

Non linéarité parfaite généralisée au sens des actions de groupe, contribution aux fondements de la solidité cryptographique

Laurent Poinso

Université du Sud Toulon-Var

Directeur de thèse : Sami Harari
Lundi 12 septembre 2005

tu-logo

ur-logo

Introduction

Critères de solidité cryptographique :

- Equilibre ;
- Non corrélation ;
- Haut degré algébrique ;
- Non linéarité parfaite (fonction courbe)

tu-logo

ur-logo

Introduction

Critères de solidité cryptographique :

- Equilibre ;
- Non corrélation ;
- Haut degré algébrique ;
- Non linéarité parfaite (fonction courbe)

tu-logo

ur-logo

Introduction

Critères de solidité cryptographique :

- Equilibre ;
- Non corrélation ;
- Haut degré algébrique ;
- Non linéarité parfaite (fonction courbe)

tu-logo

ur-logo

Introduction

Critères de solidité cryptographique :

- Equilibre ;
- Non corrélation ;
- Haut degré algébrique ;
- Non linéarité parfaite (fonction courbe)

tu-logo

ur-logo

Introduction

Critères de solidité cryptographique :

- Equilibre ;
- Non corrélation ;
- Haut degré algébrique ;
- **Non linéarité parfaite** (fonction courbe)

tu-logo

ur-logo

Introduction

Soient G et H deux groupes finis commutatifs. Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** si pour tout α non nul de G et tout $\beta \in H$,

$$|\{x \in G \mid f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Posons $\sigma_\alpha : G \rightarrow G$ définie par $x \mapsto \alpha + x$. L'équation précédente se ré-écrit naturellement :

$$|\{x \in G \mid f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Introduction

Soient G et H deux groupes finis commutatifs. Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** si pour tout α non nul de G et tout $\beta \in H$,

$$|\{x \in G \mid f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Posons $\sigma_\alpha : G \rightarrow G$ définie par $x \mapsto \alpha + x$. L'équation précédente se ré-écrit naturellement :

$$|\{x \in G \mid f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Introduction

Soient G et H deux groupes finis commutatifs. Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** si pour tout α non nul de G et tout $\beta \in H$,

$$|\{x \in G \mid f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Posons $\sigma_\alpha : G \rightarrow G$ définie par $x \mapsto \alpha + x$. L'équation précédente se ré-écrit naturellement :

$$|\{x \in G \mid f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Introduction

Soient G et H deux groupes finis (H étant commutatif) et X un ensemble fini non vide sur lequel G agit à gauche. Une fonction $f : X \rightarrow H$ est **G -parfaitement non linéaire** si pour tout g non nul de G et tout $\beta \in H$,

$$|\{x \in X \mid f(g.x) - f(x) = \beta\}| = \frac{|X|}{|H|}.$$

tu-logo

ur-logo

Plan

- 1 Approche traditionnelle
 - Non linéarité parfaite
 - Fonction courbe
 - Ensemble à différences
- 2 Non linéarité parfaite au sens des actions de groupe
 - Rappels sur les actions de groupe
 - G -Non linéarité parfaite
- 3 Notion duale de fonction courbe
 - Cas commutatif
 - Cas non commutatif
- 4 G -ensembles à différences
 - Définition et Caractérisation combinatoire
 - Constructions
- 5 Conclusion et perspectives

tu-logo

ur-logo

Plan

- 1 Approche traditionnelle
 - Non linéarité parfaite
 - Fonction courbe
 - Ensemble à différences
- 2 Non linéarité parfaite au sens des actions de groupe
 - Rappels sur les actions de groupe
 - G -Non linéarité parfaite
- 3 Notion duale de fonction courbe
 - Cas commutatif
 - Cas non commutatif
- 4 G -ensembles à différences
 - Définition et Caractérisation combinatoire
 - Constructions
- 5 Conclusion et perspectives

Plan

- 1 Approche traditionnelle
 - Non linéarité parfaite
 - Fonction courbe
 - Ensemble à différences
- 2 Non linéarité parfaite au sens des actions de groupe
 - Rappels sur les actions de groupe
 - G -Non linéarité parfaite
- 3 Notion duale de fonction courbe
 - Cas commutatif
 - Cas non commutatif
- 4 G -ensembles à différences
 - Définition et Caractérisation combinatoire
 - Constructions
- 5 Conclusion et perspectives

