Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents

Eric Férard, Roger Oyono, François Rodier

Some More Functions That Are Not APN Infinitely Often. The Case of Gold and Kasami exponents

Eric Férard, Roger Oyono, and François Rodier

Abstract. We prove a necessary condition for some polynomials of Gold and Kasami degree to be APN over $\mathbb{F}_{q^n}$ for large n.

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. A function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is said to be *almost perfect nonlinear* (APN) on $\mathbb{F}_q$ if the number of solutions in $\mathbb{F}_q$ of the equation

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

is at most 2, for all $a, b \in \mathbb{F}_q$, $a \neq 0$. This kind of function has a good resistance to differential cryptanalysis as was proved by Nyberg in [**20**].

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 [**11**], or Budaghyan, Carlet, Felke and Leander [**4**]) or polynomials on small fields (Dillon [**9**]). On the other hand, several authors (Berger, Canteaut, Charpin and Laigle-Chapuy [**2**], Byrne and McGuire [**5**], Jedlicka [**17**], Rodier [**21**], or Férard and Rodier [**12, 13**]) showed that APN functions did not exist in certain cases.

There are many classes of function for which it can be shown that each function is APN for at most a finite number of extensions [**23, 21**]. So we fix a finite field $\mathbb{F}_q$ and a function $f : \mathbb{F}_q \to \mathbb{F}_q$ given by a polynomial in $\mathbb{F}_q[x]$ and we set the question of whether this function can be APN for an infinite number of extensions of $\mathbb{F}_q$.

In this approach, Hernando and McGuire [**14**] showed a result on the classification of APN monomials which has been conjectured for 40 years: the only exponents such that the monomial x^d are APN over infinitely many extension of $\mathbb{F}_2$ are of the form $2^i + 1$ or $4^i - 2^i + 1$. One calls these exponents *exceptional*

1991 *Mathematics Subject Classification.* 11T06, 12E05, 14Q10, 11T71.

Key words and phrases. APN functions, algebraic surfaces, finite fields, absolute irreducible polynomials.

exponents. Then it is natural to formulate for polynomial functions the following conjecture.

CONJECTURE 1.1 (Aubry, McGuire and Rodier). *A polynomial on $\mathbb{F}_q$ 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* [**7**]*) 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

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

(which is a polynomial in $\mathbb{F}_q[x,y,z]$) are all in a surface V made of the three planes $x+y=0, x+z=0, y+z=0$.

Some cases of this conjecture have been studied already, in particular the case of polynomials of odd degree, not Gold or Kasami [**1**]. It is also true for polynomials of degree < 13 (see [**1**] and [**21**]). Some partials results have been obtain in case of polynomials of Gold degree or of even degree [**1, 22**]. We recall them in Section 3 (see Theorems 3.1 to 3.5). Nevertheless, in characteristic 3, there exists polynomials, not equivalent to monomials, which are PN for an infinity of extensions of $\mathbb{F}_q$ (see [**18**, théorème 3.3.7] or [**8, 10**]). In this paper, we will study polynomials of Kasami degree. The proofs happen to be somehow the same as in Gold degree, with a few changes anyway.

In Section 5, we study the special case of binomials of Gold and Kasami degree. For instance, we prove that any binomial of Gold degree could not be APN on infinitely many extensions of $\mathbb{F}_q$.

2. Preliminaries

We define

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

which is a polynomial in $\mathbb{F}_q[x,y,z]$. This polynomial defines a surface X in the three dimensional affine space $\mathbb{A}^3$.

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 [**21**], this follows from the Lang-Weil bound for surfaces, which guarantees many $\mathbb{F}_{q^n}$-rational points on the surface for all n sufficiently large.

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

We recall a result due to Janwa, Wilson, [**15**, Theorem 5] about Kasami exponents.

THEOREM 2.1. *If $f(x)=x^{2^{2k}-2^k+1}$ then*

$$\phi(x,y,z)=\prod_{\alpha\in\mathbb{F}_{2^k}-\mathbb{F}_2} p_\alpha(x,y,z) \tag{2.1}$$

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

3. Some Functions That Are Not APN Infinitely Often

The best known examples of APN functions are the Gold functions x^{2^k+1} and the Kasami-Welch functions $x^{4^k-2^k+1}$. These functions are defined over $\mathbb{F}_2$, and are APN on any field $\mathbb{F}_{2^m}$ where $\gcd(k,m)=1$. For other odd degree polynomial functions, we can state a general result.

