Testing generalized affine equivalence and applications to the classification of GAPN functions

Ana Sălăgean Nikolay Stoyanov Kaleyski Ferruh Özbudak

Loughborough University, UK

University of Bergen, Norway

Sabancı University, Istanbul, Türkiye

Outline

- Background: GAPN functions, generalized affine equivalence
- Invariants
- Canonical form w.r.t. left linear transformations
- Classification of GAPN functions of degree 3 over $\mathbb{F}_3^3$

Outline

- Background: GAPN functions, generalized affine equivalence
- Invariants
- Canonical form w.r.t. left linear transformations
- Classification of GAPN functions of degree 3 over $\mathbb{F}_3^3$

Outline

- Background: GAPN functions, generalized affine equivalence
- Invariants
- Canonical form w.r.t. left linear transformations
- Classification of GAPN functions of degree 3 over $\mathbb{F}_3^3$

Outline

- Background: GAPN functions, generalized affine equivalence
- Invariants
- Canonical form w.r.t. left linear transformations
- Classification of GAPN functions of degree 3 over $\mathbb{F}_3^3$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$

f_i are polynomial functions of degree at most $p - 1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1 x_2 x_3 + x_1 x_2 + x_3, 2x_1 x_2, x_3 + 2) \\ &= (1,0,0)x_1 x_2 x_3 + (1,2,0)x_1 x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$

f_i are polynomial functions of degree at most $p - 1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1x_2x_3 + x_1x_2 + x_3, 2x_1x_2, x_3 + 2) \\ &= (1,0,0)x_1x_2x_3 + (1,2,0)x_1x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$

f_i are polynomial functions of degree at most $p-1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1x_2x_3 + x_1x_2 + x_3, 2x_1x_2, x_3 + 2) \\ &= (1,0,0)x_1x_2x_3 + (1,2,0)x_1x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$

f_i are polynomial functions of degree at most $p-1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1x_2x_3 + x_1x_2 + x_3, 2x_1x_2, x_3 + 2) \\ &= (1,0,0)x_1x_2x_3 + (1,2,0)x_1x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$
f_i are polynomial functions of degree at most $p - 1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1 x_2 x_3 + x_1 x_2 + x_3, 2x_1 x_2, x_3 + 2) \\ &= (1,0,0)x_1 x_2 x_3 + (1,2,0)x_1 x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$
f_i are polynomial functions of degree at most $p - 1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1x_2x_3 + x_1x_2 + x_3, 2x_1x_2, x_3 + 2) \\ &= (1,0,0)x_1x_2x_3 + (1,2,0)x_1x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$
f_i are polynomial functions of degree at most $p - 1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1 x_2 x_3 + x_1 x_2 + x_3, 2x_1 x_2, x_3 + 2) \\ &= (1, 0, 0) x_1 x_2 x_3 + (1, 2, 0) x_1 x_2 + (1, 0, 1) x_3 + (0, 0, 2) \end{aligned}$$

Algebraic normal form

F function with n inputs and n outputs over $\mathbb{F}_p$

Univariate representation

or

Multivariate ANF (algebraic normal form)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

$F = (f_1, \ldots, f_n)$
f_i are polynomial functions of degree at most $p - 1$ in each variable

Example over $\mathbb{F}_3^3$

$$\begin{aligned} F(x_1, x_2, x_3) &= (x_1 x_2 x_3 + x_1 x_2 + x_3, 2x_1 x_2, x_3 + 2) \\ &= (1,0,0)x_1 x_2 x_3 + (1,2,0)x_1 x_2 + (1,0,1)x_3 + (0,0,2) \end{aligned}$$

Differentiation

Definition

The discrete derivative of F in direction $a \neq 0$ is

$$\Delta_a F(x) = F(x+a) - F(x) - F(a) + F(0)$$

Higher order differentiation (higher order derivative)

$$\Delta^{(k)}_{a_1,\dots,a_k} F = \Delta_{a_1} \Delta_{a_2} \dots \Delta_{a_k} F$$

We denote $\Delta^{(k)}_a F = \Delta^{(k)}_{a,\dots,a} F$.

$\deg(\Delta_a F) \leq \deg(F) - 1$ [Lai,1994]

Differentiation

Definition

The discrete derivative of F in direction $a \neq 0$ is

$$\Delta_a F(x) = F(x+a) - F(x) - F(a) + F(0)$$

Higher order differentiation (higher order derivative)

$$\Delta^{(k)}_{a_1,\ldots,a_k} F = \Delta_{a_1} \Delta_{a_2} \ldots \Delta_{a_k} F$$

We denote $\Delta^{(k)}_a F = \Delta^{(k)}_{a,\ldots,a} F$.

$\deg(\Delta_a F) \leq \deg(F) - 1$ [Lai,1994]

Differentiation

Definition

The discrete derivative of F in direction $a \neq 0$ is

$$\Delta_a F(x) = F(x+a) - F(x) - F(a) + F(0)$$

Higher order differentiation (higher order derivative)

$$\Delta^{(k)}_{a_1,\ldots,a_k} F = \Delta_{a_1} \Delta_{a_2} \ldots \Delta_{a_k} F$$

We denote $\Delta^{(k)}_a F = \Delta^{(k)}_{a,\ldots,a} F$.

$\deg(\Delta_a F) \leq \deg(F) - 1$ [Lai,1994]

Differentiation

Definition

The discrete derivative of F in direction $a \neq 0$ is

$$\Delta_a F(x) = F(x+a) - F(x) - F(a) + F(0)$$

Higher order differentiation (higher order derivative)

$$\Delta^{(k)}_{a_1,\ldots,a_k} F = \Delta_{a_1}\Delta_{a_2}\ldots\Delta_{a_k} F$$

We denote $\Delta^{(k)}_a F = \Delta^{(k)}_{a,\ldots,a} F$.

$\deg(\Delta_a F) \leq \deg(F) - 1$ [Lai,1994]

Differentiation

Definition

The discrete derivative of F in direction $a \neq 0$ is

$$\Delta_a F(x) = F(x+a) - F(x) - F(a) + F(0)$$

Higher order differentiation (higher order derivative)

$$\Delta^{(k)}_{a_1,\ldots,a_k} F = \Delta_{a_1}\Delta_{a_2}\ldots\Delta_{a_k} F$$

We denote $\Delta^{(k)}_a F = \Delta^{(k)}_{a,\ldots,a} F$.

$\deg(\Delta_a F) \leq \deg(F) - 1$ [Lai,1994]

APN functions

Definition
$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN (almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ the equation

$$\Delta_a F(x) = b$$

has at most 2 solutions.

