Fonctions Booléennes Courbes dans les Cas Impossibles : les Dimensions Impaires et Planes

Laurent Poinsot

Université du Sud Toulon-Var (France)

Journées C2 2006

Plan

Plan

Plan

Plan

Plan de la présentation

Systèmes de chiffrement itérés par blocs

- Dans un système de chiffrement par blocs les messages clairs et chiffrés sont considérés comme des blocs de bits de taille identique ;
- Dans un système de chiffrement par blocs à r tours le bloc chiffré x_r est obtenu à partir d'un bloc de clair x_0 par r itérations d'une fonction de tour T

$$x_i = T(x_{i-1}, k_i)\ 1 \leq i \leq r$$

où k_i est la (sous-)clef du ième tour ;
- Exemples : Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) ou l'Advanced Encryption Standard (AES).

Systèmes de chiffrement itérés par blocs

- Dans un système de chiffrement par blocs les messages clairs et chiffrés sont considérés comme des blocs de bits de taille identique ;
- Dans un système de chiffrement par blocs à r tours le bloc chiffré x_r est obtenu à partir d'un bloc de clair x_0 par r itérations d'une fonction de tour T

$$x_i = T(x_{i-1}, k_i)\ 1 \leq i \leq r$$

où k_i est la (sous-)clef du ième tour ;
- Exemples : Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) ou l'Advanced Encryption Standard (AES).

Systèmes de chiffrement itérés par blocs

- Dans un système de chiffrement par blocs les messages clairs et chiffrés sont considérés comme des blocs de bits de taille identique ;
- Dans un système de chiffrement par blocs à r tours le bloc chiffré x_r est obtenu à partir d'un bloc de clair x_0 par r itérations d'une fonction de tour T

$$x_i = T(x_{i-1}, k_i)\ 1 \leq i \leq r$$

où k_i est la (sous-)clef du ième tour ;

- Exemples : Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) ou l'Advanced Encryption Standard (AES).

Systèmes de chiffrement itérés par blocs

- Dans un système de chiffrement par blocs les messages clairs et chiffrés sont considérés comme des blocs de bits de taille identique ;
- Dans un système de chiffrement par blocs à r tours le bloc chiffré x_r est obtenu à partir d'un bloc de clair x_0 par r itérations d'une fonction de tour T

$$x_i = T(x_{i-1}, k_i)\ 1 \leq i \leq r$$

où k_i est la (sous-)clef du ième tour ;
- Exemples : Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) ou l'Advanced Encryption Standard (AES).

Les boîtes-S

Des composants **internes** de la fonction de tour, les boîtes-S, assurent la résistance à diverses attaques. En particulier, les boîtes-S doivent être (hautement) non linéaires *i.e.*

- Elles doivent être le plus éloigné possible des fonctions affines : fonctions courbes ;
- Elles doivent être très différentes des morphismes de groupes : fonctions parfaitement non linéaires.

Les boîtes-S

Des composants **internes** de la fonction de tour, les boîtes-S, assurent la résistance à diverses attaques. En particulier, les boîtes-S doivent être (hautement) non linéaires *i.e.*

- Elles doivent être le plus éloigné possible des fonctions affines : fonctions courbes ;
- Elles doivent être très différentes des morphismes de groupes : fonctions parfaitement non linéaires.

Les boîtes-S

Des composants **internes** de la fonction de tour, les boîtes-S, assurent la résistance à diverses attaques. En particulier, les boîtes-S doivent être (hautement) non linéaires *i.e.*

- Elles doivent être le plus éloigné possible des fonctions affines : fonctions courbes ;
- Elles doivent être très différentes des morphismes de groupes : fonctions parfaitement non linéaires.

Les boîtes-S

Des composants **internes** de la fonction de tour, les boîtes-S, assurent la résistance à diverses attaques. En particulier, les boîtes-S doivent être (hautement) non linéaires *i.e.*

- Elles doivent être le plus éloigné possible des fonctions affines : fonctions courbes ;
- Elles doivent être très différentes des morphismes de groupes : fonctions parfaitement non linéaires.

