Bounds on the degrees of APN polynomials

G. Leander[1] F. Rodier[2]

[1]Technical University of Denmark, Lyngby
[2]IML – Marseille

Outline

Outline

APN functions.

- Vectorial Boolean functions are useful in private key cryptography for designing block ciphers.

APN functions.

- Vectorial Boolean functions are useful in private key cryptography for designing block ciphers.
- Two main attacks on these ciphers are differential attacks and linear attacks.
  An important criterion on Boolean functions is a high resistance to the differential cryptanalysis.

APN functions.

- Vectorial Boolean functions are useful in private key cryptography for designing block ciphers.
- Two main attacks on these ciphers are differential attacks and linear attacks.
  An important criterion on Boolean functions is a high resistance to the differential cryptanalysis.
- Kaisa Nyberg has introduced the notion of almost perfect nonlinearity (APN) to characterize those functions which have the better resistance to differential attacks.

APN functions

Let us consider a vectorial Boolean function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$.

If we use the function f in a S-box of a cryptosystem, the efficiency of differential cryptanalysis is measured by the maximum of the cardinality of the set of elements x in $\mathbb{F}_2^m$ such that

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

where a and b are elements in $\mathbb{F}_2^m$ and $a \neq 0$.

APN functions

Let us consider a vectorial Boolean function $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$.

If we use the function f in a S-box of a cryptosystem, the efficiency of differential cryptanalysis is measured by the maximum of the cardinality of the set of elements x in $\mathbb{F}_2^m$ such that

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

where a and b are elements in $\mathbb{F}_2^m$ and $a \neq 0$.

Definition

The function f is said to be APN (almost perfect nonlinear) if for every $a \neq 0$ in $\mathbb{F}_2^m$ and $b \in \mathbb{F}_2^m$, there exists at most 2 elements x of $\mathbb{F}_2^m$ such that

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

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).
- $d = 2^{(m-1)/2} + 3$ with m odd (Welch functions).

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).
- $d = 2^{(m-1)/2} + 3$ with m odd (Welch functions).
- $d = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$, where $m \equiv 1 \pmod 4$, $d = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$, where $m \equiv 3 \pmod 4$ (Niho functions).

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).
- $d = 2^{(m-1)/2} + 3$ with m odd (Welch functions).
- $d = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$, where $m \equiv 1 \pmod 4$, $d = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$, where $m \equiv 3 \pmod 4$ (Niho functions).
- $d = 2^m - 2$, for m odd; (inverse function)

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).
- $d = 2^{(m-1)/2} + 3$ with m odd (Welch functions).
- $d = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$, where $m \equiv 1 \pmod 4$, $d = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$, where $m \equiv 3 \pmod 4$ (Niho functions).
- $d = 2^m - 2$, for m odd; (inverse function)
- $d = 2^{4m/5} + 2^{3m/5} + 2^{2m/5} + 2^{m/5} - 1$, where m is divisible by 5 (Dobbertin functions).

APN power functions

Up to now, the study of APN functions was especially devoted to the power functions.

The following functions $f(x) = x^d$ are APN on $\mathbb{F}_{2^m}$, where d is given by:

- $d = 2^h + 1$ where $\gcd(h, m) = 1$ (Gold functions).
- $d = 2^{2h} - 2^h + 1$ where $\gcd(h, m) = 1$ (Kasami functions).
- $d = 2^{(m-1)/2} + 3$ with m odd (Welch functions).
- $d = 2^{(m-1)/2} + 2^{(m-1)/4} - 1$, where $m \equiv 1 \pmod 4$, $d = 2^{(m-1)/2} + 2^{(3m-1)/4} - 1$, where $m \equiv 3 \pmod 4$ (Niho functions).
- $d = 2^m - 2$, for m odd; (inverse function)
- $d = 2^{4m/5} + 2^{3m/5} + 2^{2m/5} + 2^{m/5} - 1$, where m is divisible by 5 (Dobbertin functions).

The Gold and Kasami functions are the only known where d is independent from m and which give APN functions for an infinity of values of m.