THEOREM 3.1 (Aubry, McGuire and Rodier, [**1**]). *If the degree of the polynomial function f is odd and not a Gold or a Kasami-Welch number then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.*

In the even degree case, we can state the result when half of the degree is odd, with an extra minor condition.

THEOREM 3.2 (Aubry, McGuire and Rodier, [**1**]). *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.*

In [**22**] we have some results for the case of polynomials of degree $4e$ where e is odd.

THEOREM 3.3. *If the degree of the polynomial function f is even such that $\deg(f)=4e$ with $e\equiv 3 \pmod 4$, and if the polynomials of the form*

$$(x+y)(y+z)(z+x)+P$$

with

$$P(x,y,z)=c_1(x^2+y^2+z^2)+c_4(xy+xz+zy)+b_1(x+y+z)+d \tag{3.1}$$

for $c_1,c_4,b_1,d\in\mathbb{F}_{q^3}$, do not divide ϕ then f is not APN over $\mathbb{F}_{q^n}$ for n large.

We have more precise results for polynomials of degree 12.

THEOREM 3.4. *If the degree of the polynomial f defined over $\mathbb{F}_q$ is 12, then either f is not APN over $\mathbb{F}_{q^n}$ for large n or f is CCZ equivalent to the Gold function x^3. In this case f is of the form*

$$L(x^3)+L_1 \text{ or } (L(x))^3+L_1$$

where L is a linearized polynomial

$$x^4+x^2(c^{1+q}+c^{1+q^2}+c^{q+q^2})+xc^{1+q+q^2},$$

c is an element of $\mathbb{F}_{q^3}$ such that $c+c^q+c^{q^2}=0$ and L_1 is a q-affine polynomial of degree at most 8 (that is a polynomial whose monomials are of degree 0 or a power of 2).

We have some results on the polynomials of Gold degree $d=2^k+1$.

THEOREM 3.5 (Aubry, McGuire and Rodier, [**1**]). *Suppose $f(x)=x^d+g(x)$ where $\deg(g)\le 2^{k-1}+1$. Let $g(x)=\sum_{j=0}^{2^{k-1}+1}a_jx^j$. Suppose moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x,y,z)$ is absolutely irreducible (where $\phi_i(x,y,z)$ denote the polynomial $\phi(x,y,z)$ associated to x^i). Then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.*

4. Polynomials of Kasami Degree

Suppose the degree of f is a Kasami number $d = 2^{2k} - 2^k + 1$. Set d to be this value for this section. Write f as $f(x) = x^d + g(x)$ with $\deg(g) \leq d - 1$.

Then the degree of ϕ is $d - 3 = 2^{2k} - 2^k - 2$. We will prove the absolute irreducibility for a certain type of f.

4.1. The case $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$.

THEOREM 4.1. *Suppose $f(x) = x^d + g(x)$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then $\phi(x, y, z)$ is absolutely irreducible.*

Proof: Suppose $\phi(x, y, z) = P(x, y, z)Q(x, y, z)$ with $\deg P \geq \deg Q$. Write each polynomial as a sum of homogeneous parts:

$$\sum_{j=3}^{d} a_j \phi_j(x, y, z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0) \tag{4.1}$$

where P_j, Q_j are homogeneous of degree j. Then from the Theorem 2.1 we get

$$P_s Q_t = \prod_{\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2} p_\alpha(x, y, z).$$

In particular this implies that P_s and Q_t are relatively prime as the product is made of distinct irreducible factors.

The homogeneous terms of degree less than $d-3$ and greater than $2^{2k-1} - 2^{k-1}$ are 0, by the assumed bound on the degree of g. Equating terms of degree $s+t-1$ in the equation (4.1) gives $P_s Q_{t-1} + P_{s-1} Q_t = 0$. Hence P_s divides $P_{s-1} Q_t$ which implies P_s divides P_{s-1} because $\gcd(P_s, Q_t) = 1$, and we conclude $P_{s-1} = 0$ as $\deg P_{s-1} < \deg P_s$. Then we also get $Q_{t-1} = 0$. Similarly, $P_{s-2} = 0 = Q_{t-2}$, $P_{s-3} = 0 = Q_{t-3}$, and so on until we get the equation

$$P_s Q_0 + P_{s-t} Q_t = 0$$

since we suppose that $s \geq t$. This equation implies P_s divides $P_{s-t} Q_t$, which implies P_s divides P_{s-t}, which implies $P_{s-t} = 0$. Since $P_s \neq 0$ we must have $Q_0 = 0$.

