CONTEMPORARY MATHEMATICS

686

Arithmetic, Geometry, Cryptography and Coding Theory

15th International Conference
Arithmetic, Geometry, Cryptography and Coding Theory
May 18–22, 2015
CIRM, Luminy, France

Alp Bassa
Alain Couvreur
David Kohel
Editors

American Mathematical Society

Contemporary Mathematics
Volume 686, 2017
http://dx.doi.org/10.1090/conm/686/13777

A infinite class of Kasami functions that are not APN infinitely often

Eric Férard

ABSTRACT. We consider a polynomial $f(x) = x^{2^{2r}-2^r+1} + g(x)$ over $\mathbb{F}_q$ of Kasami degree where degree d of $g(x)$ is $< 2^{2r} - 2^r + 1$. We prove that if $d \equiv 3 \bmod 4$, then the function $f(x)$ is not APN on infinitely many extensions of $\mathbb{F}_q$. We also obtain obtain partial results in the case where $d = 2^i t$ with $t \equiv 1 \bmod 4$.

1. Introduction

The vector Boolean functions are used in cryptography to construct block ciphers and an important criterion on these functions is high resistance to differential cryptanalysis.

Let $q = 2^n$ for some positive integer n and $\mathbb{F}_q$ a finite field with q elements. A function $f\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is said to be *almost perfect nonlinear (APN)* if the number of solutions in $\mathbb{F}_q$ of the equation

$$f(x+a) + f(x) = b$$

is at most 2, for all $a, b \in \mathbb{F}_q$ with $a \neq 0$. Nyberg proved that this kind of functions have a good resistance to differential cryptanalysis [**23**].

So far, the study of APN functions has focused on power functions. Recently it was generalised to other functions, particularly quadratic polynomials (Edel, Kyureghyan and Pott [**13**], Budaghyan, Carlet, Felke and Leander [**6**], Bracken, Tan and Tan [**5**], or Bluher [**3**]) or polynomials on small fields (Dillon [**12**]). On the other hand, several authors (Berger, Canteaut, Charpin and Laigle-Chapuy [**2**], Byrne and McGuire [**7**], Jedlicka [**20**], Rodier [**24**], Delgado and Janwa [**11**], or Férard and Rodier [**15, 16**]) showed that APN functions did not exist for a large class of infinite families.

The Gold functions x^{2^r+1} and the Kasami-Welch functions $x^{2^{2r}-2^r+1}$ are APN for an infinite number of extensions of $\mathbb{F}_2$. An exponent t is said to be *exceptional* if the function $f(x) = x^t$ is APN for an infinite number of extensions of $\mathbb{F}_2$. In [**17**], Hernando and McGuire obtain a result on the classification of APN monomials which had been conjectured in [**18**].

THEOREM 1. *The only exceptional exponents are the Gold and Kasami-Welch exponents.*

2010 *Mathematics Subject Classification.* Primary 11T06, 12E05, 14Q10, 11T71.
Key words and phrases. APN functions, finite fields, absolute irreducible polynomials.

In [1], Aubry, McGuire and Rodier formulate the following conjecture: a function $\mathbb{F}_q \longrightarrow \mathbb{F}_q$ can be APN for an infinity of extensions of $\mathbb{F}_q$ only if it is CCZ-equivalent (as was defined by Carlet, Charpin and Zinoviev in [8]) to a monomial x^t where t is an exceptional exponent.

A means to prove this conjecture is to remark that the APN property is equivalent to the fact that the rational points of the algebraic surface X in a 3-dimensional space defined by

$$\phi_f(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

(which is a polynomial in $\mathbb{F}_q[x,y,z]$) are all in a surface made of the three planes $x+y=0, x+z=0, y+z=0$. If X is absolutely irreducible (or has an absolutely irreducible component defined over $\mathbb{F}_q$) then f is not APN on $\mathbb{F}_{q^n}$ for all n sufficiently large. As shown in [24], this follows from the Lang-Weil bound for surfaces, which guarantees many $\mathbb{F}_{q^n}$-rational points on the surface X for all n sufficiently large. In this way, Aubry, McGuire and Rodier obtained the following results.

THEOREM 2. *If the degree of the polynomial function f is odd and not a Gold or a Kasami number then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.*

THEOREM 3. *If the degree of the polynomial function f is $2e$ with e odd, and if f contains a term of odd degree, then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.*

Aubry, McGuire and Rodier obtained also some partial results in the case of polynomial of Gold degree. These results have been generalized by Delgado and Janwa [11].

THEOREM 4. *Let $r \geq 2$ be an integer. Suppose that $f(x) = x^{2^r+1} + g(x)$ where $g(x)$ is a polynomial of degree $d < 2^r + 1$. Assume that one of the following two conditions is satisfied:*

(1) $d \equiv 3 \bmod 4$,
(2) $d \equiv 1 \bmod 4$ *and* $\phi_{x^{2^r+1}}, \phi_{x^d}$ *are relatively prime.*

Then $\phi_f(x,y,z)$ is not absolutely irreducible.

Rodier [25] and Caullery [10] studied the case of polynomials of degree $4e$.

THEOREM 5. *Let $f\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ such that $\deg(f) = 4e$ with $e \equiv 3 \bmod 4$ and $e > 3$, then f cannot be APN over infinitely many extensions of $\mathbb{F}_q$.*

In this paper, we consider the case of polynomials of Kasami degree. We will generalized the following results due to Férard, Oyono and Rodier [14].

THEOREM 6. *Suppose $f(x) = x^{2^{2r}-2^r+1} + g(x)$ where $\deg(g) \leq 2^{2r-1} - 2^{r-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2r-1}-2^{r-1}+1} a_j x^j$. Suppose moreover that there exists a nonzero coefficient a_j such that ϕ_{x^j} is prime to ϕ_{x^d}. Then $\phi_f(x,y,z)$ is absolutely irreducible.*

THEOREM 7. *Let $q = 2^n$. Let $r \geq 3$ be odd and relatively prime to n. Suppose $f(x) = x^{2^{2r}-2^r+1} + g(x)$ where $g(x) \in \mathbb{F}_q[x]$ and $\deg(g) = 2^{2r-1} - 2^{r-1} + 2$. If $g(x)$ does not have the form $ax^{2^{2r-1}-2^{r-1}+2} + a^2x^3$ then ϕ_f is absolutely irreducible, while if $g(x)$ does have the form $ax^{2^{2r-1}-2^{r-1}+2} + a^2x^3$ then either ϕ_f is irreducible or ϕ_f splits into two absolutely irreducible factors which are both defined over $\mathbb{F}_q$.*

The proof of these theorems use, among other things, the factorization of $\phi_{2^{2r}-2^r+1}(x,y,z)$ over $\mathbb{F}_{2^r}$ given by Janwa and Wilson [19].

THEOREM 8. *If* $f(x) = x^{2^{2r}-2^r+1}$ *then*

$$\phi_f(x,y,z) = \prod_{\alpha \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2} q_\alpha(x,y,z)$$

where for each α, $q_\alpha(x,y,z)$ *is an absolutely irreducible polynomial of degree* 2^r+1 *on* $\mathbb{F}_{2^r}$ *such that* $q_\alpha(x,0,1) = (x-\alpha)^{2^r+1}$.

The object of the third section is to obtain more information about this factorization. Then, we will, in the four section, study the hyperplane section of the surface X by the plane $y = z$. In the fifth section, we prove that if $f(x) = x^{2^{2r}-2^r+1} + g(x)$ where $g(x)$ is a polynomial which satisfies some conditions, then $\phi_f(x,y,z)$ is absolutely irreducible. In particular, f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

2. Preliminaries

We fix an algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. Let $\mathbb{F}_q$ be a finite field of characteristic 2 and let $f\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ be a function given by a polynomial in $\mathbb{F}_q[x]$. We define

$$\phi_f(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

which is a polynomial in $\mathbb{F}_q[x,y,z]$. We write $\phi_f(x,y)$ for $\phi_f(x,y,1)$. More generally, for each polynomial $p(x,y,z)$, we write $p(x,y)$ for $p(x,y,1)$. The context should make clear whether we are thinking projectively in three variables, or affinely in two.

If $f(x) = \sum_{j=0}^{d} a_j x^j$, then

$$\phi_f(x,y,z) = \sum_{j=3}^{d} a_j \phi_j(x,y,z),$$

where $\phi_j(x,y,z)$ the ϕ function associated to the monomial x^j. The function $\phi_j(x,y,z)$ is homogeneous of degree $j-3$.