F is EA-equivalent to G if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq 1$.

The APN property is invariant to EA-equivalence.

APN functions

Definition

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN (almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ the equation

$$\Delta_a F(x) = b$$

has at most 2 solutions.

F is EA-equivalent to G if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq 1$.

The APN property is invariant to EA-equivalence.

APN functions

Definition

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN (almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ the equation

$$\Delta_a F(x) = b$$

has at most 2 solutions.

F is EA-equivalent to G if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq 1$.

The APN property is invariant to EA-equivalence.

APN functions

Definition
$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN (almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ the equation

$$\Delta_a F(x) = b$$

has at most 2 solutions.

F is EA-equivalent to G if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq 1$.

The APN property is invariant to EA-equivalence.

GAPN functions

Definition [Kuroda,Tsujie,2017]
$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is GAPN (generalized almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{p^n}$ with $a \neq 0$ the equation

$$\Delta_a^{(p-1)} F(x) = b$$

has at most p solutions.

GAPN functions

Definition [Kuroda,Tsujie,2017]
$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is GAPN (generalized almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{p^n}$ with $a \neq 0$ the equation

$$\Delta_a^{(p-1)} F(x) = b$$

has at most p solutions.

GAPN functions

Definition [Kuroda,Tsujie,2017]
$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is GAPN (generalized almost perfect nonlinear) if for all $a, b \in \mathbb{F}_{p^n}$ with $a \neq 0$ the equation

$$\Delta_a^{(p-1)} F(x) = b$$

has at most p solutions.

Affine equivalence for GAPN functions

Definition Generalized extended affine equivalence [O,S, 21]:

$F \sim_k G$ if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq k$.

The GAPN property is invariant to $\sim_{p-1}$.

Constructions of GAPN functions were given by [Kuroda,Tsujie,2017], [Kuroda,2017], [Zha,Hu,Zhang,2018], [O,S,2021], [Wang, Wang,Zhang,2022],[Bartoli et al,2022],[Beierle,2022],[S,O,2023] etc.

Affine equivalence for GAPN functions

Definition Generalized extended affine equivalence [O,S, 21]:

$F \sim_k G$ if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq k$.

The GAPN property is invariant to $\sim_{p-1}$.

Constructions of GAPN functions were given by [Kuroda,Tsujie,2017], [Kuroda,2017], [Zha,Hu,Zhang,2018], [O,S,2021], [Wang, Wang,Zhang,2022],[Bartoli et al,2022],[Beierle,2022],[S,O,2023] etc.

Affine equivalence for GAPN functions

Definition Generalized extended affine equivalence [O,S, 21]:

$F \sim_k G$ if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq k$.

The GAPN property is invariant to $\sim_{p-1}$.

Constructions of GAPN functions were given by [Kuroda,Tsujie,2017], [Kuroda,2017], [Zha,Hu,Zhang,2018], [O,S,2021], [Wang, Wang,Zhang,2022],[Bartoli et al,2022],[Beierle,2022],[S,O,2023] etc.

Affine equivalence for GAPN functions

Definition Generalized extended affine equivalence [O,S, 21]:

$F \sim_k G$ if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq k$.

The GAPN property is invariant to $\sim_{p-1}$.

Constructions of GAPN functions were given by [Kuroda,Tsujie,2017], [Kuroda,2017], [Zha,Hu,Zhang,2018], [O,S,2021], [Wang, Wang,Zhang,2022],[Bartoli et al,2022],[Beierle,2022],[S,O,2023] etc.

Affine equivalence for GAPN functions

Definition Generalized extended affine equivalence [O,S, 21]:

$F \sim_k G$ if

$$G = A_1 \circ F \circ A_2 + H$$

for some invertible affine transformations A_1, A_2 and $\deg(H) \leq k$.

The GAPN property is invariant to $\sim_{p-1}$.

Constructions of GAPN functions were given by [Kuroda,Tsujie,2017], [Kuroda,2017], [Zha,Hu,Zhang,2018], [O,S,2021], [Wang, Wang,Zhang,2022],[Bartoli et al,2022],[Beierle,2022],[S,O,2023] etc.

GAPN construction using the multivariate ANF

[S,O,23] constructed GAPN functions of degree p by using a technique similar to the construction of [Yu,Wang,Li,2014] for APN quadratic functions using matrices with certain properties.

We consider F in multivariate ANF.

If F has algebraic degree p, then $\Delta_a^{(p-1)}F$ is linear.

The equation $\Delta_a^{(p-1)}F(x) = b$ has at most p solutions iff its coefficients span a space of dimension at least $n-1$.

GAPN construction using the multivariate ANF

[S,O,23] constructed GAPN functions of degree p by using a technique similar to the construction of [Yu,Wang,Li,2014] for APN quadratic functions using matrices with certain properties.

We consider F in multivariate ANF.

If F has algebraic degree p, then $\Delta_a^{(p-1)} F$ is linear.

The equation $\Delta_a^{(p-1)} F(x) = b$ has at most p solutions iff its coefficients span a space of dimension at least $n-1$.

GAPN construction using the multivariate ANF

[S,O,23] constructed GAPN functions of degree p by using a technique similar to the construction of [Yu,Wang,Li,2014] for APN quadratic functions using matrices with certain properties.

We consider F in multivariate ANF.

If F has algebraic degree p, then $\Delta_a^{(p-1)}F$ is linear.

The equation $\Delta_a^{(p-1)}F(x) = b$ has at most p solutions iff its coefficients span a space of dimension at least $n-1$.

GAPN construction using the multivariate ANF

[S,O,23] constructed GAPN functions of degree p by using a technique similar to the construction of [Yu,Wang,Li,2014] for APN quadratic functions using matrices with certain properties.

We consider F in multivariate ANF.

If F has algebraic degree p, then $\Delta_a^{(p-1)}F$ is linear.

The equation $\Delta_a^{(p-1)}F(x) = b$ has at most p solutions iff its coefficients span a space of dimension at least $n-1$.

GAPN construction using the multivariate ANF

[S,O,23] constructed GAPN functions of degree p by using a technique similar to the construction of [Yu,Wang,Li,2014] for APN quadratic functions using matrices with certain properties.

We consider F in multivariate ANF.

If F has algebraic degree p, then $\Delta_a^{(p-1)} F$ is linear.

The equation $\Delta_a^{(p-1)} F(x) = b$ has at most p solutions iff its coefficients span a space of dimension at least $n - 1$.