CCZ equivalence

Carlet, Charpin and Zinoviev have defined an equivalence relation between Boolean functions.

For a function f of $\mathbb{F}_2^m$ in itself we denote by G_f the graph of the function f:

$$G_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^m\}.$$

Definition

The functions $f, f' : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ are equivalent in the sense of Carlet-Charpin-Zinoviev (CCZ equivalence) if there exist a linear permutation $L : \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2^{2m}$ such that $L(G_f) = G_{f'}$.

CCZ equivalence

Carlet, Charpin and Zinoviev have defined an equivalence relation between Boolean functions.

For a function f of $\mathbb{F}_2^m$ in itself we denote by G_f the graph of the function f:

$$G_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^m\}.$$

Definition

The functions $f, f' : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ are equivalent in the sense of Carlet-Charpin-Zinoviev (CCZ equivalence) if there exist a linear permutation $L : \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2^{2m}$ such that $L(G_f) = G_{f'}$.

Proposition

If f and f' are CCZ equivalent, then f is APN if and only if f' is.

Other APN functions

In 2005, Edel, Kyureghyan and Alexander Pott have proved that the function

$$\begin{array}{ccc} \mathbb{F}_{2^{10}} & \longrightarrow & \mathbb{F}_{2^{10}} \\ x & \longmapsto & x^3 + ux^{36} \end{array}$$

where u is a suitable element in the multiplicative group $\mathbb{F}_{2^{10}}^*$ was APN and not CCZ equivalent to power functions.

A number of people (Budaghyan, Carlet, Felke, Leander, Bracken, Byrne, Markin, McGuire, Dillon...) showed that certain quadratic polynomials were APN and not CCZ equivalent to known power functions.

Toward the classification of APN functions

- Some results toward the classification of APN functions given by polynomials have been proved
  - by Berger, Canteaut, Charpin, Laigle-Chapuy
    They prove that a large class of quadratic functions cannot be APN.

Toward the classification of APN functions

- Some results toward the classification of APN functions given by polynomials have been proved
  - by Berger, Canteaut, Charpin, Laigle-Chapuy
    They prove that a large class of quadratic functions cannot be APN.
  - by Byrne and McGuire
    Many quadratic functions, are not APN functions over an extension of the base field.

Toward the classification of APN functions

- Some results toward the classification of APN functions given by polynomials have been proved
  - by Berger, Canteaut, Charpin, Laigle-Chapuy
    They prove that a large class of quadratic functions cannot be APN.
  - by Byrne and McGuire
    Many quadratic functions, are not APN functions over an extension of the base field.
  - by Brinkman and Leander,
    APN functions with at most 5 variables are equivalent to power functions.

Toward the classification of APN functions

- Some results toward the classification of APN functions given by polynomials have been proved
  - by Berger, Canteaut, Charpin, Laigle-Chapuy
    They prove that a large class of quadratic functions cannot be APN.
  - by Byrne and McGuire
    Many quadratic functions, are not APN functions over an extension of the base field.
  - by Brinkman and Leander,
    APN functions with at most 5 variables are equivalent to power functions.
  - by Voloch
    Many binomials are not APN functions over an extension of the base field.
  - ...

Toward the classification of APN functions

- Some results toward the classification of APN functions given by polynomials have been proved
  - by Berger, Canteaut, Charpin, Laigle-Chapuy
    They prove that a large class of quadratic functions cannot be APN.
  - by Byrne and McGuire
    Many quadratic functions, are not APN functions over an extension of the base field.
  - by Brinkman and Leander,
    APN functions with at most 5 variables are equivalent to power functions.
  - by Voloch
    Many binomials are not APN functions over an extension of the base field.
  - ...
- I will give here some criteria for a Boolean function not to be almost perfect nonlinear.

Outline

Equivalent polynomials

A *q*-affine polynomial is a polynomial whose monomials are of degree 0 or a power of 2.

Proposition

The class of APN functions is invariant by addition of a q-affine polynomial.

Equivalent polynomials

A *q*-affine polynomial is a polynomial whose monomials are of degree 0 or a power of 2.

Proposition

The class of APN functions is invariant by addition of a q-affine polynomial.