We now have shown that $Q = Q_t$ is homogeneous. In particular, this means that $\phi_j(x, y, z)$ is divisible by $p_\alpha(x, y, z)$ for some $\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2$ and for all j such that $a_j \neq 0$. We are done if there exists such a j with $\phi_j(x, y, z)$ irreducible. Since $\phi_j(x, y, z)$ is defined over $\mathbb{F}_2$ it implies that $p_\alpha(x, y, z)$ also, which is a contradiction with the fact that α is not in $\mathbb{F}_2$.

□

REMARK 4.1. As in Theorem 3.5, the above theorem and the next corollary are true with the weaker hypothesis that there exists a nonzero coefficient a_j such that ϕ_j is prime to ϕ_d. We give in Section 5 some criterion about $j < d$ satisfying $\gcd(\phi_j, \phi_d) = 1$.

COROLLARY 4.1. *Suppose $f(x) = x^d + g(x)$ where g is a polynomial in $\mathbb{F}_q[x]$ such that $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose*

moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x,y,z)$ is absolutely irreducible. Then the polynomial f is not APN on infinitely many extensions of $\mathbb{F}_q$.

REMARK 4.2. It is well possible that, for a polynomial f as in Corollary 4.1, there is no extension of $\mathbb{F}_q$ where f is APN. This is an interesting but non trivial problem.

4.2. Next step: The case $\deg(g) = 2^{2k-1} - 2^{k-1} + 2$.

If we jump one degree more we need other arguments to prove irreducibility.

THEOREM 4.2. *Let $q = 2^n$. Suppose $f(x) = x^d + g(x)$ where $g(x) \in \mathbb{F}_q[x]$ and $\deg(g) = 2^{2k-1} - 2^{k-1} + 2$. Let $k \geq 3$ be odd and relatively prime to n. If $g(x)$ does not have the form $ax^{2^{2k-1}-2^{k-1}+2} + a^2x^3$ then ϕ is absolutely irreducible, while if $g(x)$ does have the form $ax^{2^{2k-1}-2^{k-1}+2} + a^2x^3$ then either ϕ is irreducible or ϕ splits into two absolutely irreducible factors which are both defined over $\mathbb{F}_q$.*

Proof: Suppose $\phi(x,y,z) = P(x,y,z)Q(x,y,z)$ with $\deg P \geq \deg Q$ and let

$$g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+2} a_j x^j.$$

Write each polynomial as a sum of homogeneous parts:

$$\sum_{j=3}^{d} a_j \phi_j(x,y,z) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0).$$

Then

$$P_s Q_t = \prod_{\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2} p_\alpha(x,y,z).$$

In particular this means P_s and Q_t are relatively prime as in the previous theorem.

Since $s \geq t$, we have $s \geq 2^{2k-1} - 2^{k-1} - 1$. Comparing each degree gives $P_{s-1} = 0 = Q_{t-1}$, $P_{s-2} = 0 = Q_{t-2}$, and so on until we get the equation of degree $s+1$

$$P_s Q_1 + P_{s-t+1} Q_t = 0$$

which implies $P_{s-t+1} = 0 = Q_1$.

