S-Boxes, APN Functions, Part 2

Gary McGuire

School of Mathematical Sciences
University College Dublin
Ireland
and
Claude Shannon Institute
www.shannoninstitute.ie

SORIA July 2010

Sketch of talks:

1. Talk 1: S-Boxes, Differential Attack, APN Functions, Coding Theory, Equivalence
2. Talk 3: Linear Attack, Fourier Spectrum, Nonlinearity
3. Talk 4: Nonlinearity, Algebraic Curves.

Talk 2

1. Known APNs, PNs
2. Coding Theory
3. Equivalence
4. Linearity

Recall Definitions

Definition (Perfect Nonlinear function)

Let A, B be finite abelian groups, written additively, of the same cardinality. We say $f : A \to B$ is a perfect nonlinear (PN) function iff $f(x + a) - f(x) = b$ has at most one solution for all $a \in A$, $a \neq 0$, and all $b \in B$.

Definition (Almost Perfect Nonlinear function)

Let A, B be finite abelian groups, written additively, of the same cardinality. We say $f : A \to B$ is an almost perfect nonlinear (APN) function iff $f(x + a) - f(x) = b$ has at most two solutions for all $a \in A$, $a \neq 0$ and all $b \in B$.

Recall from last time

We saw some examples, x^{2^k+1} (Gold functions) and x^{p^k+1} (Dembowski-Ostrom)

Think of an S-Box as a function $f : (\mathbb{F}_2)^n \longrightarrow (\mathbb{F}_2)^n$.
We can take $GF(2^n)$ for $(\mathbb{F}_2)^n$ if we like.
For S-Boxes we would like a function that is

1. Bijective
2. APN.

In particular, for real-world applications (cryptosystems, hash functions) $n = 8$ is very interesting, we would like a function on $GF(2^8)$ that is bijective and APN.
NO EXAMPLES ON $GF(2^8)$ ARE KNOWN!!
This is a big open problem.

There are two more things we require from this function - I will explain soon.

Questions: Existence and Classification

Existence: Are there other APN functions (besides x^{2^k+1})?
Not many are known, but a lot has been done in the last few years.

Classification of all APN functions up to equivalence seems a very hard problem.

Non-monomial APN functions have been studied since 2005.

Monomial APN Functions

List of all known d such that x^d is an APN function on $L = \mathbb{F}_{2^n}$

$2^k + 1$ (Gold numbers) $(k, n) = 1$, c. 1968
$4^k - 2^k + 1$ (Kasami-Welch numbers) $(k, n) = 1$, c. 1970

$2^n - 2$ (Inverse) n odd Exercise - now!
$2^{(n-1)/2} + 3$ (Welch) n odd, 1998
$4^t + 2^t - 1$ (Niho) $4t \equiv 3 \pmod{n}$, 2000
$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$ (Dobbertin) $n = 5t$, 2000

The Welch and Niho cases were proved by Dobbertin, Canteaut, Charpin, Hollmann, Xiang.
This list is conjectured to be the complete list of monomial APN functions. (up to equivalence)

Note: It has not been proved that these are pairwise inequivalent. (There are some results, and it is true for small n by computer.)

PN Functions

If f is a quadratic (Dembowski-Ostrom) PN function, the operation $x * y = f(x + y) - f(x) - f(y)$ defines a multiplication that makes the finite field into a semifield.
These give rise to finite projective planes.
Not many examples are known:
x^2 Finite field
x^{p^t+1} Albert's twisted field
$x^{10} \pm x^6 - x^2$ Coulter-Matthews, Ding-Yuan
Dickson, Ganley, Cohen-Ganley, Pentilla-Williams, Coulter-Henderson-Kosick, Budaghyan-Helleseth.... more

$x^{(3^t+1)/2}$ is not quadratic but is PN (characteristic 3).

Exceptional Numbers

Dillon: A number d is *exceptional* if x^d is APN on infinitely many extensions of $\mathbb{F}_2$.
e.g. x^5 is APN on $\mathbb{F}_{2^n}$ if n is odd.
The sequence goes

$$3, 5, 9, 13, 17, 33, 57, 65, 129, 241, 257, 513, 993, 1025, \ldots.$$

This is sequence number A064386 in the On-Line Encyclopedia of Integer Sequences.

