Some More Functions That Are Not APN Infinitely Often

Yves Aubry[1] Gary McGuire[2] François Rodier[3]

[1]Imath – Toulon
[2]Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography
[3]IML – Marseille

Outline

Outline

Boolean functions.

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

Boolean 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.

Boolean 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 in 1993 the notion of almost perfect nonlinearity (APN) to characterize those functions which have the best resistance to differential attacks.

APN functions

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

APN functions

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

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).

- and other functions with exponent d depending on m

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).

- and other functions with exponent d depending on m

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).

- and other functions with exponent d depending on m

F. Hernando and G. McGuire proved recently the following :

Theorem

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

APN function not equivalent to a power function

First example:

APN function not equivalent to a power function

First example:

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

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

where ω is a primitive cube root of unity in $\mathbb{F}_{2^{10}}^*$ was APN and not CCZ equivalent to a power function.

APN function not equivalent to a power function

First example:

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

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

where ω is a primitive cube root of unity in $\mathbb{F}_{2^{10}}^*$ was APN and not CCZ equivalent to a power function.

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

APN function not equivalent to a power function

First example:

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

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

where ω is a primitive cube root of unity in $\mathbb{F}^*_{2^{10}}$ was APN and not CCZ equivalent to a power function.

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

Dillon found an APN polynomial on $\mathbb{F}_{2^6}$ which was a permutation.
First APN permutation on an even number of variables.
Not CCZ equivalent to a power function.

New Conjecture

G. McGuire proposed the following conjecture.

Conjecture

The Gold and Kasami functions (up to equivalence) are the only APN functions which are APN on infinitely many extensions of their field of definition.

New Conjecture

G. McGuire proposed the following conjecture.

Conjecture

The Gold and Kasami functions (up to equivalence) are the only APN functions which are APN on infinitely many extensions of their field of definition.

We will give some results toward this conjecture.

Outline

A bound for the degree of an APN polynomial

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself.

- which has no term of degree a power of 2
- and with no constant term.

A bound for the degree of an APN polynomial

Let $q = 2^m$ and let f be a polynomial mapping of $\mathbb{F}_q$ in itself.

- which has no term of degree a power of 2
- and with no constant term.

We have the following result:

Theorem (FR)

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

$$\frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(z + y)(x + z)} = 0$$

is absolutely irreducible.

Then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

Skech of proof

- We can rephrase the definition of an APN function.

Skech of proof

- We can rephrase the definition of an APN function.

  The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface

  $$f(x) + f(y) + f(z) + f(x + y + z) = 0$$

  has all of its rational points contained in the surface

  $$(x + y)(z + y)(x + z) = 0.$$

Skech of proof

- We can rephrase the definition of an APN function.

  The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface

  $$f(x) + f(y) + f(z) + f(x + y + z) = 0$$

  has all of its rational points contained in the surface

  $$(x + y)(z + y)(x + z) = 0.$$

- The surface X has a number of rational points bounded

Skech of proof

- We can rephrase the definition of an APN function.

  The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface

  $$f(x) + f(y) + f(z) + f(x + y + z) = 0$$

  has all of its rational points contained in the surface

  $$(x + y)(z + y)(x + z) = 0.$$

- The surface X has a number of rational points bounded by Lang-Weil bound.

Skech of proof

- We can rephrase the definition of an APN function.

  The function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is APN if and only if the surface

  $$f(x) + f(y) + f(z) + f(x + y + z) = 0$$

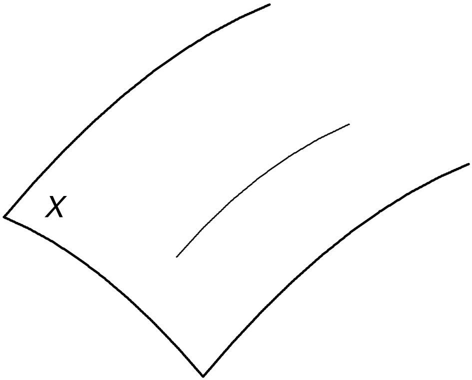
  has all of its rational points contained in the surface

  $$(x + y)(z + y)(x + z) = 0.$$

- The surface X has a number of rational points bounded by Lang-Weil bound.
- If f is APN and q too big, then the surface X has too many rational points to be contained in the surface $(x + y)(z + y)(x + z) = 0$.

