APN Polynomials: An Update

J. F. Dillon

National Security Agency
Fort George G. Meade, MD USA

Fq9, International Conference on Finite Fields
and their Applications
University College Dublin
July 2009

Background from Banff

APN Polynomials and Related Codes

J. F. Dillon
National Security Agency
Fort George G. Meade, MD
email:jfdillon@gmail.com

Polynomials over Finite Fields
and Applications
Banff International Research Station
November 2006

What's an APN?

A map $f : V := GF(2^m) \rightarrow V$ satisfying any of the following:

- $x \mapsto f(x + a) - f(x)$ is 2-to-1 for all $a \neq 0$.

What's an APN?

A map $f : V := GF(2^m) \to V$ satisfying any of the following:

- $x \mapsto f(x+a) - f(x)$ is 2-to-1 for all $a \neq 0$.
- $\forall$ distinct a, b, c, d,

$$a + b + c + d = 0 \Rightarrow f(a) + f(b) + f(c) + f(d) \neq 0$$

i.e. f does not sum to 0 on any 2-flat.

What's an APN?

A map $f : V := GF(2^m) \to V$ satisfying any of the following:

- $x \mapsto f(x+a) - f(x)$ is 2-to-1 for all $a \neq 0$.
- $\forall$ distinct a, b, c, d,

$$a + b + c + d = 0 \Rightarrow f(a) + f(b) + f(c) + f(d) \neq 0$$

  i.e. f does not sum to 0 on any 2-flat.

- If $f(0) = 0$ (which we assume from now on) the binary code with parity check matrix

$$H_f := \begin{bmatrix} \cdots & \omega^j & \cdots \\ \cdots & f(\omega^j) & \cdots \end{bmatrix}$$

  is double-error-correcting (no fewer than 5 cols sum to 0).

What's an APN?

A map $f : V := GF(2^m) \rightarrow V$ satisfying any of the following:

- $x \mapsto f(x+a) - f(x)$ is 2-to-1 for all $a \neq 0$.
- $\forall$ distinct a, b, c, d,

  $$a + b + c + d = 0 \Rightarrow f(a) + f(b) + f(c) + f(d) \neq 0$$

  i.e. f does not sum to 0 on any 2-flat.
- If $f(0) = 0$ (which we assume from now on) the binary code with parity check matrix

  $$H_f := \begin{bmatrix} \cdots & \omega^j & \cdots \\ \cdots & f(\omega^j) & \cdots \end{bmatrix}$$

  is double-error-correcting (no fewer than 5 cols sum to 0).

Example

The BCH $f(x) = x^3$ is APN for all dimensions m.

Exceptional APNs

What's known?

monomials $f(x) := x^d$

$$\begin{aligned} & \#f(x+a)+f(x)+f(a)=b \\ = \; & \#(x+a)^d+x^d+a^d=b \\ = \; & \#(x+1)^d+x^d+1=a^{-d}b \end{aligned}$$

Exceptional x^d APN for infinitely many fields.

Gold $d = 2^k+1$, $\gcd(k,m)=1$

$$(x+1)^d+x^d+1=x^{2^k}+x \quad 2-\text{to}-1.$$

Kasami-Welch $d = 4^k-2^k+1$, $\gcd(k,m)=1$

$$(x+1)^d+x^d+1=\frac{(x+x^{2^k})^{2^k+1}}{(x+x^2)^{2^k}}=\mathrm{MCM}_{k,2^k+1}(x+x^2).$$

Conjecture (JW etal).
These are the only exceptional exponents.

ref. Janwa, Wilson, McGuire, Jedlicka, Rodier

Exceptional APNs

Theorem (Hernando and McGuire 2009)

The conjecture is true.

Exceptional APNs

Theorem (Hernando and McGuire 2009)

The conjecture is true.

We look forward to Fernando's talk to hear the details of this milestone result!

The Dual Code

We'll identify the dual code with the binary row space of the matrix $\begin{bmatrix} x \\ f(x) \end{bmatrix}$, where x ranges over all of L.

The Dual Code

We'll identify the dual code with the binary row space of the matrix $\begin{bmatrix} x \\ f(x) \end{bmatrix}$, where x ranges over all of L.