Conjecture: the only exceptional exponents d are Gold and Kasami-Welch numbers.

Partial Results: van Lint, Wilson, Janwa, M, Jedlicka,

Exceptional Numbers

New Result: completed proof of this conjecture.

Theorem (Hernando, McGuire)

The only exceptional exponents d are Gold and Kasami-Welch numbers.

To appear in Journal of Algebra.

Non-Monomial APN Functions

The first non-monomial APN functions were discovered in 2005 by Edel, Khureghyan, Pott:

$$x^3 + ux^{36} \in GF(2^{10})[x]$$

with restrictions on u. Another example over $GF(2^{12})$.
Other sporadic examples have been found also (Browning-Dillon et al, Budaghyan-Carlet hexanomials, Edel-Pott non-quadratic).
Cannon et al (MAGMA group), see file

Non-Monomial APN Functions

Infinite families since discovered are:
(due to Budeghyan, Leander, Carlet, Felke, Pott, McGuire, Byrne, Bracken, Markin,...)

$x^{2^i+1} + ux^{2^{k+i}+2^{k(r-1)}}$ (BCFL) (BCL)

$ux^{2^{-k}+2^{k+s}} + u^{2^k}x^{2^s+1} + vx^{2^{k+s}+2^s}$ (BBMM)

$bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^k+1}$ (BBMM)

$x^3 + \mathrm{Tr}(x^9)$ (BCL)

$u^{2^k}x^{2^{-k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{k+s}+2^s}$ (BBMM)

$u^{2^k}x^{2^{-k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^{k+s}+2^s}$ (BBMM)

All exponents are functions of n. + a few more...

Coding Theory

Let K be a finite field with $q = 2^n$ elements and primitive element α:

$$K = \{0, 1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2^n-2}\}.$$

A classic code is the binary Hamming code of length $2^n - 1$, defined by having parity check matrix

$$H = [1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2^n-2}].$$

Think of each entry as a column vector of length n, which you can write when you pick a basis of K over $\mathbb{F}_2$.
This code consists of all *binary* vectors $(c_0, c_1, \ldots, c_{2^n-2})$ such that

$$\sum_{i=0}^{2^n-2} c_i \alpha^i = 0.$$

This code is cyclic, and has minimum distance 3, dimension $2^n - 1 - n$. The dual code has dimension n.

Another well known example is the binary double-error-correcting BCH code, defined by parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^n-2)} \end{bmatrix}$$

Think of this matrix as having columns labelled by nonzero field elements, and column x has the form

$$\begin{bmatrix} x \\ x^3 \end{bmatrix}.$$

This code has dimension $2^n - 1 - 2n$ and minimum distance 5. For a function $f : K \longrightarrow K$ consider the binary code with parity check matrix having columns

$$\begin{bmatrix} x \\ f(x) \end{bmatrix}, \quad x \in K^*$$

The minimum distance of such a code can be shown to be 3 or 4 or 5.

The function f is APN if and only if the error-correcting code of length $2^n - 1$ with parity check matrix

$$\begin{bmatrix} \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{bmatrix}$$

has minimum distance 5. (Carlet-Charpin-Zinoviev)
If $f(x) = x^d$ this is a cyclic code. Otherwise a linear code.
The idea is that a codeword of weight 3 or 4 corresponds to

$$\begin{array}{ccccccccc} a & + & b & + & c & + & d & = & 0 \\ f(a) & + & f(b) & + & f(c) & + & f(d) & = & 0. \end{array}$$

nontrivially, whereas APN does not permit this.

Weight Distributions of APN Codes

Remark: The weight distribution of an APN code is not determined.

For $n = 6$, the dual code for $f(x) = x^3$ has five weights, whereas the code for

$$f(x) = x^3 + \alpha^{11}x^5 + \alpha^{13}x^9 + x^{17} + \alpha^{11}x^{33} + x^{48}$$

has seven weights.

However, the weight distribution of x^3 is very common (more on this later).

Algebraic Degree

The 2-weight of a positive integer is the number of terms in its binary expansion.

