Boolean bent functions in impossible cases: odd and plane dimensions

Laurent Poinsot

Université du Sud Toulon-Var

SAR/SSI 2006

Outline

Outline

1. Boolean bent functions : traditional approach
   - What is a Boolean bent function ?
   - Applications for such functions
2. Boolean bent functions : Group actions based approach
   - Basics on group actions
   - Group actions ”bent” functions
   - ”Bent” functions in impossible cases
   - Application

Outline

1. Boolean bent functions : traditional approach
   - What is a Boolean bent function ?
   - Applications for such functions
2. Boolean bent functions : Group actions based approach
   - Basics on group actions
   - Group actions "bent" functions
   - "Bent" functions in impossible cases
   - Application

Some notations

Let $GF(2) = \{0, 1\}$ be the finite field with two elements. We denote by V_m any m-dimensional vector space over $GF(2)$.
V_m will be interpreted as $GF(2)^m$, the vector space of m-tuples, or as $GF(2^m)$ the finite field with 2^m elements.

Some notations

Let $GF(2) = \{0, 1\}$ be the finite field with two elements. We denote by V_m any m-dimensional vector space over $GF(2)$. V_m will be interpreted as $GF(2)^m$, the vector space of m-tuples, or as $GF(2^m)$ the finite field with 2^m elements.

Let G be a finite Abelian group. For instance $G = V_m$, $G = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ or $G = GF(2^m)^*$.

Definition

A Boolean function is a (mathematical) mapping f from G to V_n. A Boolean function $f : G \to V_n$ is called bent if its Fourier spectrum contains all the possible frequencies.

Let G be a finite Abelian group. For instance $G = V_m$, $G = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ or $G = GF(2^m)^*$.

Definition

A Boolean function is a (mathematical) mapping f from G to V_n.
A Boolean function $f : G \to V_n$ is called bent if its Fourier spectrum contains all the possible frequencies.

Let G be a finite Abelian group. For instance $G = V_m$, $G = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ or $G = GF(2^m)^*$.

Definition

A Boolean function is a (mathematical) mapping f from G to V_n. A Boolean function $f : G \to V_n$ is called bent if its Fourier spectrum contains all the possible frequencies.

Alternative definition : perfect nonlinearity

Definition

A function $f : G \rightarrow V_n$ is called perfect nonlinear if for each nonzero α in G and for each $\beta \in V_n$,

$$|\{x \in G | f(\alpha + x) \oplus f(x) = \beta\}| = \frac{|G|}{2^n} .$$

Theorem (Dillon 1976, Rothaus 1974, Carlet & Ding 2004)

A function f is bent if and only if f is perfect nonlinear.

Alternative definition : perfect nonlinearity

Definition

A function $f : G \rightarrow V_n$ is called perfect nonlinear if for each nonzero α in G and for each $\beta \in V_n$,

$$|\{x \in G | f(\alpha + x) \oplus f(x) = \beta\}| = \frac{|G|}{2^n} .$$

Theorem (Dillon 1976, Rothaus 1974, Carlet & Ding 2004)

A function f is bent if and only if f is perfect nonlinear.

Example

The function $f : GF(2)^4 \to GF(2)$ defined by

$$f(x_1, x_2, x_3, x_4) = (x_1, x_2).(x_3, x_4) = x_1 x_3 \oplus x_2 x_4$$

is bent.

Nonexistence results : impossible cases

- Odd dimension : If m is an odd integer, there is no bent function f from V_m to V_n (for any n) ;
- Plane dimension : For any integer m, there is no bent function f from V_m to itself ;
- Nevertheless in this contribution are constructed "bent" functions in these cases !

Nonexistence results : impossible cases

- Odd dimension : If m is an odd integer, there is no bent function f from V_m to V_n (for any n) ;
- Plane dimension : For any integer m, there is no bent function f from V_m to itself ;
- Nevertheless in this contribution are constructed "bent" functions in these cases !

Nonexistence results : impossible cases

- Odd dimension : If m is an odd integer, there is no bent function f from V_m to V_n (for any n) ;
- Plane dimension : For any integer m, there is no bent function f from V_m to itself ;
- Nevertheless in this contribution are constructed "bent" functions in these cases !