The columns comprise the graph Γ_f of f.

The Dual Code

We'll identify the dual code with the binary row space of the matrix $\begin{bmatrix} x \\ f(x) \end{bmatrix}$, where x ranges over all of L.

The columns comprise the graph Γ_f of f.

The codewords are

$$\{Trace(ax) : a \in L\} \oplus \{Trace(bf(x)) : b \in L\}.$$

CCZ-Equivalence

f and g are CCZ-equivalent if $\Gamma_g = \mathcal{L}\Gamma_f$ for some $\mathcal{L}$ in $GL(L^2)$.

CCZ-Equivalence

f and g are CCZ-equivalent if $\Gamma_g = \mathcal{L}\Gamma_f$ for some $\mathcal{L}$ in $GL(L^2)$.

This means that $g = f_2 \circ f_1^{-1}$, where

$$\begin{bmatrix} f_1(x) \\ f_2(x) \end{bmatrix} = \mathcal{L} \begin{bmatrix} x \\ f(x) \end{bmatrix}.$$

CCZ-Equivalence

f and g are CCZ-equivalent if $\Gamma_g = \mathcal{L}\Gamma_f$ for some $\mathcal{L}$ in $GL(L^2)$.

This means that $g = f_2 \circ f_1^{-1}$, where

$$\begin{bmatrix} f_1(x) \\ f_2(x) \end{bmatrix} = \mathcal{L} \begin{bmatrix} x \\ f(x) \end{bmatrix}.$$

For $S = \Gamma_f$ or $S = \Delta_f := \{(a, b) : \#(f(x + a) + f(x) = b) = 2\}$ the S-rank of f is the 2-rank of the matrix $[S(X + Y)]$, $X, Y \in L^2$, where we identify S with its characteristic function.

CCZ-Equivalence

f and g are CCZ-equivalent if $\Gamma_g = \mathcal{L}\Gamma_f$ for some $\mathcal{L}$ in $GL(L^2)$.

This means that $g = f_2 \circ f_1^{-1}$, where

$$\begin{bmatrix} f_1(x) \\ f_2(x) \end{bmatrix} = \mathcal{L} \begin{bmatrix} x \\ f(x) \end{bmatrix}.$$

For $S = \Gamma_f$ or $S = \Delta_f := \{(a, b) : \#(f(x + a) + f(x) = b) = 2\}$ the S-rank of f is the 2-rank of the matrix $[S(X + Y)]$, $X, Y \in L^2$, where we identify S with its characteristic function.

The Γ-rank and the Δ-rank are useful CCZ-invariants introduced by Edel, Kyureghyan and Pott.

The Banff APNs in dimension 6

dim 6

Fourier coefficients:

I.
{-8(28), 8(36)}(42),
{ 0(48), 16(10), -16(6) }(21),
{ 0(63), 64 }

II.
{-8(28), 8(36)}(46),
{ 0(48), 16(10), -16(6) }(16),
{ 0(60), -32, 32(3) },
{ 0(63), 64 }

f	$\Gamma-$rank	$\Delta-$rank	$\lvert Aut(\widetilde{\mathcal{C}(f)})\rvert$
x^3	1102	94	$2^6\cdot 6\cdot 63$
$x^3+u^{11}x^6+ux^9$	1146	94	$2^6\cdot 63$
$ux^5+x^9+u^4x^{17}+ux^{18}$ $+u^4x^{20}+ux^{24}+u^4x^{34}+ux^{40}$	1158	96	$2^6\cdot 5$
$u^7x^3+x^5+u^3x^9+u^4x^{10}+x^{17}+u^6x^{18}$	1166	94	$2^6\cdot 7$
$x^3+ux^{24}+x^{10}$	1166	96	$2^6\cdot 14$
$x^3+u^{17}(x^{17}+x^{18}+x^{20}+x^{24})$	1168	96	2^6
$x^3+u^{11}x^5+u^{13}x^9$ $+x^{17}+u^{11}x^{33}+x^{48}$	1170	96	$2^6\cdot 5^\dagger$
$u^{25}x^5+x^9+u^{38}x^{12}$ $+u^{25}x^{18}+u^{25}x^{36}$	1170	96	2^6
$u^{40}x^5+u^{10}x^6+u^{62}x^{20}+u^{35}x^{33}$ $+u^{15}x^{34}+u^{29}x^{48}$	1170	96	2^6
$u^{34}x^6+u^{52}x^9+u^{48}x^{12}+u^6x^{20}$ $+u^9x^{33}+u^{23}x^{34}+u^{25}x^{40}$	1170	96	2^6
$x^9+u^4(x^{10}+x^{18})$ $+u^9(x^{12}+x^{20}+x^{40}$	1172	96	2^6
$u^{52}x^3+u^{47}x^5+ux^6+u^9x^9+u^{44}x^{12}$ $+u^{47}x^{33}+u^{10}x^{34}+u^{33}x^{40}$	1172	96	2^6
$u(x^6+x^{10}+x^{24}+x^{33})+x^9+u^4x^{17}$	1174	96	2^6