Let r be an integer ≥ 2, ℓ be an odd integer ≥ 3 and $t = 2^r\ell + 1$. We define

$$f_t(x,y) = x^t + y^t + 1 + (x+y+1)^t.$$

We have $\phi_t(x,y) = \frac{f_t(x,y)}{(x+y)(x+1)(y+1)}$.

3. Another proof of a theorem of Janwa-Wilson

Let r be an integer ≥ 2. Let $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent. We set $e = 2^r + 1$ and $g_{k_r}(x,y) = f_{k_r}(x^e, y^e)$. We define

$$\psi_{k_r}(x,y) = \phi_{k_r}(x^e, y^e) = \frac{g_{k_r}(x,y)}{(x^e+y^e)(x^e+1)(y^e+1)}$$

which is a polynomial of degree $e(k_r - 3)$.

Let $K = \mathbb{F}_{2^r}$ and $L = \mathbb{F}_{2^{2r}}$. We will give the decomposition of $\psi_{k_r}(x,y)$ into linear factors in $L[x,y]$. We consider first the equation

$$x^e + y^e = 1 \tag{1}$$

in $(L^*)^2$. For $x \in L^*$, we have $x^e = \mathrm{Nm}_{L/K}(x)$ where $\mathrm{Nm}_{L/K}(\cdot)$ designed the norm of L over K. Therefore, this equation is equivalent to

$$\mathrm{Nm}_{L/K}(x) + \mathrm{Nm}_{L/K}(y) = 1.$$

If $\mathrm{Nm}_{L/K}(x) = 1$, then the equation has no solution in L^* (there is exactly $2^r + 1$ such elements in L^*). If $\mathrm{Nm}_{L/K}(x) \neq 1$, then the equation has exactly $2^r + 1$ solutions in L. Thus, the equation (1) has exactly

$$(2^{2r} - 1 - (2^r + 1))(2^r + 1) = (k_r - 3)e$$

solution in $(L^*)^2$.

LEMMA 1. *Let r be an integer ≥ 2, $L = \mathbb{F}_{2^{2r}}$ and $k_r = 2^{2r} - 2^r + 1$. Then*

$$\psi_{k_r}(x, y) = \prod_{(a,b)} (y + ax + b)$$

where the product is taken over the solutions (a, b) of equation (1) in $(L^*)^2$.

PROOF. For $X = x^e$ and $Y = y^e$, we have

$$g_{k_r}(x, y) = \frac{1}{(X + Y + 1)^{2^r}}(X^{2^r}Y^{k_r} + X^{k_r}Y^{2^r} + X^{2^{2r}}Y + XY^{2^{2r}} + X^{2^{2r}} + Y^{2^{2r}} + X^{k_r} + Y^{k_r} + X^{2^r} + Y^{2^r} + X + Y).$$

If we set $y = ax + b$ with $a, b \in L^*$, a calculation shows that

$$X^{2^r}Y^{k_r} + X^{k_r}Y^{2^r} + X^{2^{2r}}Y + XY^{2^{2r}} + X^{2^{2r}} + Y^{2^{2r}} + X^{k_r} + Y^{k_r} + X^{2^r} + Y^{2^r} + X + Y = (a^e + b^e + 1)(x^e + x^{e2^r} + x^{e2^{2r}} + x^{2^{3r}+1}).$$

It follows that $g_{k_r}(x, y) = 0$ if and only if $a^e + b^e = 1$. For each solution $(a, b) \in (L^*)^2$ of (1), we have $\psi_{k_r}(x, ax + b) = 0$. Since the polynomial $\psi_{k_r}(x, y)$ is monic as a univariate polynomial in the variable y and of degree $e(k_r - 3)$, we have obtained the lemma. □

We also have

$$\psi_{k_r}(x, y) = \psi_{k_r}(y, x) = \prod_{(a,b)} (x + ay + b)$$

where the product is taken over $(a, b) \in (L^*)^2$ such that $a^e + b^e = 1$.

LEMMA 2. *Let r be an integer ≥ 2, $K = \mathbb{F}_{2^r}$ and $L = \mathbb{F}_{2^{2r}}$. Given a solution $(a', b') \in (L^*)^2$ of (1), there exists an unique element $(a, b) \in (K^*)^2$ such that*

$$\mathrm{Nm}_{L/K}(a) = \mathrm{Nm}_{L/K}(a') \text{ and } \mathrm{Nm}_{L/K}(b) = \mathrm{Nm}_{L/K}(b').$$

Moreover, $b = a + 1$.

PROOF. Let $a' \in L^*$ and $a \in K^*$. If c' is an element of L such that $c'^2 = a'$, then $\mathrm{Nm}_{L/K}(a) = \mathrm{Nm}_{L/K}(a')$ if and only if $a = c'^e \in K$.

Let (a', b') be an element of $(L^*)^2$ which satisfies (1). By what we have seen just above, there exists an unique element (a, b) of $(K^*)^2$ such that $\mathrm{Nm}_{L/K}(a) = \mathrm{Nm}_{L/K}(a')$ and $\mathrm{Nm}_{L/K}(b) = \mathrm{Nm}_{L/K}(b')$. Moreover, we have

$$a^2 + b^2 = a^e + b^e = a'^e + b'^e = 1.$$

Thus $a = b + 1$. □

For each $a \in K\backslash\mathbb{F}_2$, there exists an unique $b \in K$ such that (a, b) is a solution of (1). In fact, $b = a + 1$. We define

$$u_a(x, y) = \prod_{(a',b')} (x + a'y + b')$$

where the product is taken over elements (a', b') of $(L^*)^2$ satisfying $\mathrm{Nm}_{L/K}(a') = \mathrm{Nm}_{L/K}(a)$ and $\mathrm{Nm}_{L/K}(b') = \mathrm{Nm}_{L/K}(b)$. The polynomial $u_a(x, y)$ is defined over K and of degree e^2. Indeed, if the pair (a, b) satisfies $\mathrm{Nm}_{L/K}(a') = \mathrm{Nm}_{L/K}(a)$ and $\mathrm{Nm}_{L/K}(b') = \mathrm{Nm}_{L/K}(b)$, then the same is true for the pair (a'^{e-1}, b'^{e-1}) and the polynomial

$$(x + a'y + b')(x + a'^{e-1}y + b'^{e-1}) \in K[x, y].$$

On the other hand, we have $\mathrm{Nm}_{L/K}(a') = \mathrm{Nm}_{L/K}(a)$ if and only if $a' = ua$ where u is an element of L such that $u^e = 1$. From this, we deduce that the degree of $u_a(x, y)$ is e^2.

If a_1 and a_2 are two distinct elements of $K\backslash\mathbb{F}_2$, then the polynomials $u_{a_1}(x, y)$ and $u_{a_2}(x, y)$ are relatively prime. Indeed, we have $a_1^e \neq a_2^e$. Thus, if $\mathrm{Nm}_{L/K}(a_1') = \mathrm{Nm}_{L/K}(a_1)$ and $\mathrm{Nm}_{L/K}(a_2') = \mathrm{Nm}_{L/K}(a_2)$, then $a_1' \neq a_2'$ and $x + a_1'y + 1 \neq x + a_2'y + 1$.

If g designed a primitive eth root of unity in L, then the polynomial $u_a(x, y)$ can also be written

$$u_a(x, y) = \prod_{0 \leq i,j \leq e-1} (x + g^i a y + g^j b),$$

where $b = a+1$. The following proposition is an immediate consequence of lemmas 1 and 2.

PROPOSITION 1. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ and $K = \mathbb{F}_{2^r}$. Then we have*

$$\psi_{k_r}(x, y) = \prod_{a \in K\backslash\mathbb{F}_2} u_a(x, y).$$

LEMMA 3. *Let r be an integer ≥ 2. For all $a \in \mathbb{F}_{2^r}\backslash\mathbb{F}_2$, we have $u_a(y, x) = a^4 u_{a^{-1}}(x, y)$.*

PROOF. If we set $b = a + 1$, then we have

$$\begin{aligned} u_a(y, x) &= \prod_{i,j} (y + g^i a x + g^j b) \\ &= \prod_{i,j} g^i a (g^{-i} a^{-1} y + x + g^{j-i} a^{-1} b) \\ &= a^4 \prod_{i',k} (x + g^{i'} a^{-1} y + x + g^k a^{-1} b) \\ &= a^4 u_{a^{-1}}(x, y). \end{aligned}$$

□

We will now show that there exists an unique polynomial $v_a(x, y)$ defined over K such that $u_a(x, y) = v_a(x^e, y^e)$.