Théorème

Une fonction booléenne est courbe si et seulement si elle est parfaitement non linéaire.

Corollaire

La résistance maximale à l'attaque linéaire est équivalente à la résistance maximale à l'attaque différentielle.

Théorème

Une fonction booléenne est courbe si et seulement si elle est parfaitement non linéaire.

Corollaire

La résistance maximale à l'attaque linéaire est équivalente à la résistance maximale à l'attaque différentielle.

Utilisation des boîtes-S et cryptanalyse différentielle

- Une boîte-S f est une fonction de m bits en entrée pour n bits en sortie ;
- Une telle fonction f intervient dans un tour juste après la combinaison par OU-exclusif (XOR) entre le bloc x_{i-1} et la clef k_i *i.e.* $y = f(k_i \oplus x_{i-1})$.
- La cryptanalyse différentielle de **Biham & Shamir** tire profit de cette combinaison par un XOR : les différences (au sens du XOR) entre deux sorties d'une boîte-S pour des entrées dont la différence est fixée doivent être proches de la distribution uniforme. Dans le cas contraire, le biais statistique peut être exploité par l'attaque différentielle afin de découvrir la clef utilisée lors du dernier tour.

Utilisation des boîtes-S et cryptanalyse différentielle

- Une boîte-S f est une fonction de m bits en entrée pour n bits en sortie ;
- Une telle fonction f intervient dans un tour juste après la combinaison par OU-exclusif (XOR) entre le bloc x_{i-1} et la clef k_i *i.e.* $y = f(k_i \oplus x_{i-1})$.
- La cryptanalyse différentielle de **Biham & Shamir** tire profit de cette combinaison par un XOR : les différences (au sens du XOR) entre deux sorties d'une boîte-S pour des entrées dont la différence est fixée doivent être proches de la distribution uniforme. Dans le cas contraire, le biais statistique peut être exploité par l'attaque différentielle afin de découvrir la clef utilisée lors du dernier tour.

Utilisation des boîtes-S et cryptanalyse différentielle

- Une boîte-S f est une fonction de m bits en entrée pour n bits en sortie ;
- Une telle fonction f intervient dans un tour juste après la combinaison par OU-exclusif (XOR) entre le bloc x_{i-1} et la clef k_i *i.e.* $y = f(k_i \oplus x_{i-1})$.
- La cryptanalyse différentielle de **Biham & Shamir** tire profit de cette combinaison par un XOR : les différences (au sens du XOR) entre deux sorties d'une boîte-S pour des entrées dont la différence est fixée doivent être proches de la distribution uniforme. Dans le cas contraire, le biais statistique peut être exploité par l'attaque différentielle afin de découvrir la clef utilisée lors du dernier tour.

Utilisation des boîtes-S et cryptanalyse différentielle

- Une boîte-S f est une fonction de m bits en entrée pour n bits en sortie ;
- Une telle fonction f intervient dans un tour juste après la combinaison par OU-exclusif (XOR) entre le bloc x_{i-1} et la clef k_i *i.e.* $y = f(k_i \oplus x_{i-1})$.
- La cryptanalyse différentielle de **Biham & Shamir** tire profit de cette combinaison par un XOR : les différences (au sens du XOR) entre deux sorties d'une boîte-S pour des entrées dont la différence est fixée doivent être proches de la distribution uniforme. Dans le cas contraire, le biais statistique peut être exploité par l'attaque différentielle afin de découvrir la clef utilisée lors du dernier tour.