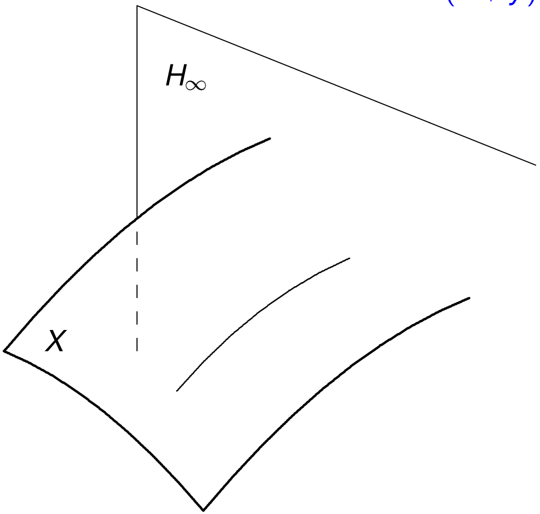
Irreducibility of X

$$X : \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$



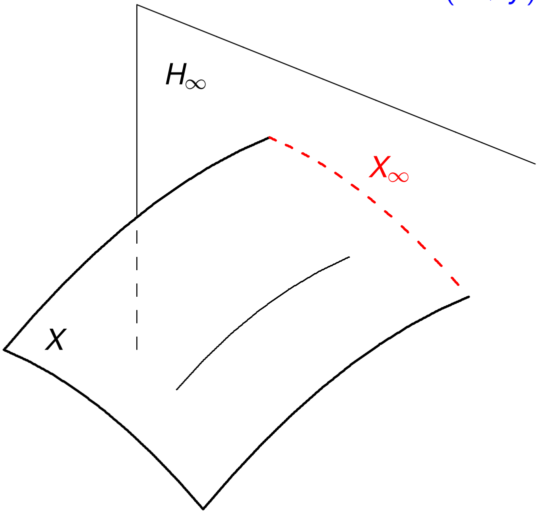
Irreducibility of X

$$X : \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$



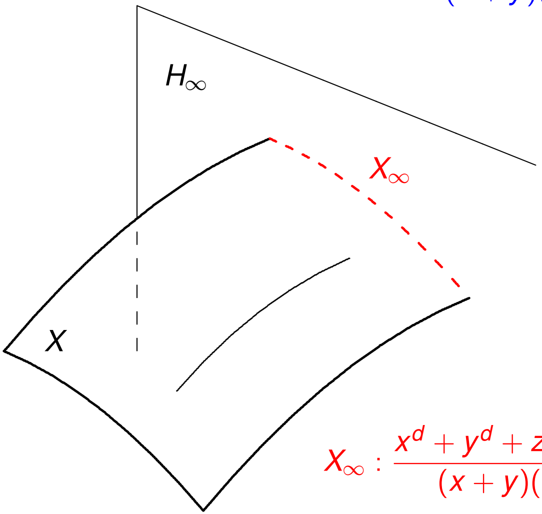
Irreducibility of X

$$X : \frac{f(x) + f(y) + f(z) + f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$



Irreducibility of X

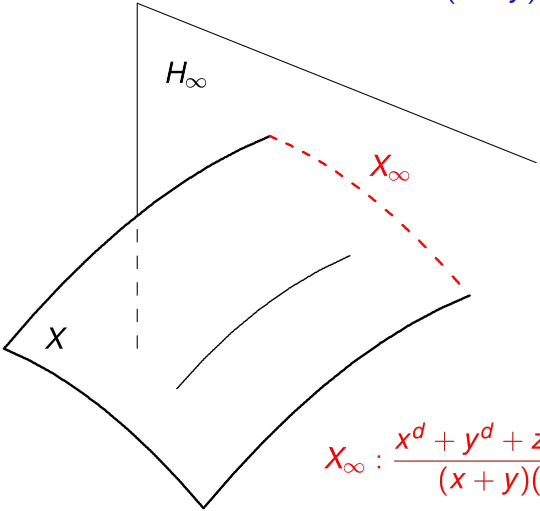
$$X : \frac{f(x) + f(y) + f(z) + f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$



$$X_\infty : \frac{x^d + y^d + z^d + (x+y+z)^d}{(x+y)(z+y)(x+z)} = 0$$

Irreducibility of X

$$X : \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(z+y)(x+z)} = 0$$



$$X_\infty : \frac{x^d+y^d+z^d+(x+y+z)^d}{(x+y)(z+y)(x+z)} = 0$$

Proposition

X_∞ *absolutely irreducible* $\Rightarrow X$ *absolutely irreducible*

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

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

Outline

The conjecture on APN functions

Irreducibility of X_∞

Let $\mathbb{F}_q$ the field of definition of f.
If the surface X is absolutely irreducible,
then the polynomial function f can be APN only for a finite number of extensions.

The conjecture on APN functions

Irreducibility of X_∞

Let $\mathbb{F}_q$ the field of definition of f.
If the surface X has an irreducible component defined over $\mathbb{F}_q$ then the polynomial function f can be APN only for a finite number of extensions.