If $s \neq t$ then $s \geq 2^{2k-1} - 2^{k-1}$. Note then that $a_{s+3}\phi_{s+3} = 0$. The equation of degree s is

$$P_s Q_0 + P_{s-t} Q_t = a_{s+3}\phi_{s+3} = 0.$$

This means that $P_{s-t} = 0$, so $Q_0 = 0$. We now have shown that $Q = Q_t$ is homogeneous. In particular, this means that $\phi(x,y,z)$ is divisible by $p_\alpha(x,y,z)$ for some $\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2$, which is impossible, as we will show. Indeed, since the leading coefficient of g is not 0, the polynomial $\phi_{2^{2k-1}-2^{k-1}+2}$ occurs in ϕ; as

$$\phi_{2^{2k-1}-2^{k-1}+2} = \phi^2_{2^{2k-2}-2^{k-2}+1}(x+y)(y+z)(z+x), \tag{4.2}$$

this polynomial is prime to ϕ, because if $p_\alpha(x,y,z)$ occurs in the polynomials $\phi_{2^{2k-1}-2^{k-1}+2}$, then it will occur in $\phi_{2^{2k-2}-2^{k-2}+1}$. If that is the case, the polynomial $p_\alpha(x,0,1) = (x-\alpha)^{2^k+1}$ would divide $\phi_{2^{2k-2}-2^{k-2}+1}(x,0,1)$. One has

$$\begin{aligned}&(x+y)(y+z)(z+x)\phi_{2^{2k-2}-2^{k-2}+1}(x,y,z)\\ &\quad = x^{2^{2k-2}-2^{k-2}+1} + y^{2^{2k-2}-2^{k-2}+1} + z^{2^{2k-2}-2^{k-2}+1} + (x+y+z)^{2^{2k-2}-2^{k-2}+1}\end{aligned}$$

hence

$$x(x+1)\phi_{2^{2k-2}-2^{k-2}+1}(x,0,1) = x^{2^{2k-2}-2^{k-2}+1} + 1 + (x+1)^{2^{2k-2}-2^{k-2}+1}.$$

Let $u = x - \alpha$. We have, for some polynomial R:

$$\begin{aligned}
& x(x+1)\phi_{2^{2k-2}-2^{k-2}+1}(x,0,1) \\
= \;& (u+\alpha)(u+\alpha+1)\phi_{2^{2k-2}-2^{k-2}+1}(u+\alpha,0,1) \\
= \;& (u+\alpha)^{2^{2k-2}-2^{k-2}+1} + 1 + (u+\alpha+1)^{2^{2k-2}-2^{k-2}+1} \\
= \;& \alpha^{2^{2k-2}-2^{k-2}+1} + u\alpha^{2^{2k-2}-2^{k-2}} + u^{2^{k-2}}\alpha^{2^{2k-2}-2^{k-1}+1} + 1 + \\
& \quad +(\alpha+1)^{2^{2k-2}-2^{k-2}+1} + u(\alpha+1)^{2^{2k-2}-2^{k-2}} \\
& \quad +u^{2^{k-2}}(\alpha+1)^{2^{2k-2}-2^{k-1}+1} + u^{2^{k-2}+1}R(u).
\end{aligned}$$

As $\alpha^{2^k-1} = 1$ we have $\alpha^{2^{2k-2}-2^{k-2}} = \alpha^{2^{k-2}(2^k-1)} = 1$. So

$$\begin{aligned}
& x(x+1)\phi_{2^{2k-2}-2^{k-2}+1}(x,0,1) \\
= \;& \alpha + u + u^{2^{k-2}}\alpha^{1-2^{k-2}} + 1 + (\alpha+1) + u + u^{2^{k-2}}(\alpha+1)^{1-2^{k-2}} + u^{2^{k-2}+1}R(u) \\
= \;& u^{2^{k-2}}(\alpha^{1-2^{k-2}} + (\alpha+1)^{1-2^{k-2}}) + u^{2^{k-2}+1}R(u)
\end{aligned}$$

which is a contradiction.

Suppose next that $s = t = 2^{2k-1} - 2^{k-1} - 1$ in which case the degree s equation is

$$P_sQ_0 + P_0Q_s = a_{s+3}\phi_{s+3}.$$

If $Q_0 = 0$, then

$$\phi(x,y,z) = \sum_{j=3}^{d} a_j\phi_j(x,y,z) = (P_s + P_0)Q_s$$

which implies that

$$\phi(x,y,z) = a_d\phi_d(x,y,z) + a_{2^{2k-1}-2^{k-1}+2}\phi_{2^{2k-1}-2^{k-1}+2}(x,y,z) = P_sQ_t + P_0Q_t$$

and $P_0 \neq 0$, since $g \neq 0$. So one has $\phi_{2^{2k-1}-2^{k-1}+2}$ divides $\phi_d(x,y,z)$ which is impossible by (4.2).