LEMMA 4. *Let r be an integer ≥ 2, $e = 2^r + 1$ and g a primitive eth root of unity in $L = \mathbb{F}_{2^{2r}}$. Let $a, b, d \in \overline{\mathbb{F}}_2$. Then*

$$\prod_{0 \leq i,j \leq e-1} (x + (g^i ad + g^j b)y) = \prod_{i=0}^{e-1} (x^e + (g^i ad + b)^e y^e).$$

PROOF. We have

$$\prod_{0 \leq i,j \leq e-1} (x + g^i ad + g^j b) = \prod_{0 \leq i_0, k \leq e-1} (x + (g^{i_0} ad + b)g^k)$$

and

$$\prod_{k=0}^{e-1} (x + (g^{i_0} ad + b)g^k) = x^e + (g^{i_0} ad + b)^e.$$

This proves our lemma. □

LEMMA 5. *Let F be a field and let e be an integer ≥ 2. Then the map*

$$\theta \colon F[x, y] \longrightarrow F[x, y], \quad A(x, y) \longmapsto A(x^e, y^e)$$

is an injective ring homomorphism.

PROOF. The map θ is clearly linear, injective and we have

$$\theta(x^i y^j x^k x^l) = x^{ie} y^{je} x^{ke} y^{le} = \theta(x^i y^j)\theta(x^k y^l).$$

So θ is a ring homomorphism. □

LEMMA 6. *Let $P(x, y)$ be a polynomial over $\overline{\mathbb{F}}_2$. Let e be an integer ≥ 2. Then there exists a polynomial $Q(x, y) \in \overline{\mathbb{F}}_2[x, y]$ such that $P(x, y) = Q(x^e, y^e)$ if and only if for all pair $(c, d) \in \overline{\mathbb{F}}_2^2$, there exists two polynomials $A_c(y) \in \overline{\mathbb{F}}_2[y]$ and $B_d(x) \in \overline{\mathbb{F}}_2[x]$ such that*

$$P(x, d) = B_d(x^e) \text{ and } P(c, y) = A_c(y^e).$$

Moreover, the polynomial $Q(x, y)$ is unique and if the polynomial $P(x, y)$ is defined over a subfield of $\overline{\mathbb{F}}_2$. the same is true for $Q(x, y)$.

PROOF. Let $P(x, y) = \sum_{i,j} a_{i,j} x^i y^j \in \overline{\mathbb{F}}_2[x, y]$. Assume that for all pair $(c, d) \in \overline{\mathbb{F}}_2^2$, there exists $A_c(y) \in \overline{\mathbb{F}}_2[y]$ and $B_d(x) \in \overline{\mathbb{F}}_2[x]$ such that $P(x, d) = B_d(x^e)$ and $P(c, y) = A_c(y^e)$. We will prove that $a_{i,j} = 0$ for all pair (i, j) such that i or j is not divisible by e. For all $d \in \overline{\mathbb{F}}_2$, we have

$$B_d(x^e) = P(x, d) = \sum_{i,j} a_{i,j} x^i d^j = \sum_i x^i \sum_j a_{i,j} d^j,$$

which implies that $\sum_j a_{i,j} d^j$ for all i not divisible by e. In other words, $\sum a_{i,j} y^j$ is the zero polynomial. Hence, $a_{i,j} = 0$ for all pair (i, j) such that i is not divisible by e. We prove similarly that $a_{i,j} = 0$ for all pair (i, j) such that j is not divisible by e. If we set $Q(x, y) = \sum a_{i,j} x^{i/e} y^{j/e}$, then $P(x, y) = Q(x^e, y^e)$. The unicity follows from the previous lemma and if $P(x, y)$ is defined over a subfield of $\overline{\mathbb{F}}_2$, it is clear that the same is true for $Q(x, y)$. The converse is trivial. □

LEMMA 7. *Let r be an integer ≥ 2 and $e = 2^r + 1$. For each $a \in \mathbb{F}_{2^r} \backslash \mathbb{F}_2$, there exists an unique polynomial $v_a(x, y)$ over $\mathbb{F}_{2^r}$ such that*

$$u_a(x, y) = v_a(x^e, y^e).$$

PROOF. By lemma 4, we have

$$u_a(x,d) = \prod_{0\le i,j\le e-1} (x + g^i ad + g^j b) = \prod_{i=1}^{e-1} (x^e + (g^i ad + g^j b)^e y^e)$$

for all $d \in \overline{\mathbb{F}}_2$. So, all the exponents of the polynomial $u_a(x,d)$ are divisible by e. The same is true for the exponents of the polynomial $u_a(c,y) = a^4 u_{a^{-1}}(y,c)$ for all $c \in \overline{\mathbb{F}}_2$. According to the previous lemma, there exists an unique polynomial $v_a(x,y) \in \mathbb{F}_{2^r}[x,y]$ such that $u_a(x,y) = v_a(x^e, y^e)$. □

We will give an elementary proof of the factorization of $\phi_{k_r}(x,y)$ obtained by Janwa-Wilson (see theorem 8). Furthermore, we obtain more information about this factorization.

THEOREM 9. *Let r be an integer ≥ 2, $K = \mathbb{F}_{2^r}$, $L = \mathbb{F}_{2^{2r}}$, $e = 2^r + 1$ and $k_r = 2^{2r} - 2^r + 1$. Then*

$$\phi_{k_r}(x,y) = \prod_{a \in K \setminus \mathbb{F}_2} v_a(x,y),$$

where for each a, $v_a(x,y)$ is an absolutely irreducible polynomial of degree e over K. Moreover, $v_a(x,y)$ is the unique polynomial over K such that

$$v_a(x^e, y^e) = \prod_{(a',b')} (x + a'y + b')$$

where the product is taken over the pair $(a',b') \in (L^*)^2$ such that $\mathrm{Nm}_{L/K}(a') = \mathrm{Nm}_{L/K}(a)$ and $\mathrm{Nm}_{L/K}(b') = \mathrm{Nm}_{L/K}(a+1)$.

PROOF. Let a be an element of $K \setminus \mathbb{F}_2$ and $b = a + 1$. We prove first that the polynomial $v_a(x,y)$ defined in lemma 7 is absolutely irreducible. Let $p(x,y)$ be a polynomial of positive degree over $\overline{\mathbb{F}}_2$ which divides $v_a(x,y)$. Then $p(x,y)q(x,y) = v_a(x,y)$ for some polynomial $q(x,y)$ over $\overline{\mathbb{F}}_2$. We have

$$p(x^e,y^e)q(x^e,y^e) = v_a(x^e,y^e) = u_a(x,y) = \prod_{i,j} (x + g^i ay + g^j b).$$

It is obvious that the polynomials in the product are relatively prime. Since we assume that the polynomial $p(x,y)$ is of positive degree, there exists i_0, j_0 such that $x + g^{i_0} ay + g^{j_0} b$ divides $p(x^e, y^e)$. Put $p_0(x,y) = x + g^{i_0} ay + g^{j_0} b$. For all the integers i', j', the polynomial $p_0(g^{i'}x, g^{j'}y)$ divides $p(x^e, y^e)$ (since $g^e = 1$). In particular, for all integers i, j such that $0 \le i, j < e$, the polynomial

$$p_0(g^{j_0-j}x, g^{i-i_0+j_0-j}y) = g^{j_0-j}x + g^{i+j_0-j}ay + g^{j_0}b = g^{j_0-j}(x + g^i ay + g^j b)$$

divides $p(x^e, y^e)$. It follows that $\prod_{i,j}(x + g^i ay + g^j)$ divides $p(x^e, y^e)$ and so $p(x^e, y^e) = v_a(x^e, y^e)$ (up to a scalar). Therefore, $p(x,y) = v_a(x,y)$ (up to a scalar). So, the polynomial $v_a(x,y)$ is absolutely irreducible.