Quadratic and Bilinear Maps

$V = L = GF(2^m)$.

$$f(X) = \sum_{0 \le i \le j \le m-1} c_{i,j} X^{2^i + 2^j} \in GF(2^m)[X]$$

Quadratic and Bilinear Maps

$V = L = GF(2^m)$.

$$f(X) = \sum_{0 \le i \le j \le m-1} c_{i,j} X^{2^i + 2^j} \in GF(2^m)[X]$$

$$\begin{aligned} \beta_f(X, Y) &:= f(X+Y) + f(X) + f(Y) \\ &= \sum_{0 \le i < j \le m-1} c_{i,j} \left[X^{2^i} Y^{2^j} + X^{2^j} Y^{2^i} \right]. \end{aligned}$$

β_f is bi-additive (i.e. $GF(2)$-bilinear) and alternating.

The Quadratic Forms

Let $f : L \to L$ be any map.
The Boolean functions $f_b(x) := Trace(bf(x))$, $b \in L$, are the components of f.
If f is a quadratic map, then the components f_b are quadratic forms on L.
Recall:

- $q : V \to GF(2)$ a quadratic form;

The Quadratic Forms

Let $f : L \rightarrow L$ be any map.
The Boolean functions $f_b(x) := Trace(bf(x))$, $b \in L$, are the components of f.
If f is a quadratic map, then the components f_b are quadratic forms on L.
Recall:

- $q : V \rightarrow GF(2)$ a quadratic form;
- $\beta_q(x, y) := q(x + y) + q(x) + q(y)$ is an alternating bilinear form;

The Quadratic Forms

Let $f : L \rightarrow L$ be any map.
The Boolean functions $f_b(x) := Trace(bf(x))$, $b \in L$, are the components of f.
If f is a quadratic map, then the components f_b are quadratic forms on L.
Recall:

- $q : V \rightarrow GF(2)$ a quadratic form;
- $\beta_q(x, y) := q(x + y) + q(x) + q(y)$ is an alternating bilinear form;
- $\text{rad}_q := \{y \in V : \beta_q(x, y) = 0 \; \forall x \in V\}$;

The Quadratic Forms

Let $f : L \to L$ be any map.
The Boolean functions $f_b(x) := Trace(bf(x))$, $b \in L$, are the components of f.
If f is a quadratic map, then the components f_b are quadratic forms on L.
Recall:

- $q : V \to GF(2)$ a quadratic form;
- $\beta_q(x, y) := q(x + y) + q(x) + q(y)$ is an alternating bilinear form;
- $\text{rad}_q := \{y \in V : \beta_q(x, y) = 0 \ \forall x \in V\}$;
- $\dim \text{rad}_q \equiv \dim V \bmod 2$.

The Quadratic Forms

Let $f : L \to L$ be any map.
The Boolean functions $f_b(x) := Trace(bf(x))$, $b \in L$, are the components of f.
If f is a quadratic map, then the components f_b are quadratic forms on L.
Recall:

- $q : V \to GF(2)$ a quadratic form;
- $\beta_q(x, y) := q(x + y) + q(x) + q(y)$ is an alternating bilinear form;
- $\text{rad}_q := \{y \in V : \beta_q(x, y) = 0 \; \forall x \in V\}$;
- $\dim \text{rad}_q \equiv \dim V \bmod 2$.