We may assume then that $P_0 = Q_0$. Then we have

$$\phi(x,y,z) = (P_s + P_0)(Q_s + Q_0) = P_sQ_s + P_0(P_s + Q_s) + P_0^2. \tag{4.3}$$

Note that this implies $a_j = 0$ for all j except $j = 3$ and $j = s+3$. This means

$$f(x) = x^d + a_{s+3}x^{s+3} + a_3x^3.$$

So if $f(x)$ does not have this form, this shows that ϕ is absolutely irreducible.

If on the contrary ϕ splits as $(P_s + P_0)(Q_s + Q_0)$, the factors $P_s + P_0$ and $Q_s + Q_0$ are irreducible, as can be shown by using the same argument.

Assume from now on that $f(x) = x^d + a_{s+3}x^{s+3} + a_3x^3$ and that (4.3) holds. Then $a_3 = P_0^2$, so clearly $P_0 = \sqrt{a_3}$ is defined over $\mathbb{F}_q$. We claim that P_s and Q_s are actually defined over $\mathbb{F}_2$.

We know from (2.1) that P_sQ_s is defined over $\mathbb{F}_2$.

Also $P_0(P_s + Q_s) = a_{s+3}\phi_{s+3}$, so $P_s + Q_s = (a_{s+3}/\sqrt{a_3})\phi_{s+3}$. On the one hand, $P_s + Q_s$ is defined over $\mathbb{F}_{2^k}$ by Theorem 2.1. On the other hand, since ϕ_{s+3} is defined over $\mathbb{F}_2$ we may say that $P_s + Q_s$ is defined over $\mathbb{F}_q$. Because $(k,n) = 1$ we may conclude that $P_s + Q_s$ is defined over $\mathbb{F}_2$. Note that the leading coefficient of

P_s+Q_s is 1, so $a_{s+3}^2 = a_3$. Whence if this condition is not true, then ϕ is absolutely irreducible.

Let σ denote the Galois automorphism $x \mapsto x^2$. Then $P_sQ_s = \sigma(P_sQ_s) = \sigma(P_s)\sigma(Q_s)$, and $P_s + Q_s = \sigma(P_s + Q_s) = \sigma(P_s) + \sigma(Q_s)$. This means σ either fixes both P_s and Q_s, in which case we are done, or else σ interchanges them. In the latter case, σ^2 fixes both P_s and Q_s, so they are defined over $\mathbb{F}_4$. Because they are certainly defined over $\mathbb{F}_{2^k}$ by Theorem 2.1, and k is odd, they are defined over $\mathbb{F}_{2^k} \cap \mathbb{F}_4 = \mathbb{F}_2$.

Finally, we have now shown that X either is irreducible, or splits into two absolutely irreducible factors defined over $\mathbb{F}_q$. □

REMARK 4.3. For $k = 3$, the polynomial ϕ corresponding to $f(x) = x^{57}+ax^{30}+a^2x^3$ where $a \in \mathbb{F}_q$ is irreducible. Indeed if it were not, we would have P_{27} and Q_{27} defined over $\mathbb{F}_2$, so by Theorem 2.1, $P_{27} = p_\beta(x,y,z)p_{\beta^2}(x,y,z)p_{\beta^4}(x,y,z)$ and $Q_{27} = p_{\beta^3}(x,y,z)p_{\beta^5}(x,y,z)p_{\beta^6}(x,y,z)$ for some $\beta \in \mathbb{F}_8 - \mathbb{F}_2$. So, up to inversion, we would check that $P_{27}(x,0,1) = (1+x+x^3)^9$ and $Q_{27}(x,0,1) = (1+x^2+x^3)^9$, hence $P_{27}(x,0,1)+Q_{27}(x,0,1) = (1+x+x^3)^9+(1+x^2+x^3)^9$, and one can check that this is not equal to $\phi_{30}(x,0,1)$ as it should be.