We have seen that

$$\phi_{k_r}(x^e, y^e) = \psi_{k_r}(x,y) = \prod_{a \in K \setminus \mathbb{F}_2} u_a(x,y) = \prod_{a \in K \setminus \mathbb{F}_2} v_a(x^e, y^e).$$

We deduce from the lemma 5 that $\phi_{k_r}(x,y) = \prod_{a \in K \setminus \mathbb{F}_2} v_a(x,y)$. □

REMARK 1. Janwa and Wilson [**18**] proved that

$$\phi_{k_r}(x,y) = \prod_{\gamma \in K\backslash \mathbb{F}_2} q_\gamma(x,y)$$

where for each γ, $q_\gamma(x,y)$ is an absolutely irreducible polynomial of degree e over K such that $q_\gamma(x,0) = (x+\gamma)^e$ (see theorem 8). With the notations of the previous theorem, we have

$$q_{b^e}(x,y) = v_a(x,y).$$

COROLLARY 1. *Let r be an integer ≥ 2, $K = \mathbb{F}_{2^r}$, $L = \mathbb{F}_{2r}$, $e = 2^r+1$ and $k_r = 2^{2r} - 2^r + 1$. Then*

$$\phi_{k_r}(x,y,z) = \frac{x^{k_r} + y^{k_r} + z^{k_r} + (x+y+z)^{k_r}}{(x+y)(x+z)(y+z)} = \prod_{a \in K\backslash \mathbb{F}_2} v_a(x,y,z),$$

where for each $a \in K\backslash\mathbb{F}_2$, $v_a(x,y,z)$ is an absolutely irreducible polynomial of degree e over K. Moreover, $v_a(x,y,z)$ is the unique polynomial over K such that

$$v_a(x^e, y^e, z^e) = \prod_{(a',b')} (x + a'y + b'z)$$

where the product is taken over the pair (a',b') of $(L^*)^2$ such that $\mathrm{Nm}_{L/K}(a') = \mathrm{Nm}_{L/K}(a)$ and $\mathrm{Nm}_{L/K}(b') = \mathrm{Nm}_{L/K}(a+1)$.

PROOF. We have

$$\phi_{k_r}(x,y,z) = \frac{x^{k_r} + y^{k_r} + z^{k_r} + (x+y+z)^{k_r}}{(x+y)(x+z)(y+z)} = \prod_{a \in K\backslash \mathbb{F}_2} v_a(x,y,z),$$

where $v_a(x,y,z) = z^e v_a\left(\frac{x}{z}, \frac{y}{z}\right)$ is the homogenization of $v_a(x,y)$. By lemma 7, we have

$$v_a(x^e, y^e, z^e) = z^{e^2} \prod_{a',b'} \left(\frac{x}{z} + a'\frac{y}{z} + b'\right) = \prod_{(a',b')} (x + a'y + b'z). \qquad \square$$

4. Hyperplane sections

The aim of this section is to study the hyperplane section by the plane $y = z$ of the surface of equation $\phi_{k_r}(x,y,z) = 0$. More precisely, we will give the decomposition into absolutely irreducible components of the hyperplane section of the surface of equation $v_a(x,y,z) = 0$ by the plane $y = z$.

COROLLARY 2. *Let r be an integer ≥ 2 and $K = \mathbb{F}_{2^r}$. For all $a \in K\backslash\mathbb{F}_2$, we have*

$$v_a(x,y,y) = (x+y) \prod_{i=1}^{2^{r-1}} (x + \rho_i(a)y)^2,$$

where $\rho_i(a) = a(a+1)(g^i + g^{-i}) + 1 \in K$.

PROOF. Put $e = 2^r+1$ and $N = (e-1)/4 = 2^{r-2}$. By corollary 1 and lemma 4, we have

$$v_a(x^e, y^e, y^e) = \prod_{i,j} (x + (g^i a + g^j b)y) = \prod_{i=0}^{4N} (x^e + (g^i a + b)^e y^e),$$

where $b = a + 1$. Since $(g^i a + b)^e = a^e + g^{-i}ab + g^i ab + b^e = \rho_i(a)$, $\rho_{2N+i}(a) = \rho_{2N+1-i}(a)$ for $i = 1, \ldots, 2N$ and $\rho_0(a) = 1$, we have

$$v_a(x^e, y^e, y^e) = (x^e + y^e) \prod_{i=1}^{2N} (x^e + \rho_i(a) y^e)^2.$$

From this, we deduce, using lemma 5, that

$$v_a(x, y, y) = (x + y) \prod_{i=1}^{2N} (x + \rho_i(a) y)^2. \qquad \square$$

We wish to determine the gcd of $v_a(x, y, y)$ and $v_{a'}(x, y, y)$. The case where $a = a' + 1$ is the object of the following lemma.

LEMMA 8. *Let r be an integer ≥ 2. Let $a, a' \in \mathbb{F}_{2^r} \backslash \mathbb{F}_2$. Then $v_a(x, y, y) = v_{a'}(x, y, y)$ if and only if $a - a' \in \mathbb{F}_2$.*

PROOF. Put $e = 2^r + 1$. We have

$$\sum_{i=1}^{(e-1)/2} \rho_i(a) = a(a+1) \sum_{i=1}^{(e-1)/2} (g^i + g^{-i}) = a(a+1) \sum_{i=1}^{e-1} g^i = a(a+1) \frac{g + g^e}{g + 1} = a(a+1).$$

If $v_a(x, y) = v_{a'}(x, y)$, then $\sum_{i=1}^{(e-1)/2} \rho_i(a) = \sum_{i=1}^{(e-1)/2} \rho_i(a')$ and $a(a+1) = a'(a'+1)$, which implies that $a = a'$ or $a = a' + 1$. The converse is trivial. $\square$

In the case where $a' \neq a$ and $a' \neq a + 1$, we need to study the equation $\rho_i(a) = \rho_{i'}(a')$. We consider first the equation $u + u^{-1} = \beta$ in L^* where β is an element of $K \backslash \mathbb{F}_2$. It is equivalent to

$$u^2 + \beta u + 1 = 0.$$

If $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta^{-1}) = 0$, it has two solutions in K. Assume that $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta^{-1}) = 1$. Note that

$$\mathrm{Tr}_{L/\mathbb{F}_2}(\beta^{-1}) = \mathrm{Tr}_{K/\mathbb{F}_2}(\mathrm{Tr}_{L/K}(\beta^{-1})) = \mathrm{Tr}_{K/\mathbb{F}_2}(0) = 0$$

as $\beta \in K$. Thus, the equation has two distinct solutions u_1, u_2 in $L \backslash K$. Since $u_1 u_2 = 1$, $\beta \in K$ and $u_1, u_2 \in L \backslash K$, we have

$$u_2 = u_1^{2^r} \text{ and } u_1^e = 1.$$

We have shown the following result.

LEMMA 9. *Let r be an integer ≥ 2, $e = 2^r + 1$, $K = \mathbb{F}_{2^r}$ and $L = \mathbb{F}_{2^{2r}}$. Let $\beta \in K \backslash \mathbb{F}_2$.*

1. *If $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta^{-1}) = 0$, then the equation $u + u^{-1} = \beta$ has two distinct solutions in K.*
2. *If $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta^{-1}) = 1$, then the equation $u + u^{-1} = \beta$ has two distinct solutions in $L \backslash K$. Moreover, if u is a solution, then $u^e = 1$ and the other solution is u^{-1}.*

For $a \in K$ and $u \in L^*$, we set

$$\rho(u, a) = a(a + 1)(u + u^{-1}) + 1 \in L.$$

Given $a \in K \backslash \mathbb{F}_2$, we have $\rho(u, a) \in K \backslash \mathbb{F}_2$ for all u such that $u^e = 1$ and $u \neq 1$. Indeed, it is obvious that $\rho(u, a) \in K$ and $\rho(u, a) \neq 1$. If $\rho(u, a) = 0$, then

$a(a+1) = \frac{1}{u+u^{-1}}$ and we have $0 = \mathrm{Tr}_{K/\mathbb{F}_2}(a^2+a) = \mathrm{Tr}_{K/\mathbb{F}_2}\frac{1}{u+u^{-1}} = 1$, which is absurd. Thus, $a(a+1) \neq \frac{1}{u+u^{-1}}$ and $\rho(u,a) \neq 0$.

For all $a, a' \in K\backslash\mathbb{F}_2$ and $u \in L\backslash\mathbb{F}_2$, we have $\rho(u,a) = \rho(u,a')$ if and only if $a = a'$ or $a = a'+1$.

LEMMA 10. *Let r be an integer ≥ 2, $e = 2^r+1$ and $K = \mathbb{F}_{2^r}$. Let $a \in K\backslash\mathbb{F}_2$, $u, u' \in L^*$ such that $u^e = u'^e = 1$. Then $\rho(u,a) = \rho(u',a)$ if and only if $u = u'$ or $u = u'^{-1}$.*

PROOF. Assume that $\rho(u,a) = \rho(u',a)$. Then $\mathrm{Tr}_{L/K}(u) = \mathrm{Tr}_{L/K}(u')$ and we can write $u = u' + d$ with $d \in K$. We have

$$1 = u^e = u'^e + u'^{e-1}d + u'd^{e-1} + d^e = 1 + (u' + u'^{-1})d + d^2.$$

It follows that $(u' + u'^{-1})d + d^2 = 0$, and finally $d = 0$ or $d = u' + u'^{-1}$. The converse is immediate. □

The following lemma is an immediate consequence of the fact that the $\mathbb{F}_2$-bilinear pairing $K \times K \longrightarrow \mathbb{F}_2, (x,y) \longmapsto \mathrm{Tr}_{K/\mathbb{F}_2}(xy)$ is nondegenerate.