GAPN construction using the multivariate ANF

Theorem (S,O,23)

$$F(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \mathbf{c}_{ij} x_i^{p-1} x_j,$$

where $\mathbf{c}_{ij} \in \mathbb{F}_p^n$ *and* $\mathbf{c}_{ii} = \mathbf{0}$.
F is GAPN iff for any $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_p^n \setminus \{\mathbf{0}\}$, *the set*

$$\left\{ \sum_{j=1}^{n} a_j \left(a_i^{p-2} \mathbf{c}_{ij} - a_j^{p-2} \mathbf{c}_{ji} \right) : i = 1, \ldots, n \right\}$$

spans a subspace of dimension $n - 1$.

GAPN construction using the multivariate ANF

Example: $n = 3, p = 3$.

$$F(x_1, x_2, x_3) = \sum_{i=1}^{3} \sum_{j=1}^{3} \mathbf{c}_{ij} x_i^2 x_j,$$

where $\mathbf{c}_{ij} \in \mathbb{F}_3^3$ and $\mathbf{c}_{ii} = \mathbf{0}$. Note $x_1 x_2 x_3$ does not appear in F.

$$\begin{pmatrix} \mathbf{0} & \mathbf{c}_{12} & \mathbf{c}_{13} \\ \mathbf{c}_{21} & \mathbf{0} & \mathbf{c}_{23} \\ \mathbf{c}_{31} & \mathbf{c}_{32} & \mathbf{0} \end{pmatrix}$$

GAPN construction using the multivariate ANF

Example: $n = 3, p = 3$.

$$F(x_1, x_2, x_3) = \sum_{i=1}^{3} \sum_{j=1}^{3} \mathbf{c}_{ij} x_i^2 x_j,$$

where $\mathbf{c}_{ij} \in \mathbb{F}_3^3$ and $\mathbf{c}_{ii} = \mathbf{0}$. Note $x_1 x_2 x_3$ does not appear in F.

$$\begin{pmatrix} \mathbf{0} & \mathbf{c}_{12} & \mathbf{c}_{13} \\ \mathbf{c}_{21} & \mathbf{0} & \mathbf{c}_{23} \\ \mathbf{c}_{31} & \mathbf{c}_{32} & \mathbf{0} \end{pmatrix}$$

GAPN construction using the multivariate ANF

Example: $n = 3, p = 3$.

$$F(x_1, x_2, x_3) = \sum_{i=1}^{3} \sum_{j=1}^{3} \mathbf{c}_{ij} x_i^2 x_j,$$

where $\mathbf{c}_{ij} \in \mathbb{F}_3^3$ and $\mathbf{c}_{ii} = \mathbf{0}$. Note $x_1 x_2 x_3$ does not appear in F.

$$\begin{pmatrix} \mathbf{0} & \mathbf{c}_{12} & \mathbf{c}_{13} \\ \mathbf{c}_{21} & \mathbf{0} & \mathbf{c}_{23} \\ \mathbf{c}_{31} & \mathbf{c}_{32} & \mathbf{0} \end{pmatrix}$$

GAPN construction using the multivariate ANF

F is GAPN iff for any $a_2, a_3 \in \mathbb{F}_3^*$ each of the following sets of vectors spans a space of dimension 2:

$\{\mathbf{c}_{12}, \mathbf{c}_{13}\}$
$\{\mathbf{c}_{21}, \mathbf{c}_{23}\}$
$\{\mathbf{c}_{31}, \mathbf{c}_{32}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21}, \mathbf{c}_{13} + \mathbf{c}_{23}\}$
$\{a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{12} + \mathbf{c}_{32}\}$
$\{a_3\mathbf{c}_{23} - \mathbf{c}_{32}, \mathbf{c}_{21} + \mathbf{c}_{31}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21} + a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{21} - a_2\mathbf{c}_{12} + a_3\mathbf{c}_{23} - a_2\mathbf{c}_{32}, \mathbf{c}_{31} - a_3\mathbf{c}_{13} + a_2\mathbf{c}_{32} - a_3\mathbf{c}_{23}\}$

We can assume that $\mathbf{c}_{12} = \mathbf{e}_1$ and $\mathbf{c}_{13} = \mathbf{e}_2$.

GAPN construction using the multivariate ANF

F is GAPN iff for any $a_2, a_3 \in \mathbb{F}_3^*$ each of the following sets of vectors spans a space of dimension 2:

$\{\mathbf{c}_{12}, \mathbf{c}_{13}\}$
$\{\mathbf{c}_{21}, \mathbf{c}_{23}\}$
$\{\mathbf{c}_{31}, \mathbf{c}_{32}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21}, \mathbf{c}_{13} + \mathbf{c}_{23}\}$
$\{a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{12} + \mathbf{c}_{32}\}$
$\{a_3\mathbf{c}_{23} - \mathbf{c}_{32}, \mathbf{c}_{21} + \mathbf{c}_{31}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21} + a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{21} - a_2\mathbf{c}_{12} + a_3\mathbf{c}_{23} - a_2\mathbf{c}_{32}, \mathbf{c}_{31} - a_3\mathbf{c}_{13} + a_2\mathbf{c}_{32} - a_3\mathbf{c}_{23}\}$

We can assume that $\mathbf{c}_{12} = \mathbf{e}_1$ and $\mathbf{c}_{13} = \mathbf{e}_2$.

GAPN construction using the multivariate ANF

F is GAPN iff for any $a_2, a_3 \in \mathbb{F}_3^*$ each of the following sets of vectors spans a space of dimension 2:

$\{\mathbf{c}_{12}, \mathbf{c}_{13}\}$
$\{\mathbf{c}_{21}, \mathbf{c}_{23}\}$
$\{\mathbf{c}_{31}, \mathbf{c}_{32}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21}, \mathbf{c}_{13} + \mathbf{c}_{23}\}$
$\{a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{12} + \mathbf{c}_{32}\}$
$\{a_3\mathbf{c}_{23} - \mathbf{c}_{32}, \mathbf{c}_{21} + \mathbf{c}_{31}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21} + a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{21} - a_2\mathbf{c}_{12} + a_3\mathbf{c}_{23} - a_2\mathbf{c}_{32},$
$\mathbf{c}_{31} - a_3\mathbf{c}_{13} + a_2\mathbf{c}_{32} - a_3\mathbf{c}_{23}\}$

We can assume that $\mathbf{c}_{12} = \mathbf{e}_1$ and $\mathbf{c}_{13} = \mathbf{e}_2$.