Utilisation des boîtes-S et cryptanalyse différentielle

- Une boîte-S f est une fonction de m bits en entrée pour n bits en sortie ;
- Une telle fonction f intervient dans un tour juste après la combinaison par OU-exclusif (XOR) entre le bloc x_{i-1} et la clef k_i *i.e.* $y = f(k_i \oplus x_{i-1})$.
- La cryptanalyse différentielle de **Biham & Shamir** tire profit de cette combinaison par un XOR : les différences (au sens du XOR) entre deux sorties d'une boîte-S pour des entrées dont la différence est fixée doivent être proches de la distribution uniforme. Dans le cas contraire, le biais statistique peut être exploité par l'attaque différentielle afin de découvrir la clef utilisée lors du dernier tour.

Utilisation des boîtes-S et cryptanalyse différentielle

- Une boîte-S f est une fonction de m bits en entrée pour n bits en sortie ;
- Une telle fonction f intervient dans un tour juste après la combinaison par OU-exclusif (XOR) entre le bloc x_{i-1} et la clef k_i *i.e.* $y = f(k_i \oplus x_{i-1})$.
- La cryptanalyse différentielle de **Biham & Shamir** tire profit de cette combinaison par un XOR : les différences (au sens du XOR) entre deux sorties d'une boîte-S pour des entrées dont la différence est fixée doivent être proches de la distribution uniforme. Dans le cas contraire, le biais statistique peut être exploité par l'attaque différentielle afin de découvrir la clef utilisée lors du dernier tour.

Plan de la présentation

Autres lois de groupes

- Le système IDEA de **Lai & Massey** utilise le XOR mais aussi l'addition dans un groupe cyclique et la multiplication dans un corps fini ;
- GOST, l'analogue russe du DES, utilise l'addition dans un groupe cyclique ;
- Alexander Pott écrit : " *It seems that in most applications (in particular in cryptography) people use nonlinear functions on finite fields. However, there is no technical reason why you should restrict yourselves to this case.* ".

Autres lois de groupes

- Le système IDEA de **Lai & Massey** utilise le XOR mais aussi l'addition dans un groupe cyclique et la multiplication dans un corps fini ;
- GOST, l'analogue russe du DES, utilise l'addition dans un groupe cyclique ;
- Alexander Pott écrit : " *It seems that in most applications (in particular in cryptography) people use nonlinear functions on finite fields. However, there is no technical reason why you should restrict yourselves to this case.* ".

Autres lois de groupes

- Le système IDEA de **Lai & Massey** utilise le XOR mais aussi l'addition dans un groupe cyclique et la multiplication dans un corps fini ;
- GOST, l'analogue russe du DES, utilise l'addition dans un groupe cyclique ;
- Alexander Pott écrit : " *It seems that in most applications (in particular in cryptography) people use nonlinear functions on finite fields. However, there is no technical reason why you should restrict yourselves to this case.* ".

Autres lois de groupes

- Le système IDEA de **Lai & Massey** utilise le XOR mais aussi l'addition dans un groupe cyclique et la multiplication dans un corps fini ;
- GOST, l'analogue russe du DES, utilise l'addition dans un groupe cyclique ;
- Alexander Pott écrit : " *It seems that in most applications (in particular in cryptography) people use nonlinear functions on finite fields. However, there is no technical reason why you should restrict yourselves to this case.* ".

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X via un homomorphisme de groupes ϕ de G dans le groupe symétrique $S(X)$ de X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = f(\phi(k_i)(x_{i-1}))$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$ et où $\phi(k_i)(x_{i-1})$ représente l'action de la clef k_i sur le message x_{i-1} ;

- Notation : on pose $k.x = \phi(k)(x)$. Le symbole " . " désignant ainsi une loi de composition externe de G sur X.

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X via un homomorphisme de groupes ϕ de G dans le groupe symétrique $S(X)$ de X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = f(\phi(k_i)(x_{i-1}))$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$ et où $\phi(k_i)(x_{i-1})$ représente l'action de la clef k_i sur le message x_{i-1} ;
- Notation : on pose $k.x = \phi(k)(x)$. Le symbole " . " désignant ainsi une loi de composition externe de G sur X.