LEMMA 11. *Let r be an integer ≥ 2, $K = \mathbb{F}_{2^r}$ and n an integer between 1 and r. Let $(\lambda_0, \ldots, \lambda_{n-1})$ be a linearly independent family of elements of K. Let $\delta_0, \ldots, \delta_{n-1}$ be elements of $\mathbb{F}_2$. Then the system*

$$\mathrm{Tr}_{K/\mathbb{F}_2}(\lambda_0 x) = \delta_0, \ldots, \mathrm{Tr}_{K/\mathbb{F}_2}(\lambda_{n-1}x) = \delta_{n-1}$$

has 2^{r-n} solutions.

We denote by T a system of representatives of the orbits of $K\backslash\mathbb{F}_2$ acted on additively by $\mathbb{F}_2$. We now define an equivalence relation on the set of elements $u \in L\backslash\mathbb{F}_2$ such that $u^e = 1$. Two such elements u, u' are said equivalent if $u = u'$ or $u = u'^{-1}$. We denote by U a system of representatives of the classes of this relation.

We recall that we define, for all integer i, $\rho_i(a) = \rho(g^i, a)$. We recall also that

$$v_a(x,y,y) = (x+y)\prod_{i=1}^{2N}(x + \rho_i(a)y)^2$$

with $N = 2^{r-2}$. The lemma 10 shows that one can write

$$v_a(x,y,y) = (x+y)\prod_{u\in U}(x+uy)^2.$$

Moreover, the factors are pairwise distinct.

LEMMA 12. *Let r be an integer ≥ 2. Let a, a' be two distinct elements of T. Then there exists exactly 2^{r-2} elements $u' \in U$ such that the equation*

$$\rho(u,a) = \rho(u',a')$$

has exactly one solution u (resp. has no solution) in U.

PROOF. The equation $\rho(u,a) = \rho(u',a')$ is equivalent to

$$u + u^{-1} = \frac{u' + u'^{-1}}{\lambda} \text{ with } \lambda = \frac{a(a+1)}{a'(a'+1)}.$$

By lemma 9, it has an unique solution in U if and only if $\mathrm{Tr}_{K/\mathbb{F}_2} \frac{\lambda}{u'+u'^{-1}} = 1$. This last condition is equivalent to $y = \frac{1}{u'+u'^{-1}}$ and $\mathrm{Tr}_{K/\mathbb{F}_2} \lambda y = 1$. Since $K \cap U = \emptyset$, the lemma 9 shows that this is the same as saying that

$$\begin{cases} \mathrm{Tr}_{K/\mathbb{F}_2} y = 1, \\ \mathrm{Tr}_{K/\mathbb{F}_2} \lambda y = 1. \end{cases}$$

Moreover, for each solution $y \in K$ of this system, there exists exactly one solution $u \in U$ of the equation $\rho(u, a) = \rho(u', a')$. Since $\lambda \notin \mathbb{F}_2$, the previous lemma shows that there exists 2^{r-2} elements $u' \in U$ such that the system has exactly one solution. Moreover, for every other elements of U, there is no solution. To conclude, there exists exactly 2^{r-2} elements $u' \in U$ such that the equation $\rho(u, a) = \rho(u', a')$ has exactly one solution (resp. has no solution) in U. □

PROPOSITION 2. *Let r be an integer ≥ 2. Put $N = 2^{r-2}$. Let $a, a' \in \mathbb{F}_{2^r} - \mathbb{F}_2$ such that $a \neq a', a'+1$. Then there exists distinct integers $i_1, \ldots, i_N$ between 1 and $2N$ such that the gcd of $v_a(x, y, y)$ and $v_{a'}(x, y, y)$ is*

$$(x+y) \prod_{k=1}^{N} (x + \rho_{i_k}(a) y)^2.$$

PROOF. Let i' be an integer between 1 and $2N$. Consider the equation

$$\rho_i(a) = \rho_{i'}(a')$$

with i, $1 \leq i \leq 2N$. By lemma 12, there exists N integers i' between 1 and $2N$ such that the equation has exactly one solution (resp. no solution).

On the other hand, we have seen that

$$v_a(x, y, y) = (x+y) \prod_{i=1}^{2N} (x + \rho_i(a) y)^2 \text{ and } v_{a'}(x, y, y) = (x+y) \prod_{i'=1}^{2N} (x + \rho_{i'}(a') y)^2.$$

Therefore, there exists N distinct integers $i_1, \ldots, i_N$ (the solutions of the equation) between 1 and $2N$ such that the gcd of $v_a(x, y, y)$ and $v_{a'}(x, y, y)$ is

$$(x+y) \prod_{k=1}^{N} (x + \rho_{i_k}(a) y)^2.$$ □

REMARK 2. One can prove that there exists distinct integers $i_1, \ldots, i_{N/2}$ between 1 and $2N$ such that the gcd of $v_a(x, y, y)$ and $v_{a'}(x, y, y)$ is

$$(x+y) \prod_{k=1}^{N/2} (x + \rho_{i_k}(a) y)^2 (x + \rho_{i_k}(a)^{-1} y)^2.$$

We will now prove that for each element a of $K \backslash \mathbb{F}_2$, there exists an primitive element γ of K such that $x + \gamma y$ divides $v_a(x, y, y)$. To each family $(\gamma_1, \ldots, \gamma_{n-1})$ of K, we associate a system of equations

$$\rho(u_1, a) = \gamma_1, \ldots, \rho(u_n, a) = \gamma_n \tag{2}$$

with $(a, u_1, \ldots, u_{n-1}) \in T \times U^{n-1}$. It is clearly equivalent to

$$\begin{cases} a^2 + a &= \frac{\gamma_1+1}{u_1+u_1^{-1}}, \\ a^2 + a &= \frac{\gamma_2+1}{u_2+u_2^{-1}}, \\ &\vdots \\ a^2 + a &= \frac{\gamma_{n-1}+1}{u_{n-1}+u_{n-1}^{-1}}. \end{cases}$$

Note that if $(a, u_1, \ldots, u_{n-1})$ is a solution of (2) in $T \times U^{n-1}$, then $u_1, \ldots, u_{n-1} \in U$ are entirely determined by a.

Consider the linear system of equations

$$\begin{cases} \mathrm{Tr}_{K/\mathbb{F}_2} y & = 1, \\ \mathrm{Tr}_{K/\mathbb{F}_2}(\gamma_1 + 1)y & = 0, \\ \mathrm{Tr}_{K/\mathbb{F}_2} \frac{\gamma_1+1}{\gamma_2+1} y & = 1, \\ & \vdots \\ \mathrm{Tr}_{K/\mathbb{F}_2} \frac{\gamma_1+1}{\gamma_{n-1}+1} y & = 1 \end{cases} \tag{3}$$

with $y \in K$.

LEMMA 13. *The solutions of the system (2) (in $T \times U^{n-1}$) are in bijection with the solutions of the system (3) (in K).*

PROOF. Let θ be the map which associate to each solution $(a, u_1, \ldots, u_{n-1}) \in T \times U^{n-1}$ of (2) the solution $y = \frac{1}{u_1+u_1^{-1}}$ of (3). It is clearly surjective and if $\theta(a, u_1, \ldots, u_{n-1}) = \theta(a', u'_1, \ldots, u'_{n-1})$, then

$$\frac{1}{u_1 + u_1^{-1}} = \frac{1}{u'_1 + u'^{-1}_1},$$

which implies $u_1 = u'_1 \in T$, $a = a' \in T$ and finally $u_2 = u'_2$, $\ldots$, $u_{n-1} = u'_{n-1}$. □

LEMMA 14. *Let r be an integer ≥ 2 and $K = \mathbb{F}_{2^r}$. Let $\gamma_1, \ldots, \gamma_{r-1}$ be elements of $K \backslash \mathbb{F}_2$ such that the family $(1, \frac{1}{\gamma_1+1}, \ldots, \frac{1}{\gamma_{r-1}+1})$ is a basis of K over $\mathbb{F}_2$. Then, for each $a \in K \backslash \mathbb{F}_2$, there exists an integer j between 1 and $r-1$ such that the equation $\rho(u, a) = \gamma_j$ has a solution in U.*