GAPN construction using the multivariate ANF

F is GAPN iff for any $a_2, a_3 \in \mathbb{F}_3^*$ each of the following sets of vectors spans a space of dimension 2:

$\{\mathbf{c}_{12}, \mathbf{c}_{13}\}$
$\{\mathbf{c}_{21}, \mathbf{c}_{23}\}$
$\{\mathbf{c}_{31}, \mathbf{c}_{32}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21}, \mathbf{c}_{13} + \mathbf{c}_{23}\}$
$\{a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{12} + \mathbf{c}_{32}\}$
$\{a_3\mathbf{c}_{23} - \mathbf{c}_{32}, \mathbf{c}_{21} + \mathbf{c}_{31}\}$
$\{a_2\mathbf{c}_{12} - \mathbf{c}_{21} + a_3\mathbf{c}_{13} - \mathbf{c}_{31}, \mathbf{c}_{21} - a_2\mathbf{c}_{12} + a_3\mathbf{c}_{23} - a_2\mathbf{c}_{32},$
$\mathbf{c}_{31} - a_3\mathbf{c}_{13} + a_2\mathbf{c}_{32} - a_3\mathbf{c}_{23}\}$

We can assume that $\mathbf{c}_{12} = \mathbf{e}_1$ and $\mathbf{c}_{13} = \mathbf{e}_2$.

GAPN construction using the multivariate ANF

By computer search we found 83 484 GAPN functions of this type.

How many of these functions are inequivalent under $\sim_2$?

More generally, could we test efficiently (in)equivalence under $\sim_{d-1}$ for functions of degree d?

GAPN construction using the multivariate ANF

By computer search we found 83 484 GAPN functions of this type.

How many of these functions are inequivalent under $\sim_2$?

More generally, could we test efficiently (in)equivalence under $\sim_{d-1}$ for functions of degree d?

GAPN construction using the multivariate ANF

By computer search we found 83 484 GAPN functions of this type.

How many of these functions are inequivalent under $\sim_2$?

More generally, could we test efficiently (in)equivalence under $\sim_{d-1}$ for functions of degree d?

Invariants

Related use of invariants in previous work:

- Classification of APN functions under EA-equivalence: orthoderivatives [Canteaut, Couvreur, Perrin '22], etc.
- Classification of Boolean functions of degree d under $\sim_{d-1}$: [Hou '96], [Langevin, Leander '07] etc.

Invariants

Related use of invariants in previous work:

- Classification of APN functions under EA-equivalence: orthoderivatives [Canteaut, Couvreur, Perrin '22], etc.
- Classification of Boolean functions of degree d under $\sim_{d-1}$: [Hou '96], [Langevin, Leander '07] etc.

Invariants

Related use of invariants in previous work:

- Classification of APN functions under EA-equivalence: orthoderivatives [Canteaut, Couvreur, Perrin '22], etc.
- Classification of Boolean functions of degree d under $\sim_{d-1}$: [Hou '96], [Langevin, Leander '07] etc.

Invariants

Related use of invariants in previous work:

- Classification of APN functions under EA-equivalence: orthoderivatives [Canteaut, Couvreur, Perrin '22], etc.
- Classification of Boolean functions of degree d under $\sim_{d-1}$: [Hou '96], [Langevin, Leander '07] etc.

Invariants: dimension of the image of the derivative

$\deg(F) = d$

$\deg(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F) \leq 1$

The multiset $\{\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) : a_1, \ldots, a_{d-1} \in \mathbb{F}_p^n\}$ is invariant under $\sim_{d-1}$.

$\mathrm{DerIm}_F(i)$ number of derivatives of F which have image of dimension i

A refinement of this invariant:
$\mathrm{DerImProj}_F(i, j, k)$: the number of $(a_1, \ldots, a_k)$ for which there are exactly j values of $(a_{k+1}, \ldots, a_{d-1})$ such that $\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) = i$

Invariants: dimension of the image of the derivative

$\deg(F) = d$

$\deg(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F) \leq 1$

The multiset $\{\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) : a_1, \ldots, a_{d-1} \in \mathbb{F}_p^n\}$ is invariant under $\sim_{d-1}$.

$\mathrm{DerIm}_F(i)$ number of derivatives of F which have image of dimension i

A refinement of this invariant:
$\mathrm{DerImProj}_F(i, j, k)$: the number of $(a_1, \ldots, a_k)$ for which there are exactly j values of $(a_{k+1}, \ldots, a_{d-1})$ such that $\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) = i$

Invariants: dimension of the image of the derivative

$\deg(F) = d$

$\deg(\Delta^{(d-1)}_{a_1,\dots,a_{d-1}} F) \leq 1$

The multiset $\{\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\dots,a_{d-1}} F)) : a_1, \dots, a_{d-1} \in \mathbb{F}_p^n\}$ is invariant under $\sim_{d-1}$.

$\mathrm{DerIm}_F(i)$ number of derivatives of F which have image of dimension i

A refinement of this invariant:
$\mathrm{DerImProj}_F(i, j, k)$: the number of $(a_1, \dots, a_k)$ for which there are exactly j values of $(a_{k+1}, \dots, a_{d-1})$ such that $\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\dots,a_{d-1}} F)) = i$

Invariants: dimension of the image of the derivative

$\deg(F) = d$

$\deg(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F) \leq 1$

The multiset $\{\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) : a_1, \ldots, a_{d-1} \in \mathbb{F}_p^n\}$ is invariant under $\sim_{d-1}$.

$\mathrm{DerIm}_F(i)$ number of derivatives of F which have image of dimension i

A refinement of this invariant:
$\mathrm{DerImProj}_F(i, j, k)$: the number of $(a_1, \ldots, a_k)$ for which there are exactly j values of $(a_{k+1}, \ldots, a_{d-1})$ such that $\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) = i$

Invariants: dimension of the image of the derivative

$\deg(F) = d$

$\deg(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F) \leq 1$

The multiset $\{\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) : a_1, \ldots, a_{d-1} \in \mathbb{F}_p^n\}$ is invariant under $\sim_{d-1}$.

$\mathrm{DerIm}_F(i)$ number of derivatives of F which have image of dimension i

A refinement of this invariant:

$\mathrm{DerImProj}_F(i, j, k)$: the number of $(a_1, \ldots, a_k)$ for which there are exactly j values of $(a_{k+1}, \ldots, a_{d-1})$ such that $\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) = i$

Invariants: dimension of the image of the derivative

$\deg(F) = d$

$\deg(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F) \leq 1$

The multiset $\{\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) : a_1, \ldots, a_{d-1} \in \mathbb{F}_p^n\}$ is invariant under $\sim_{d-1}$.