Plan

- 1 Approche traditionnelle
 - Non linéarité parfaite
 - Fonction courbe
 - Ensemble à différences
- 2 Non linéarité parfaite au sens des actions de groupe
 - Rappels sur les actions de groupe
 - G -Non linéarité parfaite
- 3 Notion duale de fonction courbe
 - Cas commutatif
 - Cas non commutatif
- 4 G -ensembles à différences
 - Définition et Caractérisation combinatoire
 - Constructions
- 5 Conclusion et perspectives

Plan

- 1 Approche traditionnelle
 - Non linéarité parfaite
 - Fonction courbe
 - Ensemble à différences
- 2 Non linéarité parfaite au sens des actions de groupe
 - Rappels sur les actions de groupe
 - G -Non linéarité parfaite
- 3 Notion duale de fonction courbe
 - Cas commutatif
 - Cas non commutatif
- 4 G -ensembles à différences
 - Définition et Caractérisation combinatoire
 - Constructions
- 5 Conclusion et perspectives

Historique

Définition (Nyberg, 1991)

Une fonction $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ est **parfaitement non linéaire** si pour tout α non nul de \mathbb{F}_2^m et tout $\beta \in \mathbb{F}_2^n$,

$$|\{x \in \mathbb{F}_2^m \mid f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n}.$$

Résistance maximale face à la cryptanalyse différentielle de Biham et Shamir.

Dans le cadre des groupes finis abéliens (1)

Pour un groupe G , e_G est son élément neutre et $G^* = G \setminus \{e_G\}$.

Définitions

Soient G et H deux groupes finis commutatifs et $f : G \rightarrow H$.

- f est **équilibrée** si pour tout $\beta \in H$,

$$|\{x \in G \mid f(x) = \beta\}| = \frac{|G|}{|H|};$$
- La **dérivée** de f dans la direction $\alpha \in G$ est définie par

$$\begin{aligned} d_\alpha f : G &\rightarrow H \\ x &\mapsto f(\alpha + x) - f(x). \end{aligned}$$

Dans le cadre des groupes finis abéliens (2)

Définition

Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** (au sens classique) si $\forall \alpha \in G^*$, $d_\alpha f$ est équilibrée, *i.e.* $\forall \alpha \in G^*$ et $\forall \beta \in H$,

$$|\{x \in G \mid f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Remarque

Si G est non abélien, on parle alors de **non linéarité parfaite (au sens des translations) à gauche**.

Dans le cadre des groupes finis abéliens (2)

Définition

Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** (au sens classique) si $\forall \alpha \in G^*$, $d_\alpha f$ est équilibrée, i.e. $\forall \alpha \in G^*$ et $\forall \beta \in H$,

$$|\{x \in G \mid f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Remarque

Si G est non abélien, on parle alors de **non linéarité parfaite (au sens des translations) à gauche**.

Dans le cadre des groupes finis abéliens (2)

Définition

Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** (au sens classique) si $\forall \alpha \in G^*$, $d_\alpha f$ est équilibrée, i.e. $\forall \alpha \in G^*$ et $\forall \beta \in H$,

$$|\{x \in G \mid f(\alpha + x) - f(x) = \beta\}| = \frac{|G|}{|H|}.$$

Remarque

Si G est non abélien, on parle alors de **non linéarité parfaite (au sens des translations) à gauche**.

Caractérisations équivalentes

La non linéarité parfaite \Leftrightarrow

- Par la transformée de Fourier : notion de **fonction courbe** ;
- Caractérisation combinatoire par les **ensembles à différences**.

Caractérisations équivalentes

La non linéarité parfaite \Leftrightarrow

- Par la transformée de Fourier : notion de **fonction courbe** ;
- Caractérisation combinatoire par les **ensembles à différences**.

Caractérisations équivalentes

La non linéarité parfaite \Leftrightarrow

- Par la transformée de Fourier : notion de **fonction courbe** ;
- Caractérisation combinatoire par les **ensembles à différences**.