Nonexistence results : impossible cases

- Odd dimension : If m is an odd integer, there is no bent function f from V_m to V_n (for any n) ;
- Plane dimension : For any integer m, there is no bent function f from V_m to itself ;
- Nevertheless in this contribution are constructed "bent" functions in these cases !

Outline

- Cryptography ;
- Mobile communications.

- Cryptography ;
- Mobile communications.

- Cryptography ;
- Mobile communications.

Cryptography (I/IV) : DES-like cryptosystem

Let M be the plaintext and f be a mapping. An encryption using a DES-like cryptosystem consists in the iterative process

- $X_0 := M$;
- $X_i := f(K_i + X_{i-1})$ for $n \geq i > 0$.

By definition the ciphertext is $C := X_n$.

Cryptography (I/IV) : DES-like cryptosystem

Let M be the plaintext and f be a mapping. An encryption using a DES-like cryptosystem consists in the iterative process

- $X_0 := M$;
- $X_i := f(K_i + X_{i-1})$ for $n \geq i > 0$.

By definition the ciphertext is $C := X_n$.

Cryptography (I/IV) : DES-like cryptosystem

Let M be the plaintext and f be a mapping. An encryption using a DES-like cryptosystem consists in the iterative process

- $X_0 := M$;
- $X_i := f(K_i + X_{i-1})$ for $n \geq i > 0$.

By definition the ciphertext is $C := X_n$.

Cryptography (II/II) : Differential and linear attacks

- Biham & Shamir's Differential attack takes advantage of a possible weakness of the DES-like cryptosystem in a first-order derivation ;
- Matsui's linear attack exploits the possible existence of an approximation of the entire cryptosystem by a linear function ;
- The resistance of DES-like cryptosystem relies on the mapping f used.

The mappings f that offer the best resistance against the differential and linear attacks are exactly the bent functions.

Cryptography (II/II) : Differential and linear attacks

- Biham & Shamir's Differential attack takes advantage of a possible weakness of the DES-like cryptosystem in a first-order derivation ;
- Matsui's linear attack exploits the possible existence of an approximation of the entire cryptosystem by a linear function ;
- The resistance of DES-like cryptosystem relies on the mapping f used.

The mappings f that offer the best resistance against the differential and linear attacks are exactly the bent functions.

Cryptography (II/II) : Differential and linear attacks

- Biham & Shamir's Differential attack takes advantage of a possible weakness of the DES-like cryptosystem in a first-order derivation ;
- Matsui's linear attack exploits the possible existence of an approximation of the entire cryptosystem by a linear function ;
- The resistance of DES-like cryptosystem relies on the mapping f used.

The mappings f that offer the best resistance against the differential and linear attacks are exactly the bent functions.

Cryptography (II/II) : Differential and linear attacks

- Biham & Shamir's Differential attack takes advantage of a possible weakness of the DES-like cryptosystem in a first-order derivation ;
- Matsui's linear attack exploits the possible existence of an approximation of the entire cryptosystem by a linear function ;
- The resistance of DES-like cryptosystem relies on the mapping f used.

The mappings f that offer the best resistance against the differential and linear attacks are exactly the bent functions.

Cryptography (II/II) : Differential and linear attacks

- Biham & Shamir's Differential attack takes advantage of a possible weakness of the DES-like cryptosystem in a first-order derivation ;
- Matsui's linear attack exploits the possible existence of an approximation of the entire cryptosystem by a linear function ;
- The resistance of DES-like cryptosystem relies on the mapping f used.

The mappings f that offer the best resistance against the differential and linear attacks are exactly the bent functions.

Mobile communications (I/V) : Code Division Multiple Access (CDMA)

Definition

Two vectors $u = (u_1, \dots, u_m)$ and $v = (v_1, \dots, v_m)$ are called orthogonal if

$$u.v = \sum_{i=1}^{m} u_i v_i = 0 \ .$$

For instance $u = (1, 1, 1, -1)$ and $v = (1, -1, 1, 1)$ are othogonal.

Mobile communications (II/V) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (II/V) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (II/V) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (II/V) : CDMA

- V : set of mutually orthogonal vectors ;
- Each sender S_x has a different, unique vector $x \in V$ called chip code.
  For instance S_u has $u = (1, 1, 1, -1)$ and S_v has $v = (1, -1, 1, 1)$;
- Objective : Simultaneous transmission of messages by several senders on the same channel (multiplexing).