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X via un homomorphisme de groupes ϕ de G dans le groupe symétrique $S(X)$ de X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = f(\phi(k_i)(x_{i-1}))$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$ et où $\phi(k_i)(x_{i-1})$ représente l'action de la clef k_i sur le message x_{i-1} ;

- Notation : on pose $k.x = \phi(k)(x)$. Le symbole " . " désignant ainsi une loi de composition externe de G sur X.

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X via un homomorphisme de groupes ϕ de G dans le groupe symétrique $S(X)$ de X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = f(\phi(k_i)(x_{i-1}))$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$ et où $\phi(k_i)(x_{i-1})$ représente l'action de la clef k_i sur le message x_{i-1} ;

- Notation : on pose $k.x = \phi(k)(x)$. Le symbole " . " désignant ainsi une loi de composition externe de G sur X.

Combinaison par une action de groupe

- Supposons que les clefs de tour sont choisies dans un groupe fini G qui agit sur un ensemble fini non vide X via un homomorphisme de groupes ϕ de G dans le groupe symétrique $S(X)$ de X et soit H un groupe fini ;
- Dans ce cas les boîtes-S sont utilisées comme suit :

$$y = f(\phi(k_i)(x_{i-1}))$$

avec $x_{i-1} \in X$, $y \in H$, $k_i \in G$ et où $\phi(k_i)(x_{i-1})$ représente l'action de la clef k_i sur le message x_{i-1} ;

- Notation : on pose $k.x = \phi(k)(x)$. Le symbole " . " désignant ainsi une loi de composition externe de G sur X.

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme, où R est le chiffrement réduit défini par $R = T_{k_{r-1}} \circ \ldots \circ T_{k_1}$ avec $T_k : x \mapsto T(x, k)$ (supposée inversible $\forall k$) ;
- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$T^{-1}_{\hat{k}_r}(x'_r) - T^{-1}_{\hat{k}_r}(x_r) = \beta \, .$$

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme, où R est le chiffrement réduit défini par $R = T_{k_{r-1}} \circ \ldots \circ T_{k_1}$ avec $T_k : x \mapsto T(x, k)$ (supposée inversible $\forall k$) ;

- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$T^{-1}_{\hat{k}_r}(x'_r) - T^{-1}_{\hat{k}_r}(x_r) = \beta \ .$$

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme, où R est le chiffrement réduit défini par $R = T_{k_{r-1}} \circ \ldots \circ T_{k_1}$ avec $T_k : x \mapsto T(x, k)$ (supposée inversible $\forall k$) ;

- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$T^{-1}_{\hat{k}_r}(x'_r) - T^{-1}_{\hat{k}_r}(x_r) = \beta \ .$$

Attaque différentielle modifiée

- Trouver une paire $(\alpha, \beta) \in G \times H$ telle que la probabilité

$$Pr(R(\alpha.x) - R(x) = \beta)$$

est la plus éloignée possible de la distribution uniforme, où R est le chiffrement réduit défini par $R = T_{k_{r-1}} \circ \ldots \circ T_{k_1}$ avec $T_k : x \mapsto T(x, k)$ (supposée inversible $\forall k$) ;
- Tirer au hasard un texte clair x_0 et soumettre au chiffrement à la fois x_0 et $\alpha.x_0$. On obtient deux couples clair/chiffré : (x_0, x_r) et $(\alpha.x_0, x'_r)$;
- Trouver toutes les valeurs possibles $\hat{k}_r$ pour la clef du dernier tour telles que

$$T^{-1}_{\hat{k}_r}(x'_r) - T^{-1}_{\hat{k}_r}(x_r) = \beta \ .$$

Objectif

Le but de cette présentation est de montrer qu'il existe des boîtes-S qui assurent une résistance maximale face à cette attaque différentielle modifiée.

En particulier il existe de telles fonctions dans des cas où l'approche traditionnelle conclut à la non-existence de tels objets.

Objectif

Le but de cette présentation est de montrer qu'il existe des boîtes-S qui assurent une résistance maximale face à cette attaque différentielle modifiée.
En particulier il existe de telles fonctions dans des cas où l'approche traditionnelle conclut à la non-existence de tels objets.