$\mathrm{DerIm}_F(i)$ number of derivatives of F which have image of dimension i

A refinement of this invariant:
$\mathrm{DerImProj}_F(i, j, k)$: the number of $(a_1, \ldots, a_k)$ for which there are exactly j values of $(a_{k+1}, \ldots, a_{d-1})$ such that $\dim(\mathrm{Im}(\Delta^{(d-1)}_{a_1,\ldots,a_{d-1}} F)) = i$

Invariants: orthoderivatives

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

An orthoderivative of F is a function $\pi_F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\pi_F(0) = 0$ and $\pi_F(a)$ orthogonal to $\mathrm{Im}(\Delta_a F)$; moreover, if $a \neq 0$ then $\pi_F(0) \neq 0$.

If F quadratic APN function, π_F exists and is unique.

If F, G are EA-equivalent and have unique orthoderivatives, then π_F, π_G are affine equivalent [Canteaut et al, '22].

Invariants: orthoderivatives

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
An orthoderivative of F is a function $\pi_F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\pi_F(0) = 0$ and $\pi_F(a)$ orthogonal to $\mathrm{Im}(\Delta_a F)$; moreover, if $a \neq 0$ then $\pi_F(0) \neq 0$.

If F quadratic APN function, π_F exists and is unique.

If F, G are EA-equivalent and have unique orthoderivatives, then π_F, π_G are affine equivalent [Canteaut et al, '22].

Invariants: orthoderivatives

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
An orthoderivative of F is a function $\pi_F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\pi_F(0) = 0$ and $\pi_F(a)$ orthogonal to $\mathrm{Im}(\Delta_a F)$; moreover, if $a \neq 0$ then $\pi_F(0) \neq 0$.

If F quadratic APN function, π_F exists and is unique.

If F, G are EA-equivalent and have unique orthoderivatives, then π_F, π_G are affine equivalent [Canteaut et al, '22].

Invariants: orthoderivatives

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
An orthoderivative of F is a function $\pi_F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
with $\pi_F(0) = 0$ and $\pi_F(a)$ orthogonal to $\mathrm{Im}(\Delta_a F)$;
moreover, if $a \neq 0$ then $\pi_F(0) \neq 0$.

If F quadratic APN function, π_F exists and is unique.

If F, G are EA-equivalent and have unique orthoderivatives, then π_F, π_G are affine equivalent [Canteaut et al, '22].

Invariants: orthoderivatives

Proposed generalization:

An order r orthoderivative of F is any function $\pi_F^{(r)} : \mathbb{F}_{p^n}^r \to \mathbb{F}_{p^n}$
$\pi_F^{(r)}(a_1, \ldots, a_r) = v^{p-1}$ with v orthogonal to $\mathrm{Im}(\Delta^{(r)}_{a_1,a_2,\ldots,a_r} F)$; moreover, v is non-zero if a non-zero orthogonal element exists.

Note if v is orthogonal to a particular vectorspace, then so is αv for any scalar $\alpha \in \mathbb{F}_p^*$; we have $(\alpha v)^{p-1} = v^{p-1}$.

Invariants: orthoderivatives

Proposed generalization:

An order r orthoderivative of F is any function $\pi_F^{(r)} : \mathbb{F}_{p^n}^r \to \mathbb{F}_{p^n}$ $\pi_F^{(r)}(a_1, \ldots, a_r) = v^{p-1}$ with v orthogonal to $\mathrm{Im}(\Delta^{(r)}_{a_1,a_2,\ldots,a_r} F)$; moreover, v is non-zero if a non-zero orthogonal element exists.

Note if v is orthogonal to a particular vectorspace, then so is αv for any scalar $\alpha \in \mathbb{F}_p^*$; we have $(\alpha v)^{p-1} = v^{p-1}$.

Invariants: orthoderivatives

Proposed generalization:

An order r orthoderivative of F is any function $\pi_F^{(r)} : \mathbb{F}_{p^n}^r \to \mathbb{F}_{p^n}$
$\pi_F^{(r)}(a_1, \ldots, a_r) = v^{p-1}$ with v orthogonal to $\mathrm{Im}(\Delta^{(r)}_{a_1,a_2,\ldots,a_r} F)$;
moreover, v is non-zero if a non-zero orthogonal element exists.

Note if v is orthogonal to a particular vectorspace, then so is αv for any scalar $\alpha \in \mathbb{F}_p^*$; we have $(\alpha v)^{p-1} = v^{p-1}$.

Invariants: orthoderivatives

Proposition

Let $F \sim_{d-1} G$, i.e. $F = A_1 \circ G \circ A_2 + H$ for A_1, A_2 affine and bijective and $\deg(H) \leq d-1$. Then for any order $d-1$ orthoderivative $\pi_F^{(d-1)}$ of F, there exists $\pi_G^{(d-1)}$ of G such that for all $a_1, \ldots a_{d-1} \in \mathbb{F}_{p^n}^*$ we have

$$\pi_F^{(d-1)}(A_2(a_1), \ldots, A_2(a_{d-1})) = L_1^*(\pi_G^{(d-1)}(a_1, \ldots, a_{d-1})), \qquad (1)$$

where L_1^* is the adjoint operator of the linear part L_1 of A_1.

If $\pi_F^{(d-1)}$ is unique, the number of elements in $\mathrm{Im}(\pi_F^{(d-1)})$ and their multiplicities are invariant under $\sim_{d-1}$.

Invariants: orthoderivatives

Proposition

Let $F \sim_{d-1} G$, i.e. $F = A_1 \circ G \circ A_2 + H$ for A_1, A_2 affine and bijective and $\deg(H) \leq d-1$. Then for any order $d-1$ orthoderivative $\pi_F^{(d-1)}$ of F, there exists $\pi_G^{(d-1)}$ of G such that for all $a_1, \dots a_{d-1} \in \mathbb{F}_{p^n}^*$ we have

$$\pi_F^{(d-1)}(A_2(a_1), \dots, A_2(a_{d-1})) = L_1^*(\pi_G^{(d-1)}(a_1, \dots, a_{d-1})), \quad (1)$$

where L_1^* is the adjoint operator of the linear part L_1 of A_1.

If $\pi_F^{(d-1)}$ is unique, the number of elements in $\mathrm{Im}(\pi_F^{(d-1)})$ and their multiplicities are invariant under $\sim_{d-1}$.

Invariants: orthoderivatives

"Diagonalised" version of $\pi_F^{(d-1)}$:

$\tilde{\pi}_F^{(d-1)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
$\tilde{\pi}_F^{(d-1)}(a) = \pi_F^{(d-1)}(a, a, \ldots, a)$.