The *algebraic degree* of a polynomial function $f : K \longrightarrow K$ is the largest 2-weight in a term.
e.g. x^{2^k+1} has algebraic degree 2.
e.g. polynomials with all terms of the form $x^{2^i+2^j}$ have algebraic degree 2 (quadratic).
e.g. $x^{-1} = x^{2^n-2}$ has algebraic degree $n-1$.

High algebraic degree is a requirement for S-boxes.
(There is an attack on functions with low algebraic degree)

S-Box Criteria

For S-Boxes we now require

1. Bijective
2. APN
3. High algebraic degree

One more to come.

Equivalence

Recall that two binary codes with $k \times n$ generator matrices G_1 and G_2 are equivalent iff

$$G_2 P = M G_1$$

where M is $k \times k$ invertible, and P is an $n \times n$ permutation matrix.

Recall also that two codes are equivalent if and only if their dual codes are equivalent.

Consider a function $f : K \longrightarrow K$ and the binary code with $2n \times (2^n - 1)$ parity check matrix

$$\begin{bmatrix} \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{bmatrix}$$

We know $d(C) = 5$ iff f is APN.
Consider an equivalent code, and let's see what happens to f.

Consider an equivalent code, and let's see what happens to f.
Multiply by a $2n \times 2n$ invertible:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} \cdots & x & \cdots \\ \cdots & f(x) & \cdots \end{bmatrix}$$

$$= \begin{bmatrix} \cdots & Ax + Bf(x) & \cdots \\ \cdots & Cx + Df(x) & \cdots \end{bmatrix}$$

Suppose $f_1(x) := Ax + Bf(x)$ is bijective.
Then this matrix can be written

$$\begin{bmatrix} \cdots & y & \cdots \\ \cdots & g(y) & \cdots \end{bmatrix}$$

where $y = f_1(x)$, $f_2(x) = Cx + Df(x)$ and $g(y) = f_2(f_1^{-1}(y))$.
Note the columns are in a different order (so we need P).

We get a new function g !

What about g

Claim: If f is APN then so is g.
Proof: Code equivalence preserves minimum distance.
More generally, the differential uniformity of g is the same as f.
(Proof later)
We say g is (linear) CCZ equivalent to f.

Exercise: If f is bijective, show that f is equivalent to f^{-1}.

This shows that algebraic degree is NOT preserved by this transformation.
e.g. $f(x) = x$ has algebraic degree 1, but x^{-1} has ...

We should include 0, because f is defined on the whole field K.
(next slide)
This means we should really consider extended codes, but I explained it like this to give you the idea.
The most general case does not assume $f(0) = 0$, $g(0) = 0$, and that 0 is fixed by the linear transformation.

Equivalence

An extended APN code has parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^r-2} & 0 \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^r-2}) & 0 \end{bmatrix}$$

and has minimum distance 6.

Definition: Two APN functions are said to be (CCZ) equivalent if their corresponding extended APN codes are equivalent (as binary codes).

Note: this is not the standard definition, but is equivalent.

Notes

The $(2n+1) \times (2n+1)$ invertible matrix now looks like

$$\begin{bmatrix} 1 & 0 & 0 \\ \gamma_1 & A & B \\ \gamma_2 & C & D \end{bmatrix}$$

Affine (A) equivalence means $B = 0$, $C = 0$.
Extended affine (EA) equivalence means $B = 0$.

CCZ $\implies$ EA $\implies$ A

John Dillon (Banff 2006) gave a list of 13 pairwise inequivalent quadratic APNs on the field of order 64.
He showed CCZ inequivalence by checking if the codes were equivalent with MAGMA.

APN Permutations

The Dillon-Wolfe example of an APN bijection is very exciting.
Where did it come from ...

Theorem (Browning-Dillon-Kibler-McQuistan (2007))

The following are equivalent.

1. f *is CCZ equivalent to an APN permutation*

2. $C_f^\perp$ *is an extended double simplex code of dimension 6*

So to find an APN permutation we want to write $C_f^\perp = W_1 \oplus W_2$ where each W_i is a simplex code, in two ways.
This paper told us how to find APN permutations...
Nobody bothered looking for such functions. ☹
So far it has not been generalized (as far as I know).

The Equivalence Problem

Proving by hand the CCZ equivalence (or inequivalence) of two APN functions seems to be very difficult.
We have no good theoretical techniques.
Computing invariants (of the extended codes) such as the weight distribution, automorphism group, is not always possible.

