.$$

(4) Il n'existe pas $S \in \mathcal{G}_u$ et $h \in \mathbb{N}^*$ tels que $\sigma(S^{2h})$ se factorise dans $\mathcal{G}_u$.
Donc, A est de la forme

$$x^a(x+1)^b {M_1}^{c_1} {M_4}^{c_4} {M_5}^{c_5} {V_1}^{d_1} {V_2}^{d_2} {S_4}^{d_4} {S_5}^{d_5},$$

où

$$a = 11 \cdot 2^n, \quad b = 2^m v, v \in \{9, 11\}, \quad c_i = 2^{n_i} u_i, \quad d_j = 2^{m_j} v_j, \quad u_i, v_j \geq 0$$

et l'un des n, m, n_i, m_j est nul (*i.e.* $A' \neq 0$). On voit, par des analogues des Lemme 14 et Corollaire 15, que $n, m \in \{0,1,2,3\}$, $d_1 = 2^n$, $d_2 = \chi_{11}(v) \cdot 2^m, d_5 = \chi_9(v) \cdot 2^m$, $d_4 = 0$, $c_4 = 2d_1, c_5 = 2d_2$ et $c_1 = d_4 + d_5 + \chi_9(v) \cdot 2^m = 2d_5$. On trouve deux polynômes dont l'exception E_{18}.

3.2.2. *Cas* $u = 17$, $v \in \{15, 17\}$

Pour $u = 17$, par la même méthode, on peut se limiter à

$$\mathcal{G}_u = \{M_1, \ldots, M_5, S_1, S_{11}, S_{14}, V_3, \ldots, V_6\} \ldots$$

$$A = x^a(x+1)^b \prod_{i=1}^{5} {M_i}^{c_i} \prod_{j=3}^{6} {V_j}^{d_j} {S_1}^{d_1} {S_{11}}^{d_{11}} {S_{14}}^{d_{14}},$$

avec : $a = 17 \cdot 2^n, b = 2^m v, n, m \in \{0, 1, \ldots, 4\}$, $d_1 = c_4 = c_5 = \chi_{15}(v) \cdot 2^m$,
$c_2 = d_3 = d_5 = 2^n$, $c_3 = d_4 = d_6 = \chi_{17}(v) \cdot 2^m, d_{11} = d_5, d_{14} = d_6$ et $c_1 = 2d_1 + d_{11} + d_{14}$.

On obtient un seul polynôme : E_{21}.

3.3. *Remarque finale*

Les précédents calculs et d'autres nous permettent d'énoncer la

Conjecture 16. *Pour tout entier impair $u \geq 3$, il existe un polynôme unitairement parfait sur $\mathbb{F}_2$, non scindé et divisible par x^u.*

Ainsi, il y aurait une infinité de classes de polynômes unitairement parfaits sur $\mathbb{F}_2$. Cela contrasterait avec ce que l'on (ne) connaît (pas) sur les nombres (unitairement) parfaits et sur les polynômes parfaits sur $\mathbb{F}_2$ [10, Section 4].

3.4. *Quelques fonctions utiles pour des calculs avec* `Maple`

- Générer un polynôme de Mersenne – Exemple : M1 := Mers(1,1) ;

```
> Mers:=proc(a,b) sort(Expand(1+x^a*(x+1)^b) mod 2):end:
```

- Générer un polynôme de la forme $Q^{abc} := 1 + x^a(x+1)^b Q^c$
Exemple : S1 := Qabc(M1,1,1,1) ;

```
> Qabc:=proc(Q,a,b,c) sort(Expand(1+x^a*(x+1)^b*Q^c) mod 2):end:
```

- $\omega(A), \sigma(A)$ et $\sigma^*(A)$

```
> OMEGA:=proc(A) nops((Factors(A) mod 2)[2]):end:

> SIGMA:=proc(A) DivExp:={}:sig:=1: L:=Factors(A) mod 2:
r:=nops(L[2]):
for i to r do DivExp:={op(DivExp),[L[2,i,1],L[2,i,2]]}:od:
for Q in DivExp do sig:=sig*sum(Q[1]^s,s=0..Q[2]):od:
Factor(sig) mod 2:end:
```

```
> SIGMASTAR:=proc(A) DivExp:={}:sigstar:=1: L:=Factors(A) mod 2:
r:=nops(L[2]):
for i to r do DivExp:={op(DivExp),[L[2,i,1],L[2,i,2]]}:od:
for Q in DivExp do sigstar:=sigstar*(1+Q[1]^Q[2]):od:
Factor(sigstar) mod 2:end:
```

Références

[1] J. T. B. j. Beard, « Unitary perfect polynomials over $GF(q)$ », *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* **62** (1977), nº 5, p. 417-422.

[2] J. T. B. j. Beard, A. T. Bullock, M. S. Harbin, « Infinitely many perfect and unitary perfect polynomials », *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* **63** (1977), nº 5, p. 294-303.

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

[4] L. H. Gallardo, O. Rahavandrainy, « Odd perfect polynomials over $\mathbb{F}_2$ », *J. Théor. Nombres Bordeaux* **19** (2007), nº 1, p. 165-174.

[5] ———, « Even perfect polynomials over $\mathbb{F}_2$ with four prime factors », *Int. J. Pure Appl. Math.* **52** (2009), nº 2, p. 301-314.

[6] ———, « There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors », *Port. Math. (N.S.)* **66** (2009), nº 2, p. 131-145.

[7] ———, « On even (unitary) perfect polynomials over $\mathbb{F}_2$ », *Finite Fields Appl.* **18** (2012), nº 5, p. 920-932.

[8] ———, « Characterization of Sporadic perfect polynomials over $\mathbb{F}_2$ », *Funct. Approximatio, Comment. Math.* **55** (2016), nº 1, p. 7-21.

[9] ———, « On Mersenne polynomials over $\mathbb{F}_2$ », *Finite Fields Appl.* **59** (2019), p. 284-296.

[10] ———, « On odd prime divisors of binary perfect polynomials », https://arxiv.org/abs/2007.16016, 2020.