We choose for f a polynomial mapping from $\mathbb{F}_{2^m}$ in itself which has no term of degree a power of 2 and with no constant term.

Characterization of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself. We can rephrase the definition of an APN function.

Proposition

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface $f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2) = 0$ has all of its rational points contained in the surface $(x_0 + x_1)(x_2 + x_1)(x_0 + x_2) = 0$.

Characterization of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself. We can rephrase the definition of an APN function.

Proposition

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface $f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2) = 0$ has all of its rational points contained in the surface $(x_0 + x_1)(x_2 + x_1)(x_0 + x_2) = 0$.

Corollary

Let us suppose that the degree d of f is not a power of 2 and $d \geq 5$.
If f is APN

Characterization of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself. We can rephrase the definition of an APN function.

Proposition

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface $f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2) = 0$ has all of its rational points contained in the surface $(x_0 + x_1)(x_2 + x_1)(x_0 + x_2) = 0$.

Corollary

Let us suppose that the degree d of f is not a power of 2 and $d \geq 5$.
If f is APN and if the affine surface X

$$\frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible,

Characterization of APN polynomials

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself. We can rephrase the definition of an APN function.

Proposition

The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface $f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2) = 0$ has all of its rational points contained in the surface $(x_0 + x_1)(x_2 + x_1)(x_0 + x_2) = 0$.

Corollary

Let us suppose that the degree d of f is not a power of 2 and $d \geq 5$.
If f is APN and if the affine surface X

$$\frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible, then the corresponding projective surface has at most $4((d-3)q + 1)$ rational points.

$$\frac{f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)}{(x_0+x_1)(x_2+x_1)(x_0+x_2)} = 0$$

Proof –

The intersection of the surface $\overline{X}$ with the plane $x_0 + x_1 = 0$ is a curve of degree $d - 3$.

This curve has at most $(d-3)q+1$ rational points from Serre's bound.

The same for the plane at infinity.

If f is APN, the surface $\overline{X}$ has no other rational points than those in the union of the plane $x_0 + x_1 = 0$, $x_2 + x_1 = 0$ and $x_0 + x_2 = 0$ or the plane at infinity.

So it has an most $4((d-3)q+1)$ rational points.

Outline

A first bound for the degree of an APN polynomial

Theorem

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree.

Suppose that the surface X with affine equation

$$\frac{f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)}{(x_0+x_1)(x_2+x_1)(x_0+x_2)}=0$$

is absolutely irreducible.

Then, if $9 \leq d < 0.45q^{1/4}+0.5$, f is not APN.

Proof –

From an improvement of Lang-Weil's bound by Ghorpade-Lachaud, we deduce

$$|\#\overline{X}(\mathbb{F}_q) - q^2 - q - 1| \leq (d-4)(d-5)q^{3/2} + 18d^4q.$$

Proof –

From an improvement of Lang-Weil's bound by Ghorpade-Lachaud, we deduce

$$|\#\overline{X}(\mathbb{F}_q) - q^2 - q - 1| \leq (d-4)(d-5)q^{3/2} + 18d^4q.$$

Hence

$$\#\overline{X}(\mathbb{F}_q) \geq q^2 + q + 1 - (d-4)(d-5)q^{3/2} - 18d^4q.$$

Therefore, if

$$q^2 + q + 1 - (d-4)(d-5)q^{3/2} - 18d^4q > 4((d-3)q+1),$$

then $\#\overline{X}(\mathbb{F}_q) > 4((d-3)q+1)$, so f is not APN.

This condition is true for

$$q^{1/2} > 13.51 - 5d + 4.773d^2$$

Irreducibility of X

Criterion for the surface X to be irreducible.

Proposition

Let f be a polynomial of $\mathbb{F}_q$ to itself, d its degree. Let us suppose that d is not a power of 2 and that the curve X_∞ with homogeneous equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible.

Then the surface X of affine equation

$$\frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is absolutely irreducible.

Proof – The curve X_∞ with homogeneous equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is the intersection of the surface X of affine equation

$$\frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

with the plane at infinity.
Since the curve X_∞ is absolutely irreducible it is the same for the surface X.