If F is GAPN of degree p, then $\tilde{\pi}_F^{(p-1)}$ is uniquely defined;

If $F \sim_{p-1} G$, then $\tilde{\pi}_F^{(p-1)}$ and $\tilde{\pi}_G^{(p-1)}$ are affine equivalent.

Invariants: orthoderivatives

“Diagonalised” version of $\pi_F^{(d-1)}$:

$\tilde{\pi}_F^{(d-1)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
$\tilde{\pi}_F^{(d-1)}(a) = \pi_F^{(d-1)}(a, a, \ldots, a)$.

If F is GAPN of degree p, then $\tilde{\pi}_F^{(p-1)}$ is uniquely defined;

If $F \sim_{p-1} G$, then $\tilde{\pi}_F^{(p-1)}$ and $\tilde{\pi}_G^{(p-1)}$ are affine equivalent.

Invariants: orthoderivatives

"Diagonalised" version of $\pi_F^{(d-1)}$:

$\tilde{\pi}_F^{(d-1)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
$\tilde{\pi}_F^{(d-1)}(a) = \pi_F^{(d-1)}(a, a, \ldots, a)$.

If F is GAPN of degree p, then $\tilde{\pi}_F^{(p-1)}$ is uniquely defined;

If $F \sim_{p-1} G$, then $\tilde{\pi}_F^{(p-1)}$ and $\tilde{\pi}_G^{(p-1)}$ are affine equivalent.

Invariants: orthoderivatives

"Diagonalised" version of $\pi_F^{(d-1)}$:

$\tilde{\pi}_F^{(d-1)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
$\tilde{\pi}_F^{(d-1)}(a) = \pi_F^{(d-1)}(a, a, \ldots, a)$.

If F is GAPN of degree p, then $\tilde{\pi}_F^{(p-1)}$ is uniquely defined;

If $F \sim_{p-1} G$, then $\tilde{\pi}_F^{(p-1)}$ and $\tilde{\pi}_G^{(p-1)}$ are affine equivalent.

Invariants: orthoderivatives

“Diagonalised” version of $\pi_F^{(d-1)}$:

$\tilde{\pi}_F^{(d-1)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
$\tilde{\pi}_F^{(d-1)}(a) = \pi_F^{(d-1)}(a, a, \ldots, a)$.

If F is GAPN of degree p, then $\tilde{\pi}_F^{(p-1)}$ is uniquely defined;

If $F \sim_{p-1} G$, then $\tilde{\pi}_F^{(p-1)}$ and $\tilde{\pi}_G^{(p-1)}$ are affine equivalent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with $t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with

$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with

$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with

$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with
$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d-1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with
$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with
$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with
$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

If $\deg(F) = d$

$F \sim_{d-1} G$ iff $F = L_1 \circ G \circ L_2 + H$

for some invertible linear transformations L_1, L_2 and $\deg(H) \leq d - 1$.

We now concentrate on L_1.

Write $F = \sum \mathbf{b}_i t_i$, with
$t_1, \ldots, t_{p^n}$ the monomials in decreasing degree lexicographic order.

$L_1 \circ F = \sum L_1(\mathbf{b}_i) t_i$

$\mathbf{b}_i \neq \mathbf{0}$ iff $L_1(\mathbf{b}_i) \neq \mathbf{0}$

For any fixed $i_1, \ldots, i_k$, the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in F are linearly independent if and only if the coefficients of $t_{i_1}, \ldots, t_{i_k}$ in $L_1 \circ F$ are linearly independent.

Canonical form w.r.t. left linear transformations

$F = \sum \mathbf{b}_i t_i$

$$\begin{array}{ll} \mathbf{0} & \\ \vdots & \\ \mathbf{0} & \\ \mathbf{b}_{i_1} & \\ \vdots & \in \langle \mathbf{b}_{i_1} \rangle \\ \mathbf{b}_{i_2} & \notin \langle \mathbf{b}_{i_1} \rangle \\ \vdots & \in \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\ \mathbf{b}_{i_3} & \notin \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\ \vdots & \end{array}$$

We say that F is in canonical form w.r.t. left linear transformations if $\mathbf{b}_{i_1} = \mathbf{e}_1, \mathbf{b}_{i_2} = \mathbf{e}_2, \ldots$

Canonical form w.r.t. left linear transformations

$F = \sum \mathbf{b}_i t_i$

$$
\begin{array}{cl}
\mathbf{0} & \\
\vdots & \\
\mathbf{0} & \\
\mathbf{b}_{i_1} & \\
\vdots & \in \langle \mathbf{b}_{i_1} \rangle \\
\mathbf{b}_{i_2} & \not\in \langle \mathbf{b}_{i_1} \rangle \\
\vdots & \in \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\
\mathbf{b}_{i_3} & \not\in \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\
\vdots &
\end{array}
$$

We say that F is in canonical form w.r.t. left linear transformations if $\mathbf{b}_{i_1} = \mathbf{e}_1, \mathbf{b}_{i_2} = \mathbf{e}_2, \ldots$

Canonical form w.r.t. left linear transformations

$F = \sum \mathbf{b}_i t_i$

$$\begin{array}{ll}
\mathbf{0} & \\
\vdots & \\
\mathbf{0} & \\
\mathbf{b}_{i_1} & \\
\vdots & \in \langle \mathbf{b}_{i_1} \rangle \\
\mathbf{b}_{i_2} & \notin \langle \mathbf{b}_{i_1} \rangle \\
\vdots & \in \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\
\mathbf{b}_{i_3} & \notin \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\
\vdots &
\end{array}$$

We say that F is in canonical form w.r.t. left linear transformations if $\mathbf{b}_{i_1} = \mathbf{e}_1, \mathbf{b}_{i_2} = \mathbf{e}_2, \ldots$

Canonical form w.r.t. left linear transformations

$F = \sum \mathbf{b}_i t_i$

$$\begin{array}{ll} \mathbf{0} & \\ \vdots & \\ \mathbf{0} & \\ \mathbf{b}_{i_1} & \\ \vdots & \in \langle \mathbf{b}_{i_1} \rangle \\ \mathbf{b}_{i_2} & \notin \langle \mathbf{b}_{i_1} \rangle \\ \vdots & \in \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\ \mathbf{b}_{i_3} & \notin \langle \mathbf{b}_{i_1}, \mathbf{b}_{i_2} \rangle \\ \vdots & \end{array}$$

We say that F is in canonical form w.r.t. left linear transformations if $\mathbf{b}_{i_1} = \mathbf{e}_1, \mathbf{b}_{i_2} = \mathbf{e}_2, \ldots$

Canonical form w.r.t. left linear transformations

For any F, the canonical form of F is the unique function G in canonical form in the set of functions $\{L \circ F : L \text{ linear and invertible}\}$;

G can be computed efficiently as $L_1 \circ F$
with L_1 any bijective linear transformation with $L_1(\mathbf{c}_{i_j}) = \mathbf{e_j}$ for $j = 1, \ldots, k$.