Plan de la présentation

Dans cette présentation, G^* désigne l'ensemble des éléments non nuls d'un groupe G (en notation additive). Pour k un entier naturel non nul quelconque, V_k désigne un espace vectoriel de dimension k sur le corps fini $GF(2)$.

Définition

Une fonction booléenne $f : V_m \to V_n$ est dite parfaitement non linéaire (PN) si pour chaque $(\alpha, \beta) \in V_m^* \times V_n$,

$$|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n}.$$

Une fonction booléenne est courbe si et seulement si elle est PN.

Dans cette présentation, G^* désigne l'ensemble des éléments non nuls d'un groupe G (en notation additive). Pour k un entier naturel non nul quelconque, V_k désigne un espace vectoriel de dimension k sur le corps fini $GF(2)$.

Définition

Une fonction booléenne $f : V_m \to V_n$ est dite parfaitement non linéaire (PN) si pour chaque $(\alpha, \beta) \in V_m^* \times V_n$,

$$|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n}.$$

Une fonction booléenne est courbe si et seulement si elle est PN.

Dans cette présentation, G^* désigne l'ensemble des éléments non nuls d'un groupe G (en notation additive). Pour k un entier naturel non nul quelconque, V_k désigne un espace vectoriel de dimension k sur le corps fini $GF(2)$.

Définition

Une fonction booléenne $f : V_m \to V_n$ est dite parfaitement non linéaire (PN) si pour chaque $(\alpha, \beta) \in V_m^* \times V_n$,

$$|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n} .$$

Une fonction booléenne est courbe si et seulement si elle est PN.

Dans cette présentation, G^* désigne l'ensemble des éléments non nuls d'un groupe G (en notation additive). Pour k un entier naturel non nul quelconque, V_k désigne un espace vectoriel de dimension k sur le corps fini $GF(2)$.

Définition

Une fonction booléenne $f : V_m \to V_n$ est dite parfaitement non linéaire (PN) si pour chaque $(\alpha, \beta) \in V_m^* \times V_n$,

$$|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n} .$$

Une fonction booléenne est courbe si et seulement si elle est PN.

Cas impossibles

Théorème

Si $f : V_m \to V_n$ est courbe alors m est pair et $m \geq 2n$.

- Dimension impaire : m est impair ;
- Dimension plane : $m = n$.

Cas impossibles

Théorème

Si $f : V_m \longrightarrow V_n$ est courbe alors m est pair et $m \geq 2n$.

- Dimension impaire : m est impair ;
- Dimension plane : $m = n$.

Cas impossibles

Théorème

Si $f : V_m \to V_n$ est courbe alors m est pair et $m \geq 2n$.

- Dimension impaire : m est impair ;
- Dimension plane : $m = n$.

Plan de la présentation

Définition

Soit G un groupe fini de cardinal v et D un sous-ensemble de G de cardinal k. D est un (v, k, λ)-ensemble à différences de G si pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement λ solutions $(x, y) \in D^2$.

D est un ensemble à différences de Hadamard si l'on a

$$(v, k, \lambda) = (4N^2, 2N^2 \pm N, N^2 \pm N)$$

pour un certain entier N.

Définition

Soit G un groupe fini de cardinal v et D un sous-ensemble de G de cardinal k. D est un (v, k, λ)-ensemble à différences de G si pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement λ solutions $(x, y) \in D^2$.
D est un ensemble à différences de Hadamard si l'on a

$$(v, k, \lambda) = (4N^2, 2N^2 \pm N, N^2 \pm N)$$

pour un certain entier N.

Théorème

Une fonction $f : V_m \rightarrow GF(2)$ est PN si et seulement si son support $S_f := \{x \in V_m | f(x) \neq 0\}$ est un ensemble à différences de Hadamard de V_m.

Plan de la présentation

Soit G un groupe et X un ensemble non vide.