PROOF. For all integer j between 1 and $r-1$, let A_j be the set of elements a in T for which there exists $u_j \in U$ such that $\rho(u_j, a) = \gamma_j$. We want to prove that $\cup_{j=1}^{r-1} A_j = T$. For all family $(j_1, \ldots, j_m)$ of m distinct integers of $\{1, \ldots, r-1\}$ (with $1 \leq m \leq r-1$), the cardinality of $A_{j_1} \cap \cdots \cap A_{j_m}$ is the number of solutions of the system (3) associated to the family $(\gamma_{j_1}, \ldots, \gamma_{j_m})$. Since the family

$$\left(1, \gamma_{j_1} + 1, \frac{\gamma_{j_1}+1}{\gamma_{j_2}+1}, \ldots, \frac{\gamma_{j_1}+1}{\gamma_{j_m}+1}\right)$$

is linearly independent, by lemma 11, this cardinality is $N/2^{m-1}$. By the inclusion-exclusion principle, we have

$$\begin{aligned}\#\bigcup_{j=1}^{r-1} A_j &= \sum_{m=1}^{r-1}\Big((-1)^{m-1}\sum_{1\le j_1<j_2<\cdots<j_m\le r-1}\#A_{j_1}\cap A_{j_2}\cap\cdots\cap A_{j_m}\Big)\\ &= \sum_{m=1}^{r-1}(-1)^{m+1}\binom{r-1}{m}\frac{N}{2^{m-1}} = \frac{N}{2^{r-2}}\sum_{m=1}^{r-1}(-1)^{m+1}\binom{r-1}{m}2^{r-m-1}\\ &= 2N-1 = \#T\end{aligned}$$

as $N = 2^{r-2}$ and

$$1 = (2-1)^{r-1} = \sum_{m=0}^{r-1}(-1)^m\binom{r-1}{m}2^{r-1-m}.$$

It follows that for each element a in T, there exists an integer j between 1 and $2N$ such that the equation $\rho(u,a) = \gamma_j$ has a solution in U. □

LEMMA 15. *Let r be an integer ≥ 2 and $K = \mathbb{F}_{2^r}$. Given $a \in K\backslash\mathbb{F}_2$, there exists at least an integer i between 1 and 2^{r-1} such that $\rho_i(a)$ is an primitive element of K.*

PROOF. We handle the case where $r = 4$ with Magma. Assume that $r \neq 4$. According to a theorem of Kapetanakis [**21**], one can find a primitive normal basis $(\gamma_0, \gamma_1, \ldots, \gamma_{r-1})$ of K over $\mathbb{F}_2$ such that

$$\Big(\frac{1}{\gamma_0+1}, \ldots, \frac{1}{\gamma_{r-1}+1}\Big)$$

is a basis of K over $\mathbb{F}_2$. The sum $\sum_{i=0}^{r-1}\frac{1}{\gamma_i+1}$ is invariant by Galois, hence equal to 0 or 1. Since the family $(\frac{1}{\gamma_0+1}, \ldots, \frac{1}{\gamma_{r-1}+1})$ is linearly independent, it must be equal to 1. So, the family $(1, \frac{1}{\gamma_1+1}, \ldots, \frac{1}{\gamma_{r-1}+1})$ is linearly independent. By the previous lemma, for each $a \in K\backslash\mathbb{F}_2$, there exists two integers i, j with $1 \le i \le 2^{r-1}$ and $1 \le j \le r-1$ such that $\rho_i(a) = \gamma_j$. □

LEMMA 16. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$, j be an integer ≥ 2, ℓ be an odd integer ≥ 1 and $t = 2^j\ell + 1$. If $\phi_{k_r}(x,y,z)$ and $\phi_t(x,y,z)$ are not relatively prime, then $2^r - 1$ divides ℓ.*

PROOF. By theorem 9, $v_a(x,y,z)$ divides $\phi_t(x,y,z)$ for some element a of $K\backslash\mathbb{F}_2$. It follows $v_a(x,y,y)$ divides $\phi_t(x,y,y)$. On the other hand, Delgado-Janwa [**11**] proved that

$$\phi_t(x,y,y) = \frac{(x^\ell + y^\ell)^{2^j}}{(x+y)^2}.$$

From this, we deduce, using corollary 2, that $\rho_i(a)^\ell = 1$ for $i = 1, \ldots, 2^{r-1}$. By lemma 15, we conclude that $2^r - 1$ divides ℓ. □

REMARK 3. Let t be an integer ≥ 7 with $t \equiv 3 \bmod 4$. We write $t = 3 + 4m$ with an integer $m \ge 1$. If $\phi_{k_r}(x,y,z)$ and $\phi_t(x,y,z)$ are not relatively prime, then

$$m \equiv 2^{r-1} - 1 \bmod 2^r - 1.$$

Indeed, we have $\phi_t(x,y,y) = \frac{(x^{1+2m}+y^{1+2m})^2}{(x+y)^2}$ (see lemma 2 in [**11**]) and we prove, as in the previous lemma, that $2^r - 1$ divides $1 + 2m$.

LEMMA 17. *Let r be an integer ≥ 2 and $K = \mathbb{F}_{2^r}$. Let A, A' be a partition of $K\backslash\mathbb{F}_2$. Then there exists $a_0 \in A$, $a'_0 \in A'$ and a primitive element γ of K such that $x + \gamma y$ divides $v_{a_0}(x, y, y)$ and $v_{a'_0}(x, y, y)$.*

PROOF. If there exists $a \in A$ (resp. $a' \in A'$) such that $a + 1 \in A'$ (resp. $a' + 1 \in A$) , the lemma is trivial (since $v_a(x, y, y) = v_{a+1}(x, y, y)$). So, we can assume that this is not the case. Let $a \in A$ and $a' \in A'$. Since A and A' are stable by $\mathbb{F}_2$ by the above hypothesis, we can assume that $a, a' \in T$. By corollary 2 and proposition 2, we can write

$$v_a(x, y, y) = (x + y)\prod_{i=1}^{2N}(x + \gamma_i y)^2$$

and

$$v_{a'}(x, y, y) = (x + y)\prod_{i'=1}^{N}(x + \gamma'_{i'} y)^2 \prod_{i=N+1}^{2N}(x + \gamma_i y)^2$$

with $N = 2^{r-2}$ and $\gamma_i, \gamma_{i'} \in K\backslash\mathbb{F}_2$. The elements γ_i are pairwise distinct and, for all i, i', $1 \leq i, i' \leq N$, we have $\gamma_i \neq \gamma'_{i'}$.

We will prove that the system (2), or equivalently (3), associated to the family $(\gamma_1, \ldots, \gamma_N)$ has at least two distinct solutions. Since it has solution, it suffices to prove that the family $(1, \gamma_1 + 1, \frac{\gamma_1+1}{\gamma_2+1} \ldots, \frac{\gamma_1+1}{\gamma_N+1})$, or equivalently the family $(1, \frac{1}{\gamma_1+1}, \ldots, \frac{1}{\gamma_N+1})$, is of rank $< r$. If it is of rank r, then, we can assume (reordering the indices if necessary) that the family $(1, \frac{1}{\gamma_1+1}, \ldots, \frac{1}{\gamma_{r-1}+1})$ is a basis of K over $\mathbb{F}_2$. By lemma 14, there exists an integer j, $1 \leq j \leq r - 1$ and $u \in U$ such that $\rho(u, a') = \gamma_j$. Then $x + \gamma_j y$ is a factor of $v_{a'}(x, y, y)$. Since the elements γ_i are pairwise distinct, γ_j must be equal to a $\gamma_{i'}$, $1 \leq i' \leq N$, which contradict our hypothesis

Since the system has at least two distinct solutions, there exists an element $a'' \in T$, $a'' \neq a, a'$, such that $x + \gamma_1 y, \ldots, x + \gamma_N y$ divides $v_{a''}(x, y, y)$. Then, by proposition 2, we have necessarily

$$v_{a''}(x, y, y) = (x + y)\prod_{i=1}^{N}(x + \gamma_i y)^2(x + \gamma'_i y)^2.$$

If one of the elements $\gamma_{N+1}, \ldots, \gamma_{2N}$ is a primitive element of K, it suffices to choose $a_0 = a$ and $a'_0 = a'$. If this is not the case, by the lemma 15, there exists two integers i_0 and i'_0 between 1 and N such that γ_{i_0} and $\gamma'_{i'_0}$ are primitives elements. We choose $a_0 = a''$ and $a'_0 = a'$ if $a'' \in A$ and $a_0 = a$ and $a'_0 = a''$ in the contrary. □

5. Polynomials of Kasami Degree

In this section, we prove, under some hypothesis, that if $f(x)$ is a polynomial of Kasami degree, then $\phi_f(x, y, z)$ is not absolutely irreducible. In particular, the function $f(x)$ can not be APN on infinitely many extensions.