Historique

Définition (Dillon 1974, Rothaus 1976)

Une fonction $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ est **courbe** si pour tout $\alpha \in \mathbb{F}_2^m$,

$$\sum_{x \in \mathbb{F}_2^m} (-1)^{f(x) \oplus \alpha \cdot x} = \pm 2^{\frac{m}{2}} .$$

Résistance maximale face à la cryptanalyse linéaire de Matsui.

Dans le cadre des groupes finis abéliens (1)

Le groupe **dual** de G , noté \widehat{G} , est l'ensemble des homomorphismes (de groupe) de G dans \mathbb{U} .
Il est isomorphe à G . Ces éléments sont appelés **caractères** :
pour $\alpha \in G$, le caractère correspondant à α (via l'isomorphisme) est noté χ_G^α .

Dans le cadre des groupes finis abéliens (2)

Définition

Soient G un groupe fini abélien et $\varphi : G \rightarrow \mathbb{C}$. La **transformée de Fourier (discrète)** de φ est l'application $\hat{\varphi}$ définie par

$$\begin{aligned} \hat{\varphi} : G &\rightarrow \mathbb{C} \\ \alpha &\mapsto \sum_{x \in G} \varphi(x) \chi_G^\alpha(x). \end{aligned}$$

Caractérisation duale

Théorème (Carlet & Ding, 2004)

Soient G et H deux groupes finis abéliens. Soit $f : G \rightarrow H$. La fonction f est parfaitement non linéaire si et seulement si

$\forall \alpha \in G, \forall \beta \in H^*,$

$$|\widehat{\chi_H^\beta \circ f}(\alpha)|^2 = |G|.$$

Définition

Soit G un groupe fini commutatif. Soit $D \subset G$. D est un (v, k, λ) **ensemble à différences** de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement λ solutions distinctes dans D^2 .

Définition

Soit G un groupe fini commutatif. Soit $D \subset G$. D est un (v, k, λ) **ensemble à différences** de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement λ solutions distinctes dans D^2 .

Définition

Soit G un groupe fini commutatif. Soit $D \subset G$. D est un (v, k, λ) **ensemble à différences** de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement λ solutions distinctes dans D^2 .

Définition

Soit G un groupe fini commutatif. Soit $D \subset G$. D est un (v, k, λ) **ensemble à différences** de G si

- $v = |G|$;
- $k = |D|$;
- Pour chaque $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement λ solutions distinctes dans D^2 .

Ensemble à différences de Hadamard

Définition

Un (v, k, λ) ensemble à différences D de G est dit de **Hadamard** si

$$(v, k, \lambda) = (4n^2, 2n^2 \pm n, n(n \pm 1)) .$$

Caractérisation combinatoire

Théorème (Carlet & Ding, 2004)

Soit G un groupe fini commutatif tel que $|G| = 4n^2$. Une fonction $f : G \rightarrow \mathbb{F}_2$ est parfaitement non linéaire si et seulement si son support $S_f = \{x \in G \mid f(x) = 1\}$ est un ensemble à différences de Hadamard de G .

Dillon (1974) avait établi un résultat identique pour $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$.

Plan

- Rappels sur les actions de groupe ;
- Non linéarité parfaite généralisée par les actions de groupe.

Actions de groupe (1)

Soit $(G, *)$ un groupe et X un ensemble non vide.

Une **action de groupe** (à gauche) de G sur X est un homomorphisme de groupes ϕ de G dans le groupe $S(X)$ des bijections de X .

En particulier,

- $\phi(e_G) = Id_X$;
- $\forall (g_1, g_2) \in G^2, \phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$.

Actions de groupe (2)

Notation

Pour $x \in X$ et $g \in G$, on pose

$$g.x = \phi(g)(x) .$$

Actions de groupe (3)

Soit G un groupe agissant (à gauche) sur un ensemble non vide X .

Pour $x \in X$, l'**application orbitale** de x est définie par

$$\begin{aligned}\phi_x : G &\rightarrow X \\ g &\mapsto g.x\end{aligned}$$

Actions de groupe (4)

Définition

L'action de G sur X par l'homomorphisme de groupes ϕ est

- **fidèle** si ϕ est injectif ;
- **régulière** si pour chaque $x \in X$, ϕ_x est bijective.