Let's call $rad_q^* := rad_q \backslash \{0\}$ the pointed radical.

The Radicals of a Quadratic APN

Theorem

Let f be a quadratic APN on $L = GF(2^m)$.
Then the nonempty pointed radicals $rad^*_{f_b}$ partition $L^\times$.

The Radicals of a Quadratic APN

Theorem

Let f be a quadratic APN on $L = GF(2^m)$.
Then the nonempty pointed radicals $rad^*_{f_b}$ partition $L^\times$.

Corollary (Nyberg's Theorem 1994)

- *If m is odd, then all components f_b, $b \neq 0$, are near-bent;i.e. dim $rad_{f_b} = 1$;*
- *If m is even, then at least two-thirds of the f_b, $b \neq 0$, are bent; i.e. $rad_{f_b} = 0$;*

What Boolean functions can be added?

Observation. $f : L \to L$ APN; $g : L \to GF(2)$ Boolean.
TFAE:

- $h := f + g$ is APN;
- g sums to 0 on every 2-flat on which f sums to 1.

What Boolean functions can be added?

Observation. $f : L \rightarrow L$ APN; $g : L \rightarrow GF(2)$ Boolean. TFAE:

- $h := f + g$ is APN;
- g sums to 0 on every 2-flat on which f sums to 1.

Budaghyan and Carlet discovered the beautiful general example

$$x^3 + Trace(x^9).$$

What Boolean functions can be added?

Observation. $f : L \to L$ APN; $g : L \to GF(2)$ Boolean.
TFAE:

- $h := f + g$ is APN;
- g sums to 0 on every 2-flat on which f sums to 1.

Budaghyan and Carlet discovered the beautiful general example

$$x^3 + Trace(x^9).$$

Such g's constitute the dual of the binary code spanned by (the characteristic functions of) the 2-flats on which f sums to 1.

What Boolean functions can be added?

Observation. $f : L \to L$ APN; $g : L \to GF(2)$ Boolean.
TFAE:

- $h := f + g$ is APN;
- g sums to 0 on every 2-flat on which f sums to 1.

Budaghyan and Carlet discovered the beautiful general example

$$x^3 + Trace(x^9).$$

Such g's constitute the dual of the binary code spanned by (the characteristic functions of) the 2-flats on which f sums to 1.
Some of the APNs in the Banff lists are related in this way...

What Boolean functions can be added?

Observation. $f : L \to L$ APN; $g : L \to GF(2)$ Boolean.
TFAE:

- $h := f + g$ is APN;
- g sums to 0 on every 2-flat on which f sums to 1.

Budaghyan and Carlet discovered the beautiful general example

$$x^3 + Trace(x^9).$$

Such g's constitute the dual of the binary code spanned by (the characteristic functions of) the 2-flats on which f sums to 1.
Some of the APNs in the Banff lists are related in this way...

but Edel and Pott had a better idea!!!

Switching

Replace JFD's Boolean function g by cg for c any element in $L^{\times}$. The above proposition and coding interpretation remain true on replacing 1 by c.

Switching

Replace JFD's Boolean function g by cg for c any element in $L^\times$.
The above proposition and coding interpretation remain true on replacing 1 by c.
But this switching operation can be iterated with different c's!!!
Edel and Pott applied this idea to the Banff lists of APNs.

Switching

Replace JFD's Boolean function g by cg for c any element in $L^\times$. The above proposition and coding interpretation remain true on replacing 1 by c.

But this switching operation can be iterated with different c's!!!

Edel and Pott applied this idea to the Banff lists of APNs.

Some results:

For $m = 6$ the Banff list of 13 APNs breaks into TWO switching classes represented by

- x^3 (2 members)
- $x^3 + x^{10} + u * x^{24}$ (11 members).

Switching

Replace JFD's Boolean function g by cg for c any element in $L^{\times}$.
The above proposition and coding interpretation remain true on replacing 1 by c.

But this switching operation can be iterated with different c's!!!

Edel and Pott applied this idea to the Banff lists of APNs.

Some results:

For $m = 6$ the Banff list of 13 APNs breaks into TWO switching classes represented by

- x^3 (2 members)
- $x^3 + x^{10} + u * x^{24}$ (11 members).