Let r be an integer ≥ 2 and $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent. Let d be an integer, $1 \leq d < k_r$ and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree $d < k_r$. If we set $f(x) = \sum_{i=0}^{k_r} a_i x^i$, then

$$\phi_f(x, y, z) = \sum_{i=3}^{k_r} a_i \phi_i(x, y, z).$$

We will consider two cases: $d \equiv 3 \bmod 4$ and $d = 2^i t$ with $t \equiv 1 \bmod 4$. In the first case, we follow the ideas of Aubry-McGuire-Rodier [1] and Delgado-Janwa [11].

THEOREM 10. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent, d be an integer, $1 \leq d < k_r$ and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d. If $d \equiv 3 \bmod 4$, then $\phi_f(x, y, z)$ is absolutely irreducible.*

PROOF. Delgado-Janwa [11] have shown that $x + y$ does not divide $\phi_d(x, y, y)$.

Assume that $\phi_f(x, y, z)$ is not absolutely irreducible. There exists two polynomials P and Q of positive degree such that $\phi_f(x, y, z) = P(x, y, z)Q(x, y, z)$. If we write P and Q as a sum of homogeneous polynomials, we get

$$\phi_f(x, y, z) = PQ = (P_s + \cdots + P_0)(Q_t + \cdots + Q_0) = \sum_{\ell=0}^{s+t} \sum_{j=0}^{t} P_{s+t-\ell-j} Q_j,$$

where P_j and Q_j are homogeneous of degree j (we put $P_i = 0$ if $i < 0$ and Q_j if $j < 0$). We can assume that $s \geq t > 0$. We have $s + t = k_r - 3$ and $0 < t \leq \frac{k_r - 3}{2} \leq s < k_r - 3$. On the other hand, we have

$$P_s(x, y, z)Q_t(x, y, z) = \phi_{k_r}(x, y, z) = \prod_{a \in K \setminus \mathbb{F}_2} v_a(x, y, z)$$

with $K = \mathbb{F}_{2^r}$. In particular, this implies that P_s and Q_t are relatively prime as the product is made of distinct irreducible factors. Moreover, we can write

$$P_s(x, y, z) = \prod_{a \in A} v_a(x, y, z) \text{ and } Q_t(x, y, z) = \prod_{a \in A'} v_a(x, y, z)$$

where A and A' is a partition of $K \setminus \mathbb{F}_2$. We set $e = k_r - d$. Delgado-Janwa [11] showed that $P_{s-1} = \cdots = P_{s-(e-1)} = 0 = Q_{t-1} = \cdots = Q_{t-(e-1)}$ and

$$a_d \phi_d(x, y, z) = P_s Q_{t-e} + P_{s-e} Q_t.$$

If $Q_{t-e} = 0$, then $a_d \phi_d = P_{s-e} Q_t$. Thus, there exists $a' \in A'$ such that $v_{a'}(x, y, y)$ divides $\phi_d(x, y, y)$ and, in particular, $x + y$ divides $\phi_d(x, y, y)$, which is impossible, as we said above. We prove similarly that $P_{t-e} \neq 0$.

Assume $Q_{t-e} \neq 0$ and $P_{t-e} \neq 0$. Then we have

$$a_d \phi_d(x, y, y) = P_s(x, y, y)Q_{t-e}(x, y, y) + P_{s-e}(x, y, y)Q_t(x, y, y).$$

So there exists $a \in A$ and $a' \in A'$ such that the gcd, and in particular $x + y$, divides $\phi_d(x, y, y)$, which is impossible, as we said above. □

We now study the case where $d = 2^i t$ with $t \equiv 1 \bmod 4$.

LEMMA 18. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ be a Kasami exponent and t be an integer ≥ 5 such that $t \equiv 1 \bmod 4$. We write $t = 2^j \ell + 1$ with an integer $j \geq 2$ and an odd integer $\ell \geq 1$. If $\phi_{k_r}(x, y, z)$ and $\phi_t(x, y, z)$ are not relatively prime, then $j = r$ and*

$$\ell = \frac{2^{2r(n+1)} - 1}{2^r + 1}$$

with an integer $n \geq 0$.

PROOF. We put $K = \mathbb{F}_{2^r}$ and $e = 2^r + 1$. Recall that the factorization of $\phi_{k_r}(x, y)$ into absolutely irreducible polynomials is

$$\phi_{k_r}(x, y) = \prod_{a \in K \setminus \mathbb{F}_2} v_a(x, y).$$

Thus, there exists $a \in K\backslash\mathbb{F}_2$ such that $v_a(x,y)$ divides $\phi_t(x,y)$. It follows that $u_a(x,y) = v_a(x^e,y^e)$ divides $f_t(x^e,y^e)$. Since

$$u_a(x,y) = \prod_{0\leq i,j\leq e-1} (x + g^i a y + g^j b),$$

we see that $x + ay + b$ divides $f_t(x^e,y^e)$ where $b = a + 1$. We have

$$\begin{aligned}(ay+b)^e + y^e + 1 &= (a^e+1)y^e + a^{e-1}by^{e-1} + ab^{e-1}y + (b^e+1)\\ &= b^e y^e + a^{e-1}by^{e-1} + ab^{e-1}y + a^e\\ &= b^e(y^e + c^{e-1}y^{e-1} + cy + c^e)\\ &= b^e(y+c)^e\end{aligned}$$

where $c = a/b$. If we set $s = et$, then $s = (2^r+1)(2^j\ell+1) > 2^{r+j}$. For $x = ay + b$, we have

$$\begin{aligned}0 = f_t(x^e,y^e) &= (ay+b)^s + y^s + 1 + ((ay+b)^e + y^e + 1)^t\\ &= (ay+b)^s + y^s + 1 + b^s(y+c)^s\\ &= a^s + b^s + 1 + \sum_{i=1}^{s-1} \binom{s}{i} (a^i b^{s-i} + b^s c^{s-i}) y^i + (a^s + b^s + 1)y^s.\end{aligned}$$

From this, we get

$$\binom{s}{i}(c^i + c^{s-i}) = 0$$

for $i = 1,\ldots,s-1$.

Let ν be the order of c. Note that ν is positive and divides $2^r - 1$ (as $c \in K\backslash\mathbb{F}_2$). By lemma 16, $\ell \equiv 0 \bmod 2^r - 1$, which implies that $t \equiv 1 \bmod \nu$. For $i = 1,\ldots,s-1$, we have $c^i = c^{s-i}$ if and only if $s \equiv 2i \bmod \nu$. Since $e \equiv 2 \bmod \nu$, it is also equivalent to

$$e(t-i) \equiv e(1-i) \equiv 0 \bmod \nu.$$

Since ν and e are coprime, this is equivalent to $i \equiv 1 \bmod \nu$.

Assume that s can not be written in the form $2^k + 1$ with an integer k. Let

$$s = \sum_{p=0}^{m} s_p 2^p,$$

with $s_m = 1$, be the 2-adic development of s ($m \geq r + j \geq 4$ as $s > 2^{r+j}$). Since s is odd, we have $s_0 = 1$. By hypothesis, there exists an integer p, $0 < p < m$, such that $s_p = 1$. By Lucas' theorem [**22**], the binomial coefficient $\binom{s}{2^p+1}$ is odd (as $s_p = 1$). As $2^p + 1 \not\equiv 1 \bmod \nu$, we have

$$\binom{s}{2^p+1}(a^i b^{s-i} + b^s c^{s-i}) \neq 0,$$

which is impossible. Therefore, s can be written in the form $s = 2^k + 1$ with an integer $k > r + j$ (as $s > 2^{r+j}$). Then k is necessarily congruent to r modulo $2r$ (as $2^k \equiv -1 \bmod 2^r + 1$). So, we can write k in the form $k = r + 2r(n+1)$ with an integer $n \geq 0$ (as $k > r + j$). From this, we get

$$\ell = 2^{r-j}\frac{2^{2r(n+1)} - 1}{e}.$$

Moreover, since ℓ is odd, we have $r = j$. □

THEOREM 11. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ a Kasami exponent, d an integer, $5 \leq d \leq 2^{2r-1} - 2^{r-1} + 1$ and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d. We write $d = 2^i t$ with t an odd integer and i an integer ≥ 0. If $t \geq 5$ and $t \equiv 1 \bmod 4$, then $\phi_f(x, y, z)$ is absolutely irreducible.*

PROOF. It suffices to prove that $\phi_{k_r}(x, y)$ and $\phi_d(x, y)$ are relatively prime (see theorem 6). We write $t = 1 + 2^j \ell$ with an integer $j \geq 2$ and an odd integer $\ell \geq 1$. We have

$$\phi_d(x, y, z) = ((x + y)(x + z)(y + z))^{2^i - 1} \phi_t(x, y, z)^{2^i}.$$

Rodier proved that $(x+y)(x+z)(y+z)$ does not divide $\phi_{k_r}(x, y, z)$ (see lemma 6.1 in [**25**]). Hence, the polynomial $\phi_d(x, y)$ is relatively prime to $\phi_{k_r}(x, y)$ if and only if the polynomial $\phi_t(x, y)$ is relatively prime to $\phi_{k_r}(x, y)$.