Mobile communications (III/V) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (III/V) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (III/V) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (III/V) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (III/V) : CDMA

- S_u wants to send $d_u = (1, 0, 1)$ and S_v wants to send $d_v = (0, 0, 1)$;
- S_u computes its transmitted vector by coding d_u with the rules $0 \leftrightarrow -u$, $1 \leftrightarrow u$. He obtains $(u, -u, u)$;
- S_v computes $(-v, -v, v)$;
- The message sent on the channel is $(u - v, -u - v, u + v)$.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communications (IV/V) : CDMA

- A receiver gets the message $M = (u - v, -u - v, u + v)$ and he needs to recover d_u and/or d_v ;
- How to recover d_u ?
  - Take the first component of M, $u - v$ and compute the dot-product with u : $(u - v).u = u.u - v.u = 4$. Since this is positive, we can deduce that a one digit was sent ;
  - Take the second component of M, $-u - v$ and $(-u - v).u = -u.u - v.u = -4$. Since this is negative, we can deduce that a zero digit was sent ;
  - Continuing in this fashion with the third component, the receiver successfully decodes d_u ;
- Likewise, applying the same process with chip code v, the receiver finds the message of S_v.

Mobile communication (V/V) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \ldots, f(\alpha + m - 1)) .$$

In particular $u_0 = (f(0), f(1), \ldots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Mobile communication (V/V) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \ldots, f(\alpha + m - 1)) \ .$$

In particular $u_0 = (f(0), f(1), \ldots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Mobile communication (V/V) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha + 1), \dots, f(\alpha + m - 1)) \ .$$

In particular $u_0 = (f(0), f(1), \dots, f(m - 1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Mobile communication (V/V) : CDMA

Let $f : \mathbb{Z}_m \to \{0, 1\}$ be a bent function.
For each $\alpha \in \mathbb{Z}_m$, we define a vector :

$$u_\alpha = (f(\alpha), f(\alpha+1), \ldots, f(\alpha+m-1)) \ .$$

In particular $u_0 = (f(0), f(1), \ldots, f(m-1))$.
Then $\{u_\alpha | \alpha \in \mathbb{Z}_m\}$ is a set of mutually orthogonal vectors.

Outline

1. Boolean bent functions : traditional approach
   - What is a Boolean bent function ?
   - Applications for such functions
2. Boolean bent functions : Group actions based approach
   - Basics on group actions
   - Group actions ”bent” functions
   - ”Bent” functions in impossible cases
   - Application

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Let X be any nonempty set. We denote by $S(X)$ the symmetric group of X.

Definition

Let G be any group. An action of G on X is a group homomorphism Φ from G to $S(X)$.

Write $g.x$ instead of $\Phi(g)(x)$ for $g \in G$ and $x \in X$.

Examples

- A group G acts on itself by translation : $\alpha.x = \alpha + x$;
- Let G and H be two groups. G acts on $G \times H$ by $\alpha.(x, y) = (\alpha + x, y)$;
- Let W be a sub-vector space of V. W acts on V by translation : $\alpha.x = \alpha + x$;
- Let $\mathbb{K}$ be any field. Then $\mathbb{K}^*$ acts on $\mathbb{K}$ by $\alpha.x = \alpha x$.

Outline

Alternative definition (recall)

A function $f : G \to V_n$ is bent if for each nonzero α in G and for each $\beta \in V_n$,

$$|\{x \in G | f(\alpha + x) \oplus f(x) = \beta\}| = \frac{|G|}{2^n} .$$

Definition

Let G be a finite Abelian group acting on a finite nonempty set X. A function $f : X \rightarrow V_n$ is G-bent if for each nonzero $\alpha \in G$ and for each $\beta \in V_n$,

$$|\{x \in X | f(\alpha.x) \oplus f(x) = \beta\}| = \frac{|X|}{2^n} .$$

In particular a classical bent function $f : G \rightarrow V_n$ should be called a G-bent function in this new framework, where the considered group action is the action of G on itself by translation.