Remark The canonical form has the lexicographically smallest list of coefficients.

[Kalgin, Idrisova, '20] used the lexicographically smallest list of coefficients for the matrix associated to APN functions.

Canonical form w.r.t. left linear transformations

For any F, the canonical form of F is the unique function G in canonical form in the set of functions $\{L \circ F : L \text{ linear and invertible}\}$;

G can be computed efficiently as $L_1 \circ F$
with L_1 any bijective linear transformation with $L_1(\mathbf{c}_{i_j}) = \mathbf{e_j}$ for $j = 1, \ldots, k$.

Remark The canonical form has the lexicographically smallest list of coefficients.

[Kalgin, Idrisova, '20] used the lexicographically smallest list of coefficients for the matrix associated to APN functions.

Canonical form w.r.t. left linear transformations

For any F, the canonical form of F is the unique function G in canonical form in the set of functions $\{L \circ F : L \text{ linear and invertible}\}$;

G can be computed efficiently as $L_1 \circ F$
with L_1 any bijective linear transformation with $L_1(\mathbf{c}_{i_j}) = \mathbf{e_j}$ for $j = 1, \ldots, k$.

Remark The canonical form has the lexicographically smallest list of coefficients.

[Kalgin, Idrisova, '20] used the lexicographically smallest list of coefficients for the matrix associated to APN functions.

Canonical form w.r.t. left linear transformations

For any F, the canonical form of F is the unique function G in canonical form in the set of functions $\{L \circ F : L \text{ linear and invertible}\}$;

G can be computed efficiently as $L_1 \circ F$
with L_1 any bijective linear transformation with $L_1(\mathbf{c}_{i_j}) = \mathbf{e_j}$ for $j = 1, \ldots, k$.

Remark The canonical form has the lexicographically smallest list of coefficients.

[Kalgin, Idrisova, '20] used the lexicographically smallest list of coefficients for the matrix associated to APN functions.

Canonical form w.r.t. left linear transformations

For any F, the canonical form of F is the unique function G in canonical form in the set of functions $\{L \circ F : L \text{ linear and invertible}\}$;

G can be computed efficiently as $L_1 \circ F$
with L_1 any bijective linear transformation with $L_1(\mathbf{c}_{i_j}) = \mathbf{e_j}$ for $j = 1, \ldots, k$.

Remark The canonical form has the lexicographically smallest list of coefficients.

[Kalgin, Idrisova, '20] used the lexicographically smallest list of coefficients for the matrix associated to APN functions.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

GAPN functions over $\mathbb{F}_3^3$

We only compute GAPN functions in canonical form w.r.t. left linear transformations.

83 484 functions $\rightarrow$ 4 638 functions in canonical form

Invariants based on dimension of the image of the derivative distinguish 10 sets of inequivalent functions.

Invariants based on orthoderivatives distinguish the same 10 sets.

Size of sets: 56, 420, 912, 1188, 720, 270, 264, 480, 312, 16.

Classifying GAPN functions

Within each set $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, determine representatives for each class under $\sim_2$.

while $\mathcal{C}_i \neq \emptyset$
  choose $F \in \mathcal{C}_i$ and declare F a representative
  for all the possible L_2
    compute the canonical form of $F \circ L_2$ and remove it from $\mathcal{C}_i$
end while

Note that there are 11 232 possible L_1.
If we had tested $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2), there would be $(11\ 232)^2$ combinations, so the savings are significant.

Result: **31 classes!**

Classifying GAPN functions

Within each set $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, determine representatives for each class under $\sim_2$.

while $\mathcal{C}_i \neq \emptyset$
  choose $F \in \mathcal{C}_i$ and declare F a representative
  for all the possible L_2
    compute the canonical form of $F \circ L_2$ and remove it from $\mathcal{C}_i$
end while

Note that there are 11 232 possible L_1.
If we had tested $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2), there would be $(11\ 232)^2$ combinations, so the savings are significant.

Result: **31 classes!**

Classifying GAPN functions

Within each set $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, determine representatives for each class under $\sim_2$.

while $\mathcal{C}_i \neq \emptyset$
  choose $F \in \mathcal{C}_i$ and declare F a representative
  for all the possible L_2
    compute the canonical form of $F \circ L_2$ and remove it from $\mathcal{C}_i$
end while

Note that there are 11 232 possible L_1.
If we had tested $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2), there would be $(11\ 232)^2$ combinations, so the savings are significant.

Result: **31 classes!**

Classifying GAPN functions

Within each set $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, determine representatives for each class under $\sim_2$.

while $\mathcal{C}_i \neq \emptyset$
  choose $F \in \mathcal{C}_i$ and declare F a representative
  for all the possible L_2
    compute the canonical form of $F \circ L_2$ and remove it from $\mathcal{C}_i$
end while

Note that there are 11 232 possible L_1.
If we had tested $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2), there would be $(11\ 232)^2$ combinations, so the savings are significant.

Result: **31 classes!**

Classifying GAPN functions

Within each set $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, determine representatives for each class under $\sim_2$.

while $\mathcal{C}_i \neq \emptyset$
  choose $F \in \mathcal{C}_i$ and declare F a representative
  for all the possible L_2
    compute the canonical form of $F \circ L_2$ and remove it from $\mathcal{C}_i$
end while

Note that there are 11 232 possible L_1.
If we had tested $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2), there would be $(11\ 232)^2$ combinations, so the savings are significant.

Result: **31 classes!**

Classifying GAPN functions

Within each set $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, determine representatives for each class under $\sim_2$.

while $\mathcal{C}_i \neq \emptyset$
  choose $F \in \mathcal{C}_i$ and declare F a representative
  for all the possible L_2
    compute the canonical form of $F \circ L_2$ and remove it from $\mathcal{C}_i$
end while

Note that there are 11 232 possible L_1.
If we had tested $L_1 \circ F \circ L_2$ for all pairs (L_1, L_2), there would be $(11\ 232)^2$ combinations, so the savings are significant.