By the previous lemma, $\phi_{k_r}(x, y)$ and $\phi_t(x, y)$ are relatively prime if $j \neq r$ or if ℓ can not be written in the form

$$\ell = \frac{2^{2r(n+1)} - 1}{2^r + 1}$$

with an integer $n \geq 0$. To conclude, it remains to note that if $j = r$ and $\ell = \frac{2^{2r(n+1)}-1}{2^r+1}$ with an integer $n \geq 0$, then

$$t = 2^r \ell + 1 = 2^r \frac{2^{2r(n+1)} - 1}{2^r + 1} + 1 > 2^{2r-1} - 2^{r-1} + 1,$$

which contradicts our hypothesis. □

THEOREM 12. *Let r be an integer ≥ 2, $k_r = 2^{2r} - 2^r + 1$ a Kasami exponent, d an odd integer, $5 \leq d < k_r$ and $f(x) = x^{k_r} + g(x)$ where $g(x)$ is a polynomial of degree d. Assume that $d \equiv 1 \bmod 4$. We write $d = 1 + 2^j \ell$ with ℓ an odd integer and j an integer ≥ 2. If $2^r - 1$ does not divide ℓ, then $\phi_f(x, y, z)$ is absolutely irreducible.*

PROOF. Assume that $\phi_f(x, y, z)$ is not absolutely irreducible. With the notations of the proof of theorem 10, we have

$$a_d \phi_d = P_s Q_{t-e} + P_{s-e} Q_t, P_s(x, y, z) = \prod_{a \in A} v_a(x, y, z)$$

and

$$Q_t(x, y, z) = \prod_{a \in A'} v_a(x, y, z)$$

where A and A' is a partition of $K \backslash \mathbb{F}_2$. By the lemma 17, there exists $a_0 \in A$, $a_0' \in A'$ and a primitive element γ of K such that $x + \gamma y$ divides $v_{a_0}(x, y, y)$ and $v_{a_0'}(x, y, y)$. We have

$$a_d \phi_d(x, y, y) = P_s(x, y, y) Q_{t-e}(x, y, y) + P_{s-e}(x, y, y) Q_t(x, y, y).$$

On the other hand, Delgado-Janwa [**11**] have shown that

$$\phi_d(x, y, y) = \frac{(x^\ell + y^\ell)^{2^j}}{(x + y)^2}.$$

Thus, $x + \gamma y$ divides $\phi_d(x, y, y)$. It follows that $\gamma^\ell = 1$ and $2^r - 1$ divides ℓ. □

Acknowledgements

The author would like to thanks François Rodier for helpful comments.

References

[1] Yves Aubry, Gary McGuire, and François Rodier, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 23–31, DOI 10.1090/conm/518/10193. MR2648536

[2] Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy, *On almost perfect nonlinear functions over F_2^n*, IEEE Trans. Inform. Theory **52** (2006), no. 9, 4160–4170, DOI 10.1109/TIT.2006.880036. MR2298539

[3] Antonia W. Bluher, *On existence of Budaghyan-Carlet APN hexanomials*, Finite Fields Appl. **24** (2013), 118–123, DOI 10.1016/j.ffa.2013.06.003. MR3093861

[4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. **14** (2008), no. 3, 703–714, DOI 10.1016/j.ffa.2007.11.002. MR2435056

[5] Carl Bracken, Chik How Tan, and Yin Tan, *On a class of quadratic polynomials with no zeros and its application to APN functions*, Finite Fields Appl. **25** (2014), 26–36, DOI 10.1016/j.ffa.2013.08.006. MR3130587

[6] L. Budaghyan, C. Carlet, P. Felke, G. Leander, *An infinite class of quadratic APN functions which are not equivalent to power mappings*. Proceedings of the IEEE International Symposium on Information Theory (2006), 2637–2641.

[7] E. Byrne, G. McGuire, *On the non-existence of quadratic APN and crooked functions on finite fields*. Proceedings of the Workshop on Coding and Cryptography, WCC (2005), 316–324.

[8] Claude Carlet, Pascale Charpin, and Victor Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15** (1998), no. 2, 125–156, DOI 10.1023/A:1008344232130. MR1658423

[9] Florian Caullery, *A new large class of functions not APN infinitely often*, Des. Codes Cryptogr. **73** (2014), no. 2, 601–614, DOI 10.1007/s10623-014-9956-2. MR3237947

[10] Florian Caullery, *A new large class of functions not APN infinitely often*. arXiv:1309.7776 [cs.IT]

[11] M. Delgado, H. Janwa, *On the conjecture on APN functions*, arXiv:1207.5528 [cs.IT].

[12] J. F. Dillon, *APN Polynomials: An update*. Invited talk at Fq9, the 9th International Conference on Finite Fields and their Applications, July 2009.

[13] Yves Edel, Gohar Kyureghyan, and Alexander Pott, *A new APN function which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 744–747, DOI 10.1109/TIT.2005.862128. MR2236189

[14] Eric Férard, Roger Oyono, and François Rodier, *Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 27–36, DOI 10.1090/conm/574/11423. MR2961397

[15] Eric Férard and François Rodier, *Non linéarité des fonctions booléennes données par des polynômes de degré binaire 3 définies sur $\mathbb{F}_{2^m}$ avec m pair* (French, with English and French summaries), Arithmetic, geometry, cryptography and coding theory 2009, Contemp. Math., vol. 521, Amer. Math. Soc., Providence, RI, 2010, pp. 41–53, DOI 10.1090/conm/521/10272. MR2744032

[16] Eric Férard and François Rodier, *Non linéarité des fonctions booléennes données par des traces de polynômes de degré binaire 3* (French, with English and French summaries), Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 388–409, DOI 10.1142/9789812793430_0021. MR2484066

[17] Fernando Hernando and Gary McGuire, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, J. Algebra **343** (2011), 78–92, DOI 10.1016/j.jalgebra.2011.06.019. MR2824545

[18] Heeralal Janwa, Gary M. McGuire, and Richard M. Wilson, *Double-error-correcting cyclic codes and absolutely irreducible polynomials over* GF(2), J. Algebra **178** (1995), no. 2, 665–676, DOI 10.1006/jabr.1995.1372. MR1359909

[19] H. Janwa and R. M. Wilson, *Hyperplane sections of Fermat varieties in* $\mathbf{P}^3$ *in* char. 2 *and some applications to cyclic codes*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 180–194, DOI 10.1007/3-540-56686-4_43. MR1251978

[20] David Jedlicka, *APN monomials over* $\mathrm{GF}(2^n)$ *for infinitely many* n, Finite Fields Appl. **13** (2007), no. 4, 1006–1028, DOI 10.1016/j.ffa.2007.04.004. MR2360537

[21] Giorgos Kapetanakis, *Normal bases and primitive elements over finite fields*, Finite Fields Appl. **26** (2014), 123–143, DOI 10.1016/j.ffa.2013.12.002. MR3151363

[22] Edouard Lucas, *Theorie des Fonctions Numeriques Simplement Periodiques* (French), Amer. J. Math. **1** (1878), no. 4, 289–321, DOI 10.2307/2369373. MR1505176

[23] Kaisa Nyberg, *Differentially uniform mappings for cryptography*, Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 55–64, DOI 10.1007/3-540-48285-7_6. MR1290329

[24] François Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires* (French, with English summary), Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 169–181, DOI 10.1090/conm/487/09531. MR2555993

[25] François Rodier, *Functions of degree* $4e$ *that are not APN infinitely often*, Cryptogr. Commun. **3** (2011), no. 4, 227–240, DOI 10.1007/s12095-011-0050-6. MR2847294

ÉQUIPE GAATI, UNIVERSITÉ DE LA POLYNÉSIE FRANÇAISE
E-mail address: eric.ferard@upf.pf