We have been able to compute the weight distribution for all but one of the infinite families, and they are all the same!

Lots of room for further ideas here.

There is an invariant using $2^{24} \times 2^{24}$ matrices called the delta rank. The MAGMA group computed

Family	Function	Delta-Rank
Gold	x^3	7550
Gold	x^{33}	7550
Kasami-Welch	x^{993}	62550
1	$u^{16}x^{768} + ux^{33}$	7816
2	$x^3 + u^7x^{528}$	7822
5	$x^3 + x^{65} + ux^{129} + u^{64}x^{66} + u^3x^{130} + x^{192}$	7550
6	$x^3 + \mathrm{tr}(x^9)$	7846
7	$u^{16}x^{768} + ux^{33} + u^{290}x^{544}$	7900
8	$u^{16}x^{768} + ux^{33} + x^{257}$	7900
9	$u^{16}x^{768} + ux^{33} + x^{257} + u^{290}x^{544}$	7900

Thomas Feulner computed his generator matrix canonical form for families 7,8,9 and found they were different.

Equivalence Results

Conjecture (Edel)

If two quadratic APN functions are CCZ equivalent, then they are EA equivalent.

Theorem (Bracken-Byrne-M-Nebe)

True if one of the functions is a Gold function.
In other words, if a quadratic APN function is CCZ equivalent to a Gold function, then it is EA equivalent to that Gold function.

This is proved for some functions "directly" in some papers (e.g. Budaghyan Carlet Leander binomials).
Our proof uses the fact that we know the exact automorphism group of the Gold codes (Berger, and classification of finite simple groups), and any quadratic APN function has the additive group of the field in its automorphism group.

Equivalence Results

More generally

Theorem

Let h be a quadratic APN-function such that $Aut(C_h)$ is isomorphic to a subgroup of $\mathcal{G}$. Then all quadratic APN-functions that are CCZ equivalent to h are indeed EA equivalent to h.

Unfortunately, there are functions whose automorphism group is not contained in $\mathcal{G}$.

$$h_1 := x^3 + x^5 + u^{62}x^9 + u^3x^{10} + x^{18} + u^3x^{20} + u^3x^{34} + x^{40}$$

Then h_1 is APN on $GF(2^6)$ and $|Aut(C_{h_1})| = 2^6.5$, which is not a divisor of $2^6(2^6 - 1)6$. (Dillon)

Proof that CCZ Equivalence Preserves Diff. Uniformity

Let $f : L \longrightarrow L$ be a function.
Let $\mathcal{L} : L^2 \longrightarrow L^2$ be an invertible linear map.
Write $\mathcal{L} = (L_1, L_2)$ where each L_i is a linear map from L^2 to L.
Let $f_1(x) = L_1(x, f(x))$ and let $f_2(x) = L_2(x, f(x))$.
For fixed $a, b \in K$, let $\begin{pmatrix} a' \\ b' \end{pmatrix} = \mathcal{L} \begin{pmatrix} a \\ b \end{pmatrix}$.
Suppose we have a solution $(x, y) \in L^2$ to the system

$$x + y = a \quad (1)$$
$$f(x) + f(y) = b. \quad (2)$$

Then

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \mathcal{L}\begin{pmatrix} x+y \\ f(x)+f(y) \end{pmatrix} = \mathcal{L}\begin{pmatrix} x \\ f(x) \end{pmatrix} + \mathcal{L}\begin{pmatrix} y \\ f(y) \end{pmatrix} \text{ as } \mathcal{L} \text{ line}$$

$$= \begin{pmatrix} f_1(x) \\ f_2(x) \end{pmatrix} + \begin{pmatrix} f_1(y) \\ f_2(y) \end{pmatrix}$$

$$= \begin{pmatrix} f_1(x)+f_1(y) \\ f_2(x)+f_2(y) \end{pmatrix}$$

$$= \begin{pmatrix} u+v \\ g(u)+g(v) \end{pmatrix}$$

where $u = f_1(x), v = f_1(y), g = f_2 \circ f_1^{-1}$. At the last step we used the fact that f_1 is invertible.

Any such g that can be obtained from f in this fashion is CCZ equivalent to f.

Clearly, differential uniformity is preserved by CCZ equivalence.