We call these maps the cube map and the Kim map, the latter because it is the first new APN found by Kim Browning when we began to study APNs.

Switching

Replace JFD's Boolean function g by cg for c any element in $L^\times$. The above proposition and coding interpretation remain true on replacing 1 by c.

But this switching operation can be iterated with different c's!!!

Edel and Pott applied this idea to the Banff lists of APNs.

Some results:

For $m = 6$ the Banff list of 13 APNs breaks into TWO switching classes represented by

- x^3 (2 members)
- $x^3 + x^{10} + u * x^{24}$ (11 members).

We call these maps the cube map and the Kim map, the latter because it is the first new APN found by Kim Browning when we began to study APNs.

EP also discovered in the $kim(x)$ switching class a new APN which is cubic and not CCZ-equivalent to any quadratic or power map!

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6).$

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6)$.

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Proof.

It's not too hard to show that $x = 0$ is the unique zero of $kim(x)$.

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6)$.

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Proof.

It's not too hard to show that $x = 0$ is the unique zero of $kim(x)$.

For all $\lambda \in K := GF(2^3)$, $kim(\lambda z) = \lambda^3 kim(z)$.

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6).$

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Proof.

It's not too hard to show that $x = 0$ is the unique zero of $kim(x)$.

For all $\lambda \in K := GF(2^3)$, $kim(\lambda z) = \lambda^3 kim(z)$. Thus, $kim(x)$ maps the subspace Kz to the subspace $Kkim(z)$.

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6)$.

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Proof.

It's not too hard to show that $x = 0$ is the unique zero of $kim(x)$.

For all $\lambda \in K := GF(2^3)$, $kim(\lambda z) = \lambda^3 kim(z)$. Thus, $kim(x)$ maps the subspace Kz to the subspace $Kkim(z)$.

The nine subspaces Kz comprise the components of a spread for L;

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6)$.

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Proof.

It's not too hard to show that $x = 0$ is the unique zero of $kim(x)$.

For all $\lambda \in K := GF(2^3)$, $kim(\lambda z) = \lambda^3 kim(z)$. Thus, $kim(x)$ maps the subspace Kz to the subspace $Kkim(z)$.

The nine subspaces Kz comprise the components of a spread for L; and kim(x) hits exactly five of them.

Combinatorial Properties of the Kim Map

$kim(x) = x^3 + x^{10} + u * x^{24} \in L[x], L = GF(2^6).$

Theorem

The image $D := kim(L)$ is a (64,36,20)-ds in L.
Its characteristic function is a cubic bent function.

Proof.

It's not too hard to show that $x = 0$ is the unique zero of $kim(x)$.

For all $\lambda \in K := GF(2^3)$, $kim(\lambda z) = \lambda^3 kim(z)$. Thus, $kim(x)$ maps the subspace Kz to the subspace $Kkim(z)$.

The nine subspaces Kz comprise the components of a spread for L; and kim(x) hits exactly five of them.
Therefore, $kim(L)$ is a partial-spread difference set of type $\mathcal{PS}^{(+)}$.

□

Line Spread and Affine Design

If f is any quadratic APN with exactly $\frac{2(2^m-1)}{3}$ bent components, then the $\frac{2^m-1}{3}$ pointed nonzero radicals give a line spread for $L^\times = PG(m-1, 2)$.

Line Spread and Affine Design

If f is any quadratic APN with exactly $\frac{2(2^m-1)}{3}$ bent components, then the $\frac{2^m-1}{3}$ pointed nonzero radicals give a line spread for $L^\times = PG(m-1,2)$.

We know only one quadratic APN which does not share this property with x^3.

Line Spread and Affine Design

If f is any quadratic APN with exactly $\frac{2(2^m-1)}{3}$ bent components, then the $\frac{2^m-1}{3}$ pointed nonzero radicals give a line spread for $L^{\times} = PG(m-1,2)$.

We know only one quadratic APN which does not share this property with x^3.

A theorem of Rahilly gives an affine design with parameters same as $AG_{s-1}(s,4)$, $m = 2s$.

Line Spread and Affine Design

If f is any quadratic APN with exactly $\frac{2(2^m-1)}{3}$ bent components, then the $\frac{2^m-1}{3}$ pointed nonzero radicals give a line spread for $L^\times = PG(m-1, 2)$.