Exemples

- L'action naturelle de $S(X)$ sur X est fidèle ;
- L'action de G sur lui-même par translation (à gauche) est régulière.

Actions de groupe (4)

Définition

L'action de G sur X par l'homomorphisme de groupes ϕ est

- **fidèle** si ϕ est injectif ;
- **régulière** si pour chaque $x \in X$, ϕ_x est bijective.

Exemples

- L'action naturelle de $S(X)$ sur X est fidèle ;
- L'action de G sur lui-même par translation (à gauche) est régulière.

Actions de groupe (4)

Définition

L'action de G sur X par l'homomorphisme de groupes ϕ est

- **fidèle** si ϕ est injectif ;
- **régulière** si pour chaque $x \in X$, ϕ_x est bijective.

Exemples

- L'action naturelle de $S(X)$ sur X est fidèle ;
- L'action de G sur lui-même par translation (à gauche) est régulière.

Actions de groupe (4)

Définition

L'action de G sur X par l'homomorphisme de groupes ϕ est

- **fidèle** si ϕ est injectif ;
- **régulière** si pour chaque $x \in X$, ϕ_x est bijective.

Exemples

- L'action naturelle de $S(X)$ sur X est fidèle ;
- L'action de G sur lui-même par translation (à gauche) est régulière.

Actions de groupe (5)

Définition

Supposons que G_1 agisse sur X_1 par ϕ_1 et G_2 sur X_2 par ϕ_2 . Les deux actions sont dites **isomorphes** s'il existe un isomorphisme de groupes $\Psi : G_1 \rightarrow G_2$ et une application bijective $\theta : X_1 \rightarrow X_2$ tels que $\forall (g, x) \in G_1 \times X_1$,

$$\theta(\phi_1(g)(x)) = \phi_2(\Psi(g))(\theta(x)) .$$

Proposition

A un isomorphisme près, il n'existe qu'une et une seule action régulière définie sur un groupe G : son action par translation (à gauche).

Actions de groupe (5)

Définition

Supposons que G_1 agisse sur X_1 par ϕ_1 et G_2 sur X_2 par ϕ_2 . Les deux actions sont dites **isomorphes** s'il existe un isomorphisme de groupes $\Psi : G_1 \rightarrow G_2$ et une application bijective $\theta : X_1 \rightarrow X_2$ tels que $\forall (g, x) \in G_1 \times X_1$,

$$\theta(\phi_1(g)(x)) = \phi_2(\Psi(g))(\theta(x)) .$$

Proposition

A un isomorphisme près, il n'existe qu'une et une seule action régulière définie sur un groupe G : son action par translation (à gauche).

Définitions (1)

Soient G un groupe fini (commutatif ou non) agissant au moins **fidèlement** (à gauche) sur un ensemble fini non vide X et H un groupe fini abélien (en notation additive). Soit une application $f : X \rightarrow H$.

La **dérivée** de f (à gauche) dans la direction $g \in G$ est définie par

$$D_g f : X \rightarrow H$$

$$x \mapsto f(g.x) - f(x).$$

Définitions (1)

Soient G un groupe fini (commutatif ou non) agissant au moins **fidèlement** (à gauche) sur un ensemble fini non vide X et H un groupe fini abélien (en notation additive). Soit une application $f : X \rightarrow H$.

La **dérivée** de f (à gauche) dans la direction $g \in G$ est définie par

$$\begin{aligned} D_g f : X &\rightarrow H \\ x &\mapsto f(g.x) - f(x). \end{aligned}$$

Définitions (2)

Définition

La fonction $f : X \rightarrow H$ est dite **G-parfaitement non linéaire** si $\forall g \in G^*$, $D_g f$ est équilibrée, i.e. $\forall g \in G^*$ et $\forall \beta \in H$,

$$|\{x \in X \mid f(g.x) - f(x) = \beta\}| = \frac{|X|}{|H|}.$$

Définitions (3)

Remarque

Puisque l'action de G sur X est supposée fidèle, il n'existe pas de $g \in G^*$ telle que l'application

$$\begin{aligned} D_g : H^X &\rightarrow H^X \\ f &\mapsto D_g f \end{aligned}$$

soit identiquement nulle (*i.e.* identiquement égale à e_H).