Let $\mathbb{F}_q$ the field of definition of f.
If the surface X has an irreducible component defined over $\mathbb{F}_q$ then the polynomial function f can be APN only for a finite number of extensions.

Proposition

If X_∞ has an irreducible component defined over $\mathbb{F}_2$ then X has an irreducible component defined over $\mathbb{F}_q$

The conjecture on APN functions

Irreducibility of X_∞

Let $\mathbb{F}_q$ the field of definition of f.
If the surface X has an irreducible component defined over $\mathbb{F}_q$ then the polynomial function f can be APN only for a finite number of extensions.

Proposition

If X_∞ has an irreducible component defined over $\mathbb{F}_2$ then X has an irreducible component defined over $\mathbb{F}_q$

Proposition (Hernando, McGuire)

The curve X_∞ of degree d has an irreducible component defined over $\mathbb{F}_2$ for d odd, not equal to Gold or Kasami exponent.

The conjecture on APN functions

Polynomials of odd degree d

Theorem (Aubry, McGuire, Rodier)

If the degree of the polynomial function f is d with d odd, not equal to Gold or Kasami exponent, then f is not APN over $\mathbb{F}_{q^n}$ for all n sufficiently large.

The conjecture on APN functions

Polynomials of degree $d = 2e$

Theorem (Aubry, McGuire, Rodier)

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.

The conjecture on APN functions

Polynomials of degree $d = 2e$

Theorem (Aubry, McGuire, Rodier)

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.

Let

$$\phi_r = \frac{x^r + y^r + z^r + (x+y+z)^r}{(x+y)(z+y)(x+z)}.$$

The equation of X_∞ is

$$\phi_{2e}(x,y,z) = \phi_e^2(x,y,z)(x+y)(z+y)(x+z) = 0$$

The component of X_∞ which contains the line $x + y = 0$ in the plane at infinity is defined over $\mathbb{F}_2$.
It corresponds to a component of X defined over $\mathbb{F}_q$.

The conjecture on APN functions

Polynomials of degree $d = 4e$

Theorem (FR)

If the degree of the polynomial function f is even such that $\deg(f) = 4e$ *with*

- $e \equiv 3 \pmod 4$,
- $e \not\equiv 1 \pmod 7$,
- *and* $e \geq 7$.

then f is not APN over $\mathbb{F}_{q^n}$ *for n large.*

The conjecture on APN functions

Polynomials of degree $d = 4e$

Theorem (FR)

If the degree of the polynomial function f is even such that $\deg(f) = 4e$ with

- $e \equiv 3 \pmod 4$,
- $e \not\equiv 1 \pmod 7$,
- *and* $e \geq 7$.

then f is not APN over $\mathbb{F}_{q^n}$ for n large.

This case is far more intricate than the previous cases, because there are some polynomials which are CCZ equivalent to monomials for $e = 3$.

Sketch of proof. We have in this case:

$$\phi_d(x,y,z) = \phi_e(x,y,z)^4((x+y)(x+z)(y+z))^3$$

Sketch of proof. We have in this case:

$$\phi_d(x, y, z) = \phi_e(x, y, z)^4((x + y)(x + z)(y + z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x + y = 0$ in H_∞.

Sketch of proof. We have in this case:

$$\phi_d(x, y, z) = \phi_e(x, y, z)^4((x + y)(x + z)(y + z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x + y = 0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,

Sketch of proof. We have in this case:

$$\phi_d(x,y,z) = \phi_e(x,y,z)^4((x+y)(x+z)(y+z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x+y=0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

Sketch of proof. We have in this case:

$$\phi_d(x,y,z) = \phi_e(x,y,z)^4((x+y)(x+z)(y+z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x+y=0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

one is reduced to the case where

Sketch of proof. We have in this case:

$$\phi_d(x,y,z) = \phi_e(x,y,z)^4((x+y)(x+z)(y+z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x+y=0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

one is reduced to the case where

- there are three components X_0, X_1 and X_2 of ϕ, of the form $(x+y)(x+z)(y+z)+P$