We know only one quadratic APN which does not share this property with x^3.

A theorem of Rahilly gives an affine design with parameters same as $AG_{s-1}(s, 4)$, $m = 2s$.

Theorem

The (64, 16, 5)-design $\mathcal{D}$ obtained from the Rahilly construction applied to the line spread for kim(x) has:

- *2-rank* $= 19 \neq 16 =$ *2-rank of* $AG_2(3, 4)$*;*
- $|Aut(\mathcal{D})| = 2688 = 2^7 x 3 x 7$.

Another Interesting APN

g(x) =

```
w^59*x^60 + w^34*x^58 + w^8*x^57 + w^23*x^56 + w^21*x^54 + w^39*x^53 + w^48*x^52
    + w^48*x^51 + w^56*x^50 + w^24*x^49 + w^44*x^48 + w^26*x^46 + w^2*x^45 +
    w^13*x^44 + w^54*x^43 + w^45*x^42 + w^32*x^41 + w^41*x^40 + w^48*x^39 +
    w^45*x^38 + w^32*x^37 + w^14*x^36 + w^57*x^35 + w^50*x^34 + x^33 + w^5*x^32
    + w^31*x^30 + w^45*x^29 + w^51*x^28 + w^32*x^27 + w^30*x^26 + w^8*x^25 +
    w^33*x^24 + w^39*x^23 + w^36*x^22 + w^4*x^21 + w^38*x^20 + w^52*x^19 +
    w^17*x^18 + w^15*x^17 + w^31*x^16 + w^42*x^15 + w^5*x^14 + w^25*x^13 +
    w^9*x^12 + w^3*x^11 + w*x^10 + w^30*x^9 + w^22*x^8 + w^23*x^7 + w^54*x^6 +
    w^46*x^5 + w^60*x^4 + w^29*x^3 + w^20*x^2 + w^61*x
```

Where did that come from?

Where did that come from?

$g(x)$ is CCZ-equivalent to the Kim map; i.e.

$$g = f_2 \circ f_1^{-1},$$

where f_1 and f_2 are quadratics obtained as follows:

Decompositions of the Code $\mathcal{C}_f^\perp$

We have $L = GF(2^6) = K \oplus Ku$, where $K = GF(2^3)$; put $f(x) = u * kim(x)$.

Decompositions of the Code $\mathcal{C}_f^\perp$

We have $L = GF(2^6) = K \oplus Ku$, where $K = GF(2^3)$; put $f(x) = u * kim(x)$.
We have $\mathcal{C}_f^\perp = \mathcal{A} \oplus \mathcal{B}$, where
$\mathcal{A} = \{\, Tr(ax) : a \in L\}$ and $\mathcal{B} = \{\, Tr(bf(x)) : b \in L\}$.

Decompositions of the Code $\mathcal{C}_f^\perp$

We have $L = GF(2^6) = K \oplus Ku$, where $K = GF(2^3)$; put $f(x) = u * kim(x)$.
We have $\mathcal{C}_f^\perp = \mathcal{A} \oplus \mathcal{B}$, where
$\mathcal{A} = \{Tr(ax) : a \in L\}$ and $\mathcal{B} = \{Tr(bf(x)) : b \in L\}$.
Use the decomposition $L = K \oplus Ku$ to decompose $\mathcal{A}$ and $\mathcal{B}$:

$$\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2$$

and

$$\mathcal{B} = \mathcal{B}_1 \oplus \mathcal{B}_2.$$

Decompositions of the Code $\mathcal{C}_f^\perp$

We have $L = GF(2^6) = K \oplus Ku$, where $K = GF(2^3)$; put $f(x) = u * kim(x)$.
We have $\mathcal{C}_f^\perp = \mathcal{A} \oplus \mathcal{B}$, where
$\mathcal{A} = \{Tr(ax) : a \in L\}$ and $\mathcal{B} = \{Tr(bf(x)) : b \in L\}$.
Use the decomposition $L = K \oplus Ku$ to decompose $\mathcal{A}$ and $\mathcal{B}$:

$$\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2$$

and

$$\mathcal{B} = \mathcal{B}_1 \oplus \mathcal{B}_2.$$

Switch partners! :)

$$[f_1(x)] := \mathcal{A}_1 \oplus \mathcal{B}_1$$

and

$$[f_2(x)] := \mathcal{A}_2 \oplus \mathcal{B}_2.$$

Decompositions of the Code $\mathcal{C}_f^\perp$

We have $L = GF(2^6) = K \oplus Ku$, where $K = GF(2^3)$; put $f(x) = u * kim(x)$.
We have $\mathcal{C}_f^\perp = \mathcal{A} \oplus \mathcal{B}$, where
$\mathcal{A} = \{ Tr(ax) : a \in L\}$ and $\mathcal{B} = \{ Tr(bf(x)) : b \in L\}$.
Use the decomposition $L = K \oplus Ku$ to decompose $\mathcal{A}$ and $\mathcal{B}$:

$$\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2$$

and

$$\mathcal{B} = \mathcal{B}_1 \oplus \mathcal{B}_2.$$

Switch partners! :)

$$[f_1(x)] := \mathcal{A}_1 \oplus \mathcal{B}_1$$

and

$$[f_2(x)] := \mathcal{A}_2 \oplus \mathcal{B}_2.$$

so

$$\mathcal{C}_f^\perp = [f_1(x)] \oplus [f_2(x)].$$

Surprise!

$$\mathcal{C}_f^{\perp} = [f_1(x)] \oplus [f_2(x)].$$

Surprise!

$$\mathcal{C}_f^{\perp} = [f_1(x)] \oplus [f_2(x)].$$

and, incidentally ...

Surprise!

$$\mathcal{C}_f^\perp = [f_1(x)] \oplus [f_2(x)].$$

and, incidentally . . .
BOTH f_1 and f_2 are permutations!!!

Surprise!

$$\mathcal{C}_f^{\perp} = [f_1(x)] \oplus [f_2(x)].$$

and, incidentally . . .
BOTH f_1 and f_2 are permutations!!!

That's right!...
$g = f_2 \circ f_1^{-1}$ is an

APN permutation on $GF(2^6)$!!! :)

The First APN Permutation of even dimension

0	54	48	13	15	18	53	35
25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37
60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62
47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49
9	6	23	32	30	12	55	22

Adam Wolfe's Breakthrough

Theorem (Adam Wolfe)

The Kim map is CCZ-equivalent to an APN permutation.
The Kim code contains 222 simplex subcodes, 32 of which split into two sets of 16, with any pair from different sets being "disjoint".
The 256 corresponding APN permutations are, of course, all CCZ-equivalent to kim(x).

Adam Wolfe's Breakthrough

Theorem (Adam Wolfe)

The Kim map is CCZ-equivalent to an APN permutation.
The Kim code contains 222 simplex subcodes, 32 of which split into two sets of 16, with any pair from different sets being "disjoint".
The 256 corresponding APN permutations are, of course, all CCZ-equivalent to kim(x).

We need invertible $\mathcal{L}$ such that

$$\mathcal{L}\begin{bmatrix} x \\ f(x) \end{bmatrix} = \begin{bmatrix} f_1(x) \\ f_2(x) \end{bmatrix},$$

where f_1 and f_2 are permutations.

Adam Wolfe's Breakthrough

Adam found ALL simplex subcodes

$$[f_1(x)] = L_1 \begin{bmatrix} x \\ f(x) \end{bmatrix}$$

by generating L_1 in reduced row echelon form, one column at a time, from left to right using the permutation constraint $x \neq y \Rightarrow f_1(x) \neq f_1(y)$ to restrict the choice of new column in L_1; i.e. no vector in $\Sigma := \left\{ \begin{bmatrix} x+y \\ f(x)+f(y) \end{bmatrix} : x \neq y \right\}$ can be in the nullspace of L_1. Thus, avoid solutions to

$$[l_1, l_2, \cdots, l_j] \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_j \end{bmatrix} = 0,$$

where c is a vector in the sorted set Σ for which $c_t = \delta_{j,t}$ for $t \geq j$.

In Retrospect: Randomized Search

It's easier to find something

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a, b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$.