5. Binomials that are not APN infinitely often

Another class of functions which are known not to be APN on infinitely many extensions of $\mathbb{F}_q$ comes from certain binomials:

THEOREM 5.1 (Voloch[**23**]). *Let $f(x) = x^m+cx^r$, where $c \in \mathbb{F}_{2^n}^*$, $3 \le r < m$ are coprime integers, not both even, neither a power of two and such that $(m-1, r-1)$ is a power of two. Then f is not APN on infinitely many extension of $\mathbb{F}_{2^n}$.*

We note that the assumption m, r coprime could be omitted as mentioned in [**21**]. In the following we will look at binomials of Kasami degree or Gold degree, i.e. binomials of the form $f(x) = x^d + ax^{d'}$ with $d = 2^{2k} - 2^k + 1$ or $d = 2^k + 1$, $d' < d$. We will restrict to such d' which are not a power of 2 since the class of APN functions is invariant by addition of a q-affine polynomial.

5.1. Binomials of Gold degree. Let $d = 2^k + 1$ be a Gold exponent, $a \in \mathbb{F}_q^*$ and $d' < d$ an integer not a power of two. We deduce immediately from Voloch's theorem the following result:

THEOREM 5.2. *Let $k \ge 1$, $d = 2^k+1$, $a \in \mathbb{F}_q^*$ and $d' < d$ an integer not a power of two. If $f(x) = x^d + ax^{d'} \in \mathbb{F}_q[x]$, then the polynomial $\phi(x,y,z)$ is absolutely irreducible, and f is in particular not APN on infinitely many extensions of $\mathbb{F}_q$.*

5.2. Binomials of Kasami degree. Let $k \ge 3$ an integer and $d = 2^{2k}-2^k+1$ a Kasami exponent. In what follows, we will prove:

THEOREM 5.3. *Let $k \ge 3$, $d = 2^{2k} - 2^k + 1$ and $a \in \mathbb{F}_q^*$. Let $d' < d$ an integer not a power of two and not of the form $2^v(2^k\ell + 1)$ where ℓ is an integer such that $\gcd(\ell, 2^k - 1) \ne 1$. If $f(x) = x^d + ax^{d'} \in \mathbb{F}_q[x]$, then the polynomial $\phi(x,y,z)$ is absolutely irreducible, and f is in particular not APN on infinitely many extensions of $\mathbb{F}_q$.*

To prove Theorem 5.3, we will first derive the following lemma:

LEMMA 5.4. *Let $3 \leq t < d$ be an odd integer. If there is some $\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2$ such that p_α divides ϕ_t, then $t = 2^k\ell + 1$ where ℓ is an integer not coprime to $2^k - 1$.*

Proof: Suppose that there is some $\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2$ such that p_α divides ϕ_t. Then, $t - 3 \geq 2^k + 1$ and there is a polynomial $r(x, y, z)$ such that

$$(x + y)(x + z)(y + z)p_\alpha(x, y, z)r(x, y, z) = x^t + y^t + z^t + (x + y + z)^t.$$

Evaluating the above equality at $y = 0$ and $z = 1$ yields

$$x(x + 1)p_\alpha(x, 0, 1)r(x, 0, 1) = x^t + 1 + (x + 1)^t.$$

Let $u = x + \alpha$. Then

$$(u + \alpha)(u + \alpha + 1)u^{2^k+1}r(u + \alpha, 0, 1) = (u + \alpha)^t + 1 + (u + \alpha + 1)^t\,,$$

and thus

$$(u + \alpha)^t + (u + \alpha + 1)^t + 1 = 0 \mod u^{2^k+1}\,.$$

On the other hand, we know that

$$\begin{aligned} 1 + (u + \alpha)^t + (u + \alpha + 1)^t &= 1 + \sum_{i=0}^{t} \binom{t}{i} \left(\alpha^{t-i} + (\alpha + 1)^{t-i}\right) u^i \\ &= 1 + \alpha^t + (\alpha + 1)^t + (\alpha^{t-1} + (\alpha + 1)^{t-1})u \\ &\quad + \sum_{i=2}^{2^k} \binom{t}{i} \left(\alpha^{t-i} + (\alpha + 1)^{t-i}\right) u^i \mod u^{2^k+1}\,. \end{aligned}$$

Now, if $\alpha^t + (\alpha+1)^t + 1 = \alpha^{t-1} + (\alpha+1)^{t-1} = 0$, we then have $(\alpha+1)^t = \alpha^{t-1}(\alpha+1)$ and thus

$$1 = \alpha^t + (\alpha + 1)^t = \alpha^t + \alpha^{t-1}(\alpha + 1) = \alpha^{t-1}.$$

From $\alpha^{t-1} = 1$ and $\alpha^{2^k-1} = 1$ we conclude that the order of $\alpha \neq 1$ should divide $\gcd(t - 1, 2^k - 1)$, and thus $\gcd(t - 1, 2^k - 1) > 1$.