- Une action de groupe de G sur X est un homomorphisme de groupe $\phi : G \to S(X)$;
- L'action de groupe est dite fidèle si ϕ est injectif ;
- Notation : on pose $\alpha.x := \phi(\alpha)(x)$.

Soit G un groupe et X un ensemble non vide.

- Une action de groupe de G sur X est un homomorphisme de groupe $\phi : G \to S(X)$;
- L'action de groupe est dite fidèle si ϕ est injectif ;
- Notation : on pose $\alpha.x := \phi(\alpha)(x)$.

Soit G un groupe et X un ensemble non vide.

- Une action de groupe de G sur X est un homomorphisme de groupe $\phi : G \to S(X)$;
- L'action de groupe est dite fidèle si ϕ est injectif ;
- Notation : on pose $\alpha.x := \phi(\alpha)(x)$.

Soit G un groupe et X un ensemble non vide.

- Une action de groupe de G sur X est un homomorphisme de groupe $\phi : G \to S(X)$;
- L'action de groupe est dite fidèle si ϕ est injectif ;
- Notation : on pose $\alpha.x := \phi(\alpha)(x)$.

Exemples

- Un groupe G agit sur lui-même par translation : $\alpha.x := \alpha + x$;
- Soit W un sous-espace vectoriel de V. Alors W agit fidèlement sur V par translation : $w.v = w + v$;
- Le groupe multiplicatif $\mathbb{K}^*$ agit fidèlement sur le corps $\mathbb{K}$ par multiplication : $\alpha.x = \alpha x$.

Exemples

- Un groupe G agit sur lui-même par translation : $\alpha.x := \alpha + x$;
- Soit W un sous-espace vectoriel de V. Alors W agit fidèlement sur V par translation : $w.v = w + v$;
- Le groupe multiplicatif $\mathbb{K}^*$ agit fidèlement sur le corps $\mathbb{K}$ par multiplication : $\alpha.x = \alpha x$.

Exemples

- Un groupe G agit sur lui-même par translation : $\alpha.x := \alpha + x$;
- Soit W un sous-espace vectoriel de V. Alors W agit fidèlement sur V par translation : $w.v = w + v$;
- Le groupe multiplicatif $\mathbb{K}^*$ agit fidèlement sur le corps $\mathbb{K}$ par multiplication : $\alpha.x = \alpha x$.

Exemples

- Un groupe G agit sur lui-même par translation : $\alpha.x := \alpha + x$;
- Soit W un sous-espace vectoriel de V. Alors W agit fidèlement sur V par translation : $w.v = w + v$;
- Le groupe multiplicatif $\mathbb{K}^*$ agit fidèlement sur le corps $\mathbb{K}$ par multiplication : $\alpha.x = \alpha x$.

Plan de la présentation

Définition

Soit G un groupe fini agissant fidèlement sur V_m. La fonction booléenne $f : V_m \to V_n$ est dite G-parfaitement non linéaire (G-PN) si pour chaque $(\alpha, \beta) \in G^* \times V_n$,

$$|\{x \in V_m | f(\alpha.x) \oplus f(x) = \beta\}| = 2^{m-n} .$$

Définition

Soit G un groupe fini agissant fidèlement sur V_m. La fonction booléenne $f : V_m \to V_n$ est dite G-parfaitement non linéaire (G-PN) si pour chaque $(\alpha, \beta) \in G^* \times V_n$,

$$|\{x \in V_m | f(\alpha.x) \oplus f(x) = \beta\}| = 2^{m-n} .$$

Définition

Soit G un groupe fini agissant fidèlement sur un ensemble fini non vide X de cardinal v et D un sous-ensemble de X de cardinal k. D est un G-(v, k, λ)-ensemble à différences de X si pour chaque $\alpha \in G^*$, l'équation $x = \alpha.y$ admet exactement λ solutions $(x, y) \in D^2$.