Irreducibility of X_∞

Janwa, McGuire and Wilson have studied the curve X_∞ and have deduced a certain number of cases where it is absolutely irreducible.

Proposition

The curve X_∞ is absolutely irreducible for

$$d \equiv 3 \pmod 4$$

or

$$d \equiv 5 \pmod 8 \quad \textit{and} \quad d > 13.$$

A second bound

We can improve the bound for some cases.

Theorem

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree.
Let us suppose that d is not a power of 2 and that the surface X

$$\frac{f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)}{(x_0+x_1)(x_2+x_1)(x_0+x_2)}=0$$

has only a finite number of singular points.
Then if $10 \leq d < q^{1/4}+4$, f is not APN.

Proof

From an improvement of a theorem of Deligne on Weil's conjectures by Ghorpade-Lachaud, we deduce that

$$|\#\overline{X}(\mathbb{F}_q) - q^2 - q - 1| \leq (d-4)(d-5)q^{3/2} + (d^3 - 13d^2 + 57d - 82)q$$

If

$$q > d^4 - 16d^3 + 94d^2 - 228d + 175 \quad \text{and} \quad d \geq 6$$

then $\#X(\mathbb{F}_q) > 4((d-3)q + 1)$
and so f is not APN.

Singular points on X

Proposition

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree. Let us suppose that the curve X_∞ of equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is smooth.
Then the surface X has only a finite number of singular points.

Singular points on X

Proposition

Let f be a polynomial mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$, d its degree. Let us suppose that the curve X_∞ of equation

$$\frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0$$

is smooth.
Then the surface X has only a finite number of singular points.

Proof –

The curve X_∞ is the intersection of the surface X with the plane at infinity.
As X_∞ is nonsingular, one can deduce that X has only a finite number of singular points.

Nonsingularity of X_∞

Janwa and Wilson have studied the curve X_∞ and have deduced a certain number of cases where it is nonsingular.

Proposition

The curve X_∞ is nonsingular for the values of $d = 2l + 1$ where

- *l is an odd integer such as there exists an integer r with $2^r \equiv -1 \pmod{l}$.*
- *l is a prime number larger than 17 such as the order of 2 modulo l is $(l-1)/2$.*

In particular the first condition is satisfied if l is a prime number congruent to ± 3 modulo 8.

No third bound

One could ask the question whether the surface $\overline{X}$ may be smooth. It would improve the bounds on the degree of APN functions.

No third bound

One could ask the question whether the surface $\overline{X}$ may be smooth. It would improve the bounds on the degree of APN functions. That is not the case.

No third bound

One could ask the question whether the surface $\overline{X}$ may be smooth. It would improve the bounds on the degree of APN functions. That is not the case.
Let

$$\phi(x_0, x_1, x_2) = \frac{f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)}$$

the affine equation of the surface X.
The singular points of this surface X are on the surfaces with equation $\phi'_{x_i}(x_0, x_1, x_2) = 0$.

Lemma

The polynomial $x_1 + x_2$ divides $\phi'_{x_0}(x_0, x_1, x_2)$.

Therefore the intersection of the line $x_0 = x_1 = x_2$ with the surface $\overline{X}$ is made of singular points of X.

Outline

Binomials I

Improvement of a Proposition by Voloch

Proposition

Let $f(x) = x^d + ax^r$,
where
$a \in \mathbb{F}_q^*$,
$r < d$ *are integers, not both even, and not a power of 2*
and such that $(d-1, r-1)$ *be a power of 2.*

Then, if $9 \leq d < 0,45q^{1/4} + 0,5$, f *is not APN.*

Binomials I

Improvement of a Proposition by Voloch

Proposition

Let $f(x) = x^d + ax^r$,
where
$a \in \mathbb{F}_q^*$,
$r < d$ *are integers, not both even, and not a power of 2*
and such that $(d-1, r-1)$ *be a power of 2.*

Then, if $9 \leq d < 0,45q^{1/4} + 0,5$, f *is not APN.*

Example

For instance the binomial $x^{36} + ax^3$ with $a \neq 0$ can be APN only if $m \leq 24$.
(It is APN for $m = 10$ and certain a).