Result: **31 classes!**

Classifying GAPN functions

List of $(\mathbf{c}_{12}, \mathbf{c}_{13}, \mathbf{c}_{21}, \mathbf{c}_{23}, \mathbf{c}_{31}, \mathbf{c}_{32})$
ξ primitive in $\mathbb{F}_{3^3}$ satisfying $\xi^3 + 2\xi + 1 = 0$

$(1, \xi, \xi^2, \xi, \xi^2, \xi^3)$	$(1, \xi, \xi^2, \xi, \xi^2, \xi^6)$	$(1, \xi, \xi^2, \xi, \xi^2, \xi^9)$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^2)$
$(1, \xi, \xi^2, \xi, \xi^3, \xi^8)$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^{15})$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^{18})$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^{21})$
$(1, \xi, \xi^2, \xi, \xi^4, \xi^6)$	$(1, \xi, \xi^2, \xi, \xi^6, \xi^{22})$	$(1, \xi, \xi^2, \xi, \xi^8, \xi^{12})$	$(1, \xi, \xi^2, \xi, \xi^8, \xi^{25})$
$(1, \xi, \xi^2, \xi, 2, \xi^2)$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^7)$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{12})$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{19})$
$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{22})$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{25})$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^5)$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^9)$
$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^{10})$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^{18})$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^{25})$	$(1, \xi, \xi^2, \xi^3, \xi^6, \xi^5)$
$(1, \xi, \xi^2, \xi^3, \xi^8, \xi^2)$	$(1, \xi, \xi^2, \xi^3, \xi^8, \xi^{19})$	$(1, \xi, \xi^2, \xi^3, \xi^9, \xi)$	$(1, \xi, \xi^2, \xi^3, \xi^{11}, \xi^5)$
$(1, \xi, \xi^2, \xi^4, \xi^8, \xi^2)$	$(1, \xi, \xi^2, \xi^8, \xi^3, \xi^{10})$	$(1, \xi, \xi^2, \xi^8, \xi^9, \xi^{17})$	

Classifying GAPN functions

List of $(\mathbf{c}_{12}, \mathbf{c}_{13}, \mathbf{c}_{21}, \mathbf{c}_{23}, \mathbf{c}_{31}, \mathbf{c}_{32})$
ξ primitive in $\mathbb{F}_{3^3}$ satisfying $\xi^3 + 2\xi + 1 = 0$

$(1, \xi, \xi^2, \xi, \xi^2, \xi^3)$	$(1, \xi, \xi^2, \xi, \xi^2, \xi^6)$	$(1, \xi, \xi^2, \xi, \xi^2, \xi^9)$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^2)$
$(1, \xi, \xi^2, \xi, \xi^3, \xi^8)$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^{15})$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^{18})$	$(1, \xi, \xi^2, \xi, \xi^3, \xi^{21})$
$(1, \xi, \xi^2, \xi, \xi^4, \xi^6)$	$(1, \xi, \xi^2, \xi, \xi^6, \xi^{22})$	$(1, \xi, \xi^2, \xi, \xi^8, \xi^{12})$	$(1, \xi, \xi^2, \xi, \xi^8, \xi^{25})$
$(1, \xi, \xi^2, \xi, 2, \xi^2)$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^7)$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{12})$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{19})$
$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{22})$	$(1, \xi, \xi^2, \xi^3, \xi^3, \xi^{25})$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^5)$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^9)$
$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^{10})$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^{18})$	$(1, \xi, \xi^2, \xi^3, \xi^4, \xi^{25})$	$(1, \xi, \xi^2, \xi^3, \xi^6, \xi^5)$
$(1, \xi, \xi^2, \xi^3, \xi^8, \xi^2)$	$(1, \xi, \xi^2, \xi^3, \xi^8, \xi^{19})$	$(1, \xi, \xi^2, \xi^3, \xi^9, \xi)$	$(1, \xi, \xi^2, \xi^3, \xi^{11}, \xi^5)$
$(1, \xi, \xi^2, \xi^4, \xi^8, \xi^2)$	$(1, \xi, \xi^2, \xi^8, \xi^3, \xi^{10})$	$(1, \xi, \xi^2, \xi^8, \xi^9, \xi^{17})$	

Summary

- Invariants for testing inequivalence under $\sim_{d-1}$ for vectorial Boolean functions of degree d
- Canonical form w.r.t. left linear transformations
- Classification of certain GAPN functions over $\mathbb{F}_3^3$.

Summary

- Invariants for testing inequivalence under $\sim_{d-1}$ for vectorial Boolean functions of degree d
- Canonical form w.r.t. left linear transformations
- Classification of certain GAPN functions over $\mathbb{F}_3^3$.

Summary

- Invariants for testing inequivalence under $\sim_{d-1}$ for vectorial Boolean functions of degree d
- Canonical form w.r.t. left linear transformations
- Classification of certain GAPN functions over $\mathbb{F}_3^3$.

Summary

- Invariants for testing inequivalence under $\sim_{d-1}$ for vectorial Boolean functions of degree d
- Canonical form w.r.t. left linear transformations
- Classification of certain GAPN functions over $\mathbb{F}_3^3$.

Summary

- Invariants for testing inequivalence under $\sim_{d-1}$ for vectorial Boolean functions of degree d
- Canonical form w.r.t. left linear transformations
- Classification of certain GAPN functions over $\mathbb{F}_3^3$.

Further work

- Further study of invariants for $\sim_{d-1}$ and the relationship between different invariants
- Classification of all GAPN functions over $\mathbb{F}_3^3$, including the ones that contain $x_1 x_2 x_3$
- Classification of GAPN functions over $\mathbb{F}_5^5$

Further work

- Further study of invariants for $\sim_{d-1}$ and the relationship between different invariants
- Classification of all GAPN functions over $\mathbb{F}_3^3$, including the ones that contain $x_1 x_2 x_3$
- Classification of GAPN functions over $\mathbb{F}_5^5$

Further work

- Further study of invariants for $\sim_{d-1}$ and the relationship between different invariants
- Classification of all GAPN functions over $\mathbb{F}_3^3$, including the ones that contain $x_1 x_2 x_3$
- Classification of GAPN functions over $\mathbb{F}_5^5$

Further work

- Further study of invariants for $\sim_{d-1}$ and the relationship between different invariants
- Classification of all GAPN functions over $\mathbb{F}_3^3$, including the ones that contain $x_1 x_2 x_3$
- Classification of GAPN functions over $\mathbb{F}_5^5$

Further work

- Further study of invariants for $\sim_{d-1}$ and the relationship between different invariants
- Classification of all GAPN functions over $\mathbb{F}_3^3$, including the ones that contain $x_1x_2x_3$
- Classification of GAPN functions over $\mathbb{F}_5^5$