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a, b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that $b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and $b_{i+1} + s \in \mathcal{B}_1 \ \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a, b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that

$b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and

$b_{i+1} + s \in \mathcal{B}_1 \; \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

if you get stuck

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a, b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that
$b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and
$b_{i+1} + s \in \mathcal{B}_1 \; \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

if you get stuck just start over!

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a, b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that

$b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and

$b_{i+1} + s \in \mathcal{B}_1 \ \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

if you get stuck just start over!

Suppose we get the first m-dim subspace S_1.

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a,b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that

$b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and

$b_{i+1} + s \in \mathcal{B}_1 \; \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

if you get stuck just start over!

Suppose we get the first m-dim subspace S_1.

Step 2. Set $\mathcal{B}_2 = \mathcal{B} \backslash S_1$.

Repeat above **Step 1** with $\mathcal{B}_2$ in place of $\mathcal{B}_1$.

again... if stuck just start over!

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a, b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that

$b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and

$b_{i+1} + s \in \mathcal{B}_1 \; \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

if you get stuck just start over!

Suppose we get the first m-dim subspace S_1.

Step 2. Set $\mathcal{B}_2 = \mathcal{B} \backslash S_1$.

Repeat above **Step 1** with $\mathcal{B}_2$ in place of $\mathcal{B}_1$.

again... if stuck just start over!

Have upper bound on number of tries... if we hit the bound go back to **Step 1** and start over.

If we get to m in **Step 2** we're done!

In Retrospect: Randomized Search

It's easier to find something if you know it's there! .

Let $f(x)$ be an APN on $GF(2^m)$.

Compute $\mathcal{B} := \{(a,b) : Trace(ax + bf(x)) balanced\}$.

Step 1. Set $\mathcal{B}_1 = \mathcal{B}$. Choose $b_1, b_2, \ldots, b_m$ randomly so that
$b_{i+1} \notin \langle b_1, b_2, \ldots, b_i \rangle$ and
$b_{i+1} + s \in \mathcal{B}_1 \ \forall s \in \langle b_1, b_2, \ldots, b_i \rangle$.

if you get stuck just start over!

Suppose we get the first m-dim subspace S_1.

Step 2. Set $\mathcal{B}_2 = \mathcal{B} \backslash S_1$.

Repeat above **Step 1** with $\mathcal{B}_2$ in place of $\mathcal{B}_1$.

again... if stuck just start over!

Have upper bound on number of tries... if we hit the bound go back to **Step 1** and start over.

If we get to m in **Step 2** we're done!

For $m = 6$ and $f(x) = kim(x)$...$\#\mathcal{B} = 1071$...

but solutions pour out quickly! :)

Good News and Bad News

First the good news:

Good News and Bad News

First the good news:

We found an APN permutation in even dimension! :)

Good News and Bad News

First the good news:

We found an APN permutation in even dimension! :)

The bad news is: it is the ONLY one that we found! :(

Good News and Bad News

First the good news:

We found an APN permutation in even dimension! :)

The bad news is: it is the ONLY one that we found! :(
We have shown that no other on the Banff-EP-MAGMA lists of known APNs of dimension up to 10 can have a double-simplex code. :(

Good News and Bad News

First the good news:

We found an APN permutation in even dimension! :)

The bad news is: it is the ONLY one that we found! :(
We have shown that no other on the Banff-EP-MAGMA lists of known APNs of dimension up to 10 can have a double-simplex code. :(
but maybe there's hope! :)

Good News and Bad News

The highly structured decomposition of the Kim code suggests that much of the structure . . . if not all . . . should generalize to higher dimensions.

Good News and Bad News

The highly structured decomposition of the Kim code suggests that much of the structure . . . if not all . . . should generalize to higher dimensions.

Does it?

Good News and Bad News

The highly structured decomposition of the Kim code suggests that much of the structure ... if not all ... should generalize to higher dimensions.

Does it?

and $\cdots$ if not $\cdots$ does something else work?

Good News and Bad News

The highly structured decomposition of the Kim code suggests that much of the structure . . . if not all . . . should generalize to higher dimensions.

Does it?

and $\cdots$ if not $\cdots$ does something else work?

STILL **BIG APN PROBLEM:** Does there exist an APN permutation in even dimension greater than 6?