Definition

Let G be a finite Abelian group acting on a finite nonempty set X. A function $f : X \to V_n$ is G-bent if for each nonzero $\alpha \in G$ and for each $\beta \in V_n$,

$$|\{x \in X | f(\alpha . x) \oplus f(x) = \beta\}| = \frac{|X|}{2^n} .$$

In particular a classical bent function $f : G \to V_n$ should be called a G-bent function in this new framework, where the considered group action is the action of G on itself by translation.

Outline

Odd dimension

Theorem

Let m and n be two odd integers. Then it is possible to construct a function $f : V_{2m+n} \to \{0,1\}$ which is V_n-bent.

Remark

Because m and n are odd integers there is no classical bent function from V_{2m+n} to $\{0,1\}$ or also from V_n to $\{0,1\}$.

Odd dimension

Theorem

Let m and n be two odd integers. Then it is possible to construct a function $f : V_{2m+n} \rightarrow \{0, 1\}$ which is V_n-bent.

Remark

Because m and n are odd integers there is no classical bent function from V_{2m+n} to $\{0, 1\}$ or also from V_n to $\{0, 1\}$.

Odd dimension

Theorem

Let m and n be two odd integers. Then it is possible to construct a function $f : V_{2m+n} \to \{0, 1\}$ which is V_n-bent.

Remark

Because m and n are odd integers there is no classical bent function from V_{2m+n} to $\{0, 1\}$ or also from V_n to $\{0, 1\}$.

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-bent.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{(\alpha \oplus 1)} \end{array}$$

$\square$

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-bent.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{(\alpha \oplus 1)} \end{array}$$

$\square$

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-bent.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

$$\begin{array}{rrcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{(\alpha \oplus 1)} \end{array}$$

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-bent.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

$$
\begin{array}{rlcl}
 & f(\alpha.x) \oplus f(x) & = & \beta \\
\Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\
\Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\
\Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{(\alpha \oplus 1)}
\end{array}
$$

Plane dimension

Theorem

Let $f : GF(2^m) \rightarrow GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-bent.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{(\alpha \oplus 1)} \end{array}$$

Plane dimension

Theorem

Let $f : GF(2^m) \to GF(2^m)$ be a field automorphism. Then f is $GF(2^m)^*$-bent.

Proof

Let $x \in GF(2^m)$ and $\alpha \in GF(2^m)^*$, $\alpha \neq 1$. Let $\beta \in GF(2^m)$.

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & f(\alpha x \oplus x) & = & \beta \\ \Leftrightarrow & (\alpha \oplus 1)x & = & f^{-1}(\beta) \\ \Leftrightarrow & x & = & \dfrac{f^{-1}(\beta)}{(\alpha \oplus 1)} \end{array}$$

$\square$

Outline

We call a cylic bent function, a bent function $f : \mathbb{Z}_m \to \{0, 1\}$.

The only known examples of such cyclic bent functions occur when $m = 4$. It is widely conjectured that this is actually the only case.

Theorem

Let m be an even integer. Then it exists a $GF(2)^m$-bent function $f : \mathbb{Z}_{2^m} \to \{0, 1\}$.

If $m \neq 2$ then (it is conjectured that) f can not be a classical bent function.

We call a cylic bent function, a bent function $f : \mathbb{Z}_m \to \{0, 1\}$. The only known examples of such cyclic bent functions occur when $m = 4$. It is widely conjectured that this is actually the only case.

Theorem

Let m be an even integer. Then it exists a $GF(2)^m$-bent function $f : \mathbb{Z}_{2^m} \to \{0, 1\}$.

If $m \neq 2$ then (it is conjectured that) f can not be a classical bent function.

We call a cylic bent function, a bent function $f : \mathbb{Z}_m \to \{0,1\}$. The only known examples of such cyclic bent functions occur when $m = 4$. It is widely conjectured that this is actually the only case.

Theorem

Let m be an even integer. Then it exists a $GF(2)^m$-bent function $f : \mathbb{Z}_{2^m} \to \{0,1\}$.

If $m \neq 2$ then (it is conjectured that) f can not be a classical bent function.

We call a cylic bent function, a bent function $f : \mathbb{Z}_m \rightarrow \{0, 1\}$. The only known examples of such cyclic bent functions occur when $m = 4$. It is widely conjectured that this is actually the only case.

Theorem

Let m be an even integer. Then it exists a $GF(2)^m$-bent function $f : \mathbb{Z}_{2^m} \rightarrow \{0, 1\}$.