Binomials II

Extension of a lemma by Byrne and McGuire

Proposition

Let $f(x) = x^d + ax^r$, *where* $a \in \mathbb{F}_q^*$
$3 \leq r < d$, *are two integers.*

Let ϕ_s *be the polynomial* $\dfrac{x_0^s + x_1^s + x_2^s + (x_0 + x_1 + x_2)^s}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)}$

Let us suppose that $(\phi_d, \phi_r) = 1$ *and that*

- *either* ϕ_d *decomposes in distinct factors on* $\overline{\mathbb{F}_2}$ *and* $r \geq 5$;
- *or* ϕ_r *decomposes in distinct factors on* $\overline{\mathbb{F}_2}$.

Then, if $9 \leq d < 0.45q^{1/4} + 0.5$, f *is not APN.*

Binomials II

Extension of a lemma by Byrne and McGuire

Proposition

Let $f(x) = x^d + ax^r$, *where* $a \in \mathbb{F}_q^*$
$3 \leq r < d$, *are two integers.*

Let ϕ_s *be the polynomial* $\dfrac{x_0^s + x_1^s + x_2^s + (x_0 + x_1 + x_2)^s}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)}$

Let us suppose that $(\phi_d, \phi_r) = 1$ *and that*

- *either* ϕ_d *decomposes in distinct factors on* $\overline{\mathbb{F}_2}$ *and* $r \geq 5$;
- *or* ϕ_r *decomposes in distinct factors on* $\overline{\mathbb{F}_2}$.

Then, if $9 \leq d < 0.45q^{1/4} + 0.5$, f *is not APN.*

Example

This proposition shows that the polynomial $x^{13} + ax^7$ with $a \neq 0$ can be APN only if $m \leq 19$, because the polynomial ϕ_7 is irreducible and does not divide ϕ_{13}.

Polynomials of degree 3 or 5

It is enough to look at the polynomials of the form $a_5x^5 + a_3x^3$.

These polynomials are linear combination of two monomials of the form x^{2^i+1}.

They cannot be APN except if a_3 or a_5 is zero.
In this case, they are Gold functions.

Polynomials de degree 6

Proposition

Let $f(x) = x^6 + a_5x^5 + a_3x^3$ be a polynomial of degree 6.

The polynomial f is APN if and only if $a_3 = a_5 = 0$.

Then it is equivalent to a Gold function.

Polynomials de degree 6

Proposition

Let $f(x) = x^6 + a_5x^5 + a_3x^3$ be a polynomial of degree 6.

The polynomial f is APN if and only if $a_3 = a_5 = 0$.

Then it is equivalent to a Gold function.

Proof
The surface X is absolutely irreducible, except if $a_3 = a_5^3$.
The surface X has only isolated singularities if $0 \neq a_3 \neq a_5^3$.
One deduce that f can be APN only if $m \leq 4$.

Polynomials of degree 7

Proposition

Let f be a polynomial of degree 7.

For $m \geq 3$, the polynomial f can be APN only if it is CCZ-equivalent to the polynomial x^7 on $\mathbb{F}_{32}$.

Then it is equivalent to a Welsh function.

Polynomials of degree 7

Proposition

Let f be a polynomial of degree 7.

For $m \geq 3$, the polynomial f can be APN only if it is CCZ-equivalent to the polynomial x^7 on $\mathbb{F}_{32}$.

Then it is equivalent to a Welsh function.

Proof –

The surface $\overline{X}$ has only isolated singularities.
One deduce that f can be APN only if $m \leq 6$.
One deduce the proposition from the work of M. Brinkman and G. Leander and with an exhaustive research for $m = 6$.

Polynomials of degree 9

Proposition

Let f be a polynomial of degree 9.

The polynomial f cannot be APN for an infinity of m except if it is equivalent to the alertpolynomial x^9.
Then it is CCZ-equivalent to a Gold function.