Théorème

Soit G un groupe fini agissant fidèlement sur l'espace vectoriel V_m. Une fonction booléenne $f : V_m \to GF(2)$ est G-PN si et seulement si son support S_f est un G-ensemble à différences de V_m dont les paramètres (v, k, λ) satisfont l'égalité

$$v = 4(k - \lambda) .$$

Théorème

Soit G un groupe fini agissant fidèlement sur l'espace vectoriel V_m. Une fonction booléenne $f : V_m \to GF(2)$ est G-PN si et seulement si son support S_f est un G-ensemble à différences de V_m dont les paramètres (v, k, λ) satisfont l'égalité

$$v = 4(k - \lambda) .$$

Plan de la présentation

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.

On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$.

Notons qu'une action libre est fidèle.

Soit donc G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).

Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{rccc} \phi_x : & G & \to & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.
On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$.
Notons qu'une action libre est fidèle.
Soit donc G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).
Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{rccc} \phi_x : & G & \rightarrow & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.
On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$.
Notons qu'une action libre est fidèle.
Soit donc G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).
Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{rccc} \phi_x : & G & \rightarrow & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

Une action de G sur X induit une partition de X constituée d'orbites $\mathcal{O}(x) = \{\alpha.x | \alpha \in G\} = G.x$ pour $x \in X$.
On dit que l'action est libre si quel que soit $x \in X$, $|G| = |\mathcal{O}(x)|$.
Notons qu'une action libre est fidèle.
Soit donc G un groupe fini agissant librement sur V_m. On suppose en outre que G contient des ensembles à différences de Hadamard classiques (en particulier $|G| = 4N^2$).
Pour chaque $x \in V_m$, l'application orbitale de x définie par

$$\begin{array}{rccc} \phi_x : & G & \rightarrow & \mathcal{O}(x) \subset V_m \\ & \alpha & \mapsto & \alpha.x \end{array}$$

est bijective.

Concaténation d'ensembles à différences de Hadamard

A chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.
On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.
Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.
On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

A chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.

On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.

Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.

On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

A chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.
On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.
Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.
On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

A chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.
On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.
Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.
On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

A chaque orbite $\mathcal{O}$ de la partition de V_m, on associe un élément x de V_m tel que $\mathcal{O}(x) = \mathcal{O}$ et un ensemble à différences de Hadamard D_x de G. De la sorte on constitue un ensemble noté V_m/G de représentants des orbites.
On peut montrer que $\phi_x(D_x)$ est un G-ensemble à différences de $\mathcal{O}(x)$ dont les paramètres sont les mêmes que ceux de l'ensemble à différences de Hadamard D_x.
Si $(x, y) \in (V_m/G)^2$ et $x \neq y$ alors $\phi_x(D_x) \cap \phi_y(D_y) = \emptyset$.
On définit alors $D := \bigcup_{x \in V_m/G} \phi_x(D_x)$.

Concaténation d'ensembles à différences de Hadamard

L'ensemble D ainsi défini est un G-$(2^m, (2N^2-N)j+(2N^2+N)(\frac{2^m}{4N^2}-j), (N^2-N)j+(N^2+N)(\frac{2^m}{4N^2}-j))$-ensemble à différences de V_m où j est un entier entre 0 et $\frac{2^m}{4N^2}$ désignant le nombre d'ensembles à différences D_x choisis dont les paramètres sont de la forme $(4N^2, 2N^2-N, N^2-N)$.
Les paramètres de D satisfont en particulier l'équation $v = 4(k-\lambda)$.

Concaténation d'ensembles à différences de Hadamard

L'ensemble D ainsi défini est un G-$(2^m, (2N^2-N)j+(2N^2+N)(\frac{2^m}{4N^2}-j), (N^2-N)j+(N^2+N)(\frac{2^m}{4N^2}-j))$-ensemble à différences de V_m où j est un entier entre 0 et $\frac{2^m}{4N^2}$ désignant le nombre d'ensembles à différences D_x choisis dont les paramètres sont de la forme $(4N^2, 2N^2 - N, N^2 - N)$.