If $m \neq 2$ then (it is conjectured that) f can not be a classical bent function.

Proof

- Definition of the group action of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  We transport the action by translation of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  $$\alpha.x = \Theta(\alpha \oplus \Theta^{-1}(x))$$
  where Θ is the usual radix-two representation of an integer ;
- Let choose $g : GF(2)^m \to \{0,1\}$ be a (traditional) bent function (succh a function exists since m is an even integer). We define the function
  $$\begin{array}{rccl} f : & \mathbb{Z}_{2^m} & \to & \{0,1\} \\ & x & \mapsto & g(\Theta^{-1}(x)) \,. \end{array}$$

Proof

- Definition of the group action of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  We transport the action by translation of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  $$\alpha.x = \Theta(\alpha \oplus \Theta^{-1}(x))$$
  where Θ is the usual radix-two representation of an integer ;
- Let choose $g : GF(2)^m \to \{0,1\}$ be a (traditional) bent function (succh a function exists since m is an even integer). We define the function
  $$\begin{array}{rccc} f : & \mathbb{Z}_{2^m} & \to & \{0,1\} \\ & x & \mapsto & g(\Theta^{-1}(x)) \, . \end{array}$$

Proof

- Definition of the group action of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  We transport the action by translation of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:

  $$\alpha.x = \Theta(\alpha \oplus \Theta^{-1}(x))$$

  where Θ is the usual radix-two representation of an integer ;
- Let choose $g : GF(2)^m \to \{0,1\}$ be a (traditional) bent function (succh a function exists since m is an even integer). We define the function

  $$\begin{array}{llll} f : & \mathbb{Z}_{2^m} & \to & \{0,1\} \\ & x & \mapsto & g(\Theta^{-1}(x)) . \end{array}$$

Proof

- Definition of the group action of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  We transport the action by translation of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:

$$\alpha . x = \Theta(\alpha \oplus \Theta^{-1}(x))$$

  where Θ is the usual radix-two representation of an integer ;
- Let choose $g : GF(2)^m \to \{0, 1\}$ be a (traditional) bent function (succh a function exists since m is an even integer). We define the function

$$\begin{array}{llll} f : & \mathbb{Z}_{2^m} & \to & \{0,1\} \\ & x & \mapsto & g(\Theta^{-1}(x)) \,. \end{array}$$

Proof

- Definition of the group action of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:
  We transport the action by translation of $GF(2)^m$ on $\mathbb{Z}_{2^m}$:

$$\alpha.x = \Theta(\alpha \oplus \Theta^{-1}(x))$$

  where Θ is the usual radix-two representation of an integer ;
- Let choose $g : GF(2)^m \to \{0,1\}$ be a (traditional) bent function (succh a function exists since m is an even integer). We define the function

$$\begin{array}{rccl} f: & \mathbb{Z}_{2^m} & \to & \{0,1\} \\ & x & \mapsto & g(\Theta^{-1}(x)) \, . \end{array}$$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta\ . \end{array}$$

$\square$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta\,. \end{array}$$

$\square$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta\,. \end{array}$$

$\square$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$
\begin{array}{rlcl}
 & f(\alpha.x) \oplus f(x) & = & \beta \\
\Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\
\Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\
\Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\
\Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta\ .
\end{array}
$$

$\square$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta\ . \end{array}$$

$\square$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$\begin{array}{rlcl} & f(\alpha.x) \oplus f(x) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\ \Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta . \end{array}$$

$\square$

Proof (cont'd)

- Let show that f is $GF(2)^m$-bent :

$$
\begin{array}{rlcl}
 & f(\alpha.x) \oplus f(x) & = & \beta \\
\Leftrightarrow & g(\Theta^{-1}(\alpha.x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\
\Leftrightarrow & g(\Theta^{-1}(\Theta(\alpha \oplus \Theta^{-1}(x))) \oplus g(\Theta^{-1}(x)) & = & \beta \\
\Leftrightarrow & g(\alpha \oplus \Theta^{-1}(x)) \oplus g(\Theta^{-1}(x)) & = & \beta \\
\Leftrightarrow & g(\alpha \oplus y) \oplus g(y) & = & \beta\ .
\end{array}
$$

$\square$