Recall that $\alpha^t + (\alpha + 1)^t + 1 = \alpha^{t-1} + (\alpha + 1)^{t-1} = 0$. For any integer j:

$$\begin{aligned} \alpha^{t-1-2^j} + (\alpha + 1)^{t-1-2^j} &= \frac{\alpha^{t-1}}{\alpha^{2^j}} + \frac{(\alpha + 1)^{t-1}}{(\alpha + 1)^{2^j}} \\ &= \frac{\alpha^{t-1}}{\alpha^{2^j}} + \frac{\alpha^{t-1}}{(\alpha + 1)^{2^j}} = \frac{\alpha^{t-1}}{\alpha^{2^j}\,(1 + \alpha^{2^j})} \neq 0\,. \end{aligned}$$

From this, we conclude that $\binom{t}{1+2^j} \equiv 0 \mod 2$ for any $j \in [1, k - 1]$, which is equivalent, by Lucas theorem's [**19**][p. 230], to say that the $(j + 1)$-th bit of t is 0 for j in the range $[1, k - 1]$ i.e. 2^k divides $t - 1$ since t is odd. In particular there is some integer ℓ such that $t - 1 = 2^k\ell$ and thus $\gcd(t - 1, 2^k - 1) = \gcd(\ell, 2^k - 1) > 1$. □

We will use the following Lemma 5.1 from [**21**] to prove that ϕ is absolutely irreducible.

LEMMA 5.5. *Let $\phi(x, y, z) \in \mathbb{F}_q[x, y, z]$ be the sum of two homogeneous polynomials, i.e. $\phi = \phi_r + \phi_d$ where ϕ_i is a homogeneous polynomial of degree i, $r < d$. Suppose that $\gcd(\phi_d, \phi_r) = 1$ and either ϕ_d or ϕ_r factors into distinct factors over $\overline{\mathbb{F}}_q$. Then ϕ is absolutely irreducible.*

Proof of Theorem 5.3: According to the definition of ϕ and from $f(x) = x^d + ax^{d'}$ we get

$$\phi(x, y, z) = \phi_d(x, y, z) + a\phi_{d'}(x, y, z)\,,$$

where ϕ_d (resp. $\phi_{d'}$) is a homogeneous polynomial of degree $d-3$ (resp. $d'-3$).

Let denote by v the 2-adic valuation of d' and t odd such that $d' = 2^v \cdot t$ where t is ≥ 3.

From Theorem 2.1 we know that ϕ_d factors over $\overline{\mathbb{F}}_q$ as $\prod_{\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2} p_\alpha(x, y, z)$. In order to prove that ϕ is absolutely irreducible, and as a consequence of Lemma 5.5, it is then sufficient to show that $\gcd(\phi_d, \phi_{d'}) = 1$. Suppose that $\gcd(\phi_d, \phi_{d'}) \neq 1$, i.e. there is an $\alpha \in \mathbb{F}_{2^k} - \mathbb{F}_2$ such that p_α divides $\phi_{d'}$. Since $d' = 2^v t$, we have

$$\phi_{d'}(x, y, z) = \phi_t^{2^v}(x, y, z) \cdot ((x + y)(x + z)(y + z))^{2^v - 1}\,,$$