Les paramètres de D satisfont en particulier l'équation $v = 4(k - \lambda)$.

Concaténation d'ensembles à différences de Hadamard

L'ensemble D ainsi défini est un G-$(2^m, (2N^2-N)j+(2N^2+N)(\frac{2^m}{4N^2}-j), (N^2-N)j+(N^2+N)(\frac{2^m}{4N^2}-j))$-ensemble à différences de V_m où j est un entier entre 0 et $\frac{2^m}{4N^2}$ désignant le nombre d'ensembles à différences D_x choisis dont les paramètres sont de la forme $(4N^2, 2N^2 - N, N^2 - N)$.
Les paramètres de D satisfont en particulier l'équation $v = 4(k - \lambda)$.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en dimension impaire.
Soit m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.
D'après le résultat précédent, on peut construire une fonction $f : V_m \rightarrow GF(2)$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en dimension impaire.

Soit m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.

D'après le résultat précédent, on peut construire une fonction $f : V_m \rightarrow GF(2)$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en dimension impaire.
Soit m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.
D'après le résultat précédent, on peut construire une fonction $f : V_m \rightarrow GF(2)$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Concaténation d'ensembles à différences de Hadamard

On peut instancier la construction précédente de manière à obtenir des fonctions booléennes " courbes " en dimension impaire.
Soit m et k tels que $m \geq 2k$. On peut montrer que V_{2k} agit librement sur V_m et contient des ensembles à différences de Hadamard.
D'après le résultat précédent, on peut construire une fonction $f : V_m \rightarrow GF(2)$ qui est V_{2k}-PN même si m est un entier impair, ce qui est évidemment impossible pour l'approche classique des fonctions courbes.

Plan de la présentation

On a déjà vu qu'il n'existe pas de fonction courbe $f : V_m \to V_m$.
Dès que l'on a une solution x_0 à l'équation $f(\alpha \oplus x) \oplus f(x) = \beta$, on en trouve immédiatement une autre $\alpha \oplus x_0$.
Le mieux que l'on puisse espérer pour f est qu'elle soit presque parfaitement non linéaire *i.e.* pour chaque $(\alpha, \beta) \in V_m^* \times V_m$, $|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0, 2\}$.

On a déjà vu qu'il n'existe pas de fonction courbe $f : V_m \to V_m$.
Dès que l'on a une solution x_0 à l'équation $f(\alpha \oplus x) \oplus f(x) = \beta$, on en trouve immédiatement une autre $\alpha \oplus x_0$.

Le mieux que l'on puisse espérer pour f est qu'elle soit presque parfaitement non linéaire *i.e.* pour chaque $(\alpha, \beta) \in V_m^* \times V_m$, $|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0, 2\}$.

On a déjà vu qu'il n'existe pas de fonction courbe $f : V_m \to V_m$.
Dès que l'on a une solution x_0 à l'équation $f(\alpha \oplus x) \oplus f(x) = \beta$, on en trouve immédiatement une autre $\alpha \oplus x_0$.
Le mieux que l'on puisse espérer pour f est qu'elle soit presque parfaitement non linéaire *i.e.* pour chaque $(\alpha, \beta) \in V_m^* \times V_m$, $|\{x \in V_m | f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0, 2\}$.

Conjecture

Il n'existe pas de bijection presque parfaitement non linéaire pour m pair.

Théorème

Soit m un entier strictement positif quelconque. Soit $f : GF(2^m) \rightarrow GF(2^m)$ un automorphisme additif. Alors f est une bijection $GF(2^m)^*$-PN.

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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

Preuve

Pour montrer que f est $GF(2^m)^*$-PN il suffit de prouver que pour chaque $(\alpha, \beta) \in (GF(2^m)^* \setminus \{1\}) \times GF(2^m)$, il existe un et un seul $x \in GF(2^m)$ tel que $f(\alpha.x) \oplus f(x) = \beta$.

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