Sketch of proof. We have in this case:

$$\phi_d(x,y,z) = \phi_e(x,y,z)^4((x+y)(x+z)(y+z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x+y=0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

one is reduced to the case where

- there are three components X_0, X_1 and X_2 of ϕ, of the form $(x+y)(x+z)(y+z)+P$ where P is a polynomial of the form

  $$P(x,y,z) = c_1(x^2+y^2+z^2) + c_2(xy+xz+zy) + b(x+y+z) + d$$

Sketch of proof. We have in this case:

$$\phi_d(x,y,z) = \phi_e(x,y,z)^4((x+y)(x+z)(y+z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x+y=0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

one is reduced to the case where

- there are three components X_0, X_1 and X_2 of ϕ, of the form $(x+y)(x+z)(y+z)+P$ where P is a polynomial of the form

$$P(x,y,z) = c_1(x^2+y^2+z^2) + c_2(xy+xz+zy) + b(x+y+z) + d$$

Investigating these polynomials, one proves that

- they may divide ϕ only if $c_1 = c_2$, $b = 0$, $d = c_1^3$
- in this case there is an irreducible subcomponent defined over $\mathbb{F}_q$

Sketch of proof. We have in this case:

$$\phi_d(x, y, z) = \phi_e(x, y, z)^4((x + y)(x + z)(y + z))^3$$

Let X_0 a reduced absolutely irreducible component of X which contains the line $x + y = 0$ in H_∞.

- By the symmetry of the 3 variables x, y and z,
- and the action of the Galois group of the field of definition of X_0 over $\mathbb{F}_q$

one is reduced to the case where

- there are three components X_0, X_1 and X_2 of ϕ, of the form $(x + y)(x + z)(y + z) + P$ where P is a polynomial of the form

  $$P(x, y, z) = c_1(x^2 + y^2 + z^2) + c_2(xy + xz + zy) + b(x + y + z) + d$$

Investigating these polynomials, one proves that

- they may divide ϕ only if $c_1 = c_2$, $b = 0$, $d = c_1^3$
- in this case there is an irreducible subcomponent defined over $\mathbb{F}_q$ among the components which contain the curves $\phi_e(x, y, z)^4$.

The conjecture on APN functions

Polynomials of degree $d = 4 \times 3$

Theorem (FR)

If the degree of the polynomial f is 12, then

- *either f is not APN over $\mathbb{F}_{q^n}$ for n large*
- *or f is CCZ equivalent to the Gold function x^3.*

The conjecture on APN functions

Polynomials of degree $d = 4 \times 3$

Theorem (FR)

If the degree of the polynomial f is 12, then

- *either f is not APN over $\mathbb{F}_{q^n}$ for n large*
- *or f is CCZ equivalent to the Gold function x^3.*

Let $d \in \mathbb{F}_{q^3}$ such that $d + d^q + d^{q^2} = 0$. The polynomials CCZ equivalent to the Gold function x^3 are the polynomial functions

$$f(x) = L(x^3) \quad \text{or} \quad f(x) = L(x)^3$$

with

$$L(x) = x^4 + (d^{1+q} + d^{1+q^2} + d^{q+q^2})x^2 + d^{1+q+q^2}x$$

and the polynomials composed with f and an affine permutation.

The conjecture on APN functions

Gold degree

Theorem (Aubry, McGuire, Rodier)

Suppose $f(x) = x^d + g(x)$ *where*
the degree of f *is* $d = 2^k + 1$ *and* $\deg(g) \leq 2^{k-1} + 1$.
Suppose moreover that there exists a nonzero coefficient of x^r *in* g *such that*

$$\frac{x^r + y^r + z^r + (x + y + z)^r}{(x + y)(z + y)(x + z)}$$

is irreducible.
Then X *is absolutely irreducible.*

So f *is not APN over* $\mathbb{F}_{q^n}$ *for* n *large.*

The conjecture on APN functions

Kasami degree

Theorem

Suppose $f(x) = x^d + g(x)$ *where*
the degree of f is $d = 2^{2k} - 2^k + 1$ *and* $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$.
Suppose moreover that there exists a nonzero coefficient of x^r *in g such that*

$$\frac{x^r + y^r + z^r + (x+y+z)^r}{(x+y)(z+y)(x+z)}$$

is irreducible.
Then X is absolutely irreducible.

So f is not APN over $\mathbb{F}_{q^n}$ *for n large.*

Outline

Conclusion

Criteria for Boolean functions

We have shown that many polynomials cannot be APN

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

It is a consequence of Lang-Weil bound on some surfaces on finite fields.

To prove the conjecture on APN functions we have

- to prove the bound for several classes of degrees not Gold or Kasami;
  I mean $d = 2^i(2^i\ell + 1)$ with $\ell \neq 1$ and $\ell \neq 2^i - 1$ and $i \geq 2$.

Conclusion

The conjecture on APN functions

To prove the conjecture on APN functions we have

- to prove the bound for several classes of degrees not Gold or Kasami;
  I mean $d = 2^i(2^i\ell + 1)$ with $\ell \neq 1$ and $\ell \neq 2^i - 1$ and $i \geq 2$.
- to study polynomials of Gold or Kasami degree.

THANK YOU