and in particular p_α divides ϕ_t which is impossible by Lemma 5.4. □

References

1. Y. Aubry, G. McGuire, F. Rodier, A Few More Functions That Are Not APN Infinitely Often, Finite Fields: Theory and applications, Ninth International conference Finite Fields and Applications, McGuire et al. editors, Contemporary Math. n°518, AMS, Providence (RI), USA, 2010. Available on arXiv: n° 0909.2304.
2. T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, On almost perfect nonlinear functions over F_2^n, IEEE Trans. Inform. Theory, 52(9), pp. 4160–4170, 2006.
3. C. Bracken, E. Byrne, N. Markin, G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields and their Applications, 14 (2008), pp. 703–714.
4. L. Budaghyan, C. Carlet, P. Felke and G. Leander, An infinite class of quadratic APN functions which are not equivalent to power mappings, Cryptology ePrint Archive, 2005/359.
5. E. Byrne and G. McGuire On the Non-Existence of Quadratic APN and Crooked Functions on Finite Fields, WCC 2005.
6. A. Canteaut, Differential cryptanalysis of Feistel ciphers and differentially δ-uniform mappings, In Selected Areas on Cryptography, SAC'97, pp. 172–184, Ottawa, Canada, 1997.
7. C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography, 15(2), pp. 125–156, 1998.
8. R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr., 10(2), pp. 167–184, 1997.
9. J. F. Dillon, APN Polynomials: An update, Fq9 International conference on finite fields and their Applications, July 2009.
10. C. Ding and J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory Ser. A, 113(7), pp. 1526–1535, 2006.
11. Y. Edel, G. Kyureghyan and A. Pott, A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52, (2006), n°2, pp. 744–747.
12. E. Férard and F. Rodier, Non linéarité des fonctions booléennes données par des polynômes de degré binaire 3 définies sur $\mathbb{F}_{2^m}$ avec m pair [Nonlinearity of Boolean functions given by polynomials of binary degree 3 defined on $\mathbb{F}_{2^m}$ with m even]. Arithmetic, geometry, cryptography and coding theory 2009, pp. 41–53, Contemp. Math., 521, Amer. Math. Soc., Providence, RI, 2010.
13. E. Férard and F. Rodier, Non linéarité des fonctions booléennes données par des traces de polynômes de degré binaire 3 [Nonlinearity of Boolean functions given by traces of polynomials of binary degree 3]. Algebraic geometry and its applications, pp. 388–409, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, NJ, 2008.
14. F. Hernando and G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, Available on *arXiv:0903.2016v3* [cs.IT], 2009.
15. H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes, *Applied Algebra, Algebraic Algorithms and Error-Correcting*

Codes, Proceedings AAECC-10 (G Cohen, T. Mora and O. Moreno Eds.), pp. 180-194, Lecture Notes in Computer Science, Vol. 673, Springer-Verlag, NewYork/Berlin 1993.
16. H. Janwa, G. McGuire and R. M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2), *Applied J. of Algebra*, 178, pp. 665–676 (1995).
17. D. Jedlicka, APN monomials over $GF(2^n)$ for infinitely many n, Finite Fields Appl. 13 (2007), n°4, pp. 1006–1028.
18. E. Leducq, *Autour des codes de Reed-Muller généralisés*, PhD thesis, Université Paris 7, 2011. Available on http://www.math.jussieu.fr/∼elodieleducq/these.pdf
19. E. Lucas, Théorie des fonctions numériques simplement périodiques, *American Journal of Mathematics*, vol. 1, pp. 197-240 and pp. 289–321, 1878.
20. K. Nyberg, Differentially uniform mappings for cryptography, *Advances in cryptology—Eurocrypt '93* (Lofthus, 1993), pp. 55–64, Lecture Notes in Comput. Sci., Vol. 765, Springer, Berlin, 1994.
21. F. Rodier, Bornes sur le degré des polynômes presque parfaitement non-linéaires, in Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman editors, Contemporary Math. n°487, AMS, Providence (RI), USA, pp. 169-181, 2009. Available on *arXiv:math/0605232v3* [math.AG].
22. F. Rodier, Functions of degree 4e that are not APN Infinitely Often, Cryptography and Communications, 1–14, 2011.
23. F. Voloch, Symmetric cryptography and Algebraic curves, *Algebraic geometry and its applications, Proceedings of the first SAGA conference*, Ser. Number theory and its applications, World Sci. Publ., Hackensack, NJ, pp. 135–141, 2008.

Équipe GAATI, Université de la Polynésie Française
E-mail address: eric.ferard@upf.pf

Équipe GAATI, Université de la Polynésie Française
E-mail address: roger.oyono@upf.pf

Institut de Mathématiques de Luminy, CNRS, Université de la Méditerranée, Marseille
E-mail address: rodier@iml.univ-mrs.fr