Otherwise the polynomial f can be APN only for $m = 6$.
Then it is equal to a Dillon's function $f = x^9 + a_6x^6 + a_3x^3$ or to a CCZ-equivalent function.

Proof –
One can limit our study to a few families of polynomials.

The function x^9 is a Gold function.

The only other case where the surface X is reducible is when $f(x) = x^9 + a_6x^6 + a_3x^3$ with $a_3 = a_6^2 \neq 0$.
Then X is a union of two degree 3 surfaces.

For most of the cases, the surface $\overline{X}$ has only a finite number of singularities. The function f can only be APN if $m \leq 13$.

An exhaustive search proves the proposition for the remaining cases.
The only APN function we find is a function
$f = x^9 + a_6x^6 + a_3x^3$ for $m = 6$ already obtained by Dillon.

Numerical examples

When the surface X is irreducible, the function f can be APN only if $m \leq m_{max}$ where m_{max} is given by the following table.

$d \leq$	7	9	10	12	15	17	21	23	29	36	41	49
m_{max}	15	16	17	18	19	20	21	22	23	24	25	26

Numerical examples

When the surface X is irreducible, the function f can be APN only if $m \leq m_{max}$ where m_{max} is given by the following table.

$d \leq$	7	9	10	12	15	17	21	23	29	36	41	49
m_{max}	15	16	17	18	19	20	21	22	23	24	25	26

When moreover the surface X is has only a finite number of singularities, the function f can be APN only if $m \leq m_{max}$ where m_{max} is given by the following table.

$d \leq$	7	9	10	12	13	15	17	20	23	26	30	36
m_{max}	6	9	10	11	12	13	14	15	16	17	18	19

Outline

Mappings $x^{-1} + g(x)$

Proposition

Let g be a polynomial mapping from $\mathbb{F}_q$ in itself, d its degree. Then, if $5 \leq d < 0.45q^{1/4} - 4.5$, $f = x^{q-2} + g$ is not APN.

Mappings $x^{-1} + g(x)$

Proposition

Let g be a polynomial mapping from $\mathbb{F}_q$ in itself, d its degree. Then, if $5 \leq d < 0.45q^{1/4} - 4.5$, $f = x^{q-2} + g$ is not APN.

Proof

The surface X is of degree $q - 5$.
We study instead the surface X'

$$\frac{g(x_0) + g(x_1) + g(x_2) + g(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} x_0 x_1 x_2 (x_0 + x_1 + x_2) = 1$$

The surface X' is irreducible.
If f is APN then $X'(\mathbb{F}_q) \leq 8dq + 4$.

Mappings $x^{-1} + g(x)$

Proposition

Let g be a polynomial mapping from $\mathbb{F}_q$ in itself, d its degree. Then, if $5 \leq d < 0.45q^{1/4} - 4.5$, $f = x^{q-2} + g$ is not APN.

Proof

The surface X is of degree $q - 5$.
We study instead the surface X'

$$\frac{g(x_0) + g(x_1) + g(x_2) + g(x_0 + x_1 + x_2)}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} x_0 x_1 x_2 (x_0 + x_1 + x_2) = 1$$

The surface X' is irreducible.
If f is APN then $X'(\mathbb{F}_q) \leq 8dq + 4$.

Example

The functions $x^{q-2} + ax^d$ for $a \neq 0$, exponents d up to 29 and not a power of 2 are not APN.

Outline

Criteria for a Boolean functions

We have shown that many polynomials cannot be APN

if their degrees are too large with respect to the number of variables

We have done that by using bounds of the Weil type on some surfaces on finite fields.

Some perspectives

- Let δ be the maximum of the cardinality of the set of elements x in $\mathbb{F}_2^m$ such that

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

  where a and b are elements in $\mathbb{F}_2^m$ and $a \neq 0$.

  To study Boolean functions with $\delta = 4,\ 6 \ldots$
- To study polynomial functions of degree 10, ...
- To study polynomial functions of low degrees plus a quadratic function.
- Can one get better bounds on m and d by studying the special form of the surface X (for instance the symmetry of the equation in x_0, x_1, x_2)?

THANK YOU