Premiers résultats

Proposition

Soit $T(G)$ le groupe des translations de G .

Une fonction $f : G \rightarrow H$ est $T(G)$ -parfaitement non linéaire si et seulement si f est parfaitement non linéaire au sens des translations.

Proposition

Soit $f : X \rightarrow H$.

Si f est G -parfaitement non linéaire alors pour chaque sous-groupe G' de G , f est aussi G' -parfaitement non linéaire.

Premiers résultats

Proposition

Soit $T(G)$ le groupe des translations de G .

Une fonction $f : G \rightarrow H$ est $T(G)$ -parfaitement non linéaire si et seulement si f est parfaitement non linéaire au sens des translations.

Proposition

Soit $f : X \rightarrow H$.

Si f est G -parfaitement non linéaire alors pour chaque sous-groupe G' de G , f est aussi G' -parfaitement non linéaire.

Objectif

- Dualité dans le cas classique :
Non linéarité parfaite \Leftrightarrow Notion de fonction courbe (Carlet & Ding).
- Dualité dans le cas généralisé :
G-non linéarité parfaite \Leftrightarrow ??

Objectif

- Dualité dans le cas classique :
Non linéarité parfaite \Leftrightarrow Notion de fonction courbe (Carlet & Ding).
- Dualité dans le cas généralisé :
G-non linéarité parfaite \Leftrightarrow ??

Plan

- 1 Le groupe agissant G est commutatif ;
- 2 Le groupe agissant G est non commutatif.

Hypothèses et Notation

Soit la donnée (G, H, X) avec

- G et H deux groupes finis abéliens ;
- X un ensemble fini non vide ;
- G agit (au moins) **fidèlement** sur X (via ϕ).

Pour $f : X \rightarrow Y$ et $x \in X$, on définit $f_x : G \rightarrow Y$ par $f_x = f \circ \phi_x$.

Hypothèses et Notation

Soit la donnée (G, H, X) avec

- G et H deux groupes finis abéliens ;
- X un ensemble fini non vide ;
- G agit (au moins) **fidèlement** sur X (via ϕ).

Pour $f : X \rightarrow Y$ et $x \in X$, on définit $f_x : G \rightarrow Y$ par $f_x = f \circ \phi_x$.

Hypothèses et Notation

Soit la donnée (G, H, X) avec

- G et H deux groupes finis abéliens ;
- X un ensemble fini non vide ;
- G agit (au moins) **fidèlement** sur X (via ϕ).

Pour $f : X \rightarrow Y$ et $x \in X$, on définit $f_x : G \rightarrow Y$ par $f_x = f \circ \phi_x$.

Hypothèses et Notation

Soit la donnée (G, H, X) avec

- G et H deux groupes finis abéliens ;
- X un ensemble fini non vide ;
- G agit (au moins) **fidèlement** sur X (via ϕ).

Pour $f : X \rightarrow Y$ et $x \in X$, on définit $f_x : G \rightarrow Y$ par $f_x = f \circ \phi_x$.

Hypothèses et Notation

Soit la donnée (G, H, X) avec

- G et H deux groupes finis abéliens ;
- X un ensemble fini non vide ;
- G agit (au moins) **fidèlement** sur X (via ϕ).

Pour $f : X \rightarrow Y$ et $x \in X$, on définit $f_x : G \rightarrow Y$ par $f_x = f \circ \phi_x$.

Caractérisation duale

Théorème

Une fonction $f : X \rightarrow H$ est G -parfaitement non linéaire si et seulement si pour tout $\beta \in H^*$ et pour tout $g \in G$,

$$\frac{1}{|X|} \sum_{x \in X} |(\widehat{\chi_H^\beta \circ f_x})(g)|^2 = |G|.$$

Question

Si f est G -parfaitement non linéaire alors $\forall x \in X$, f_x est parfaitement non linéaire au sens de Carlet et Ding ?

Caractérisation duale : cas d'une action régulière

On suppose que G agit **régulièrement** sur X et on fixe $x_0 \in X$.
Une fonction $f : X \rightarrow H$ est G -parfaitement non linéaire si et seulement si la fonction $f_{x_0} : G \rightarrow H$ est parfaitement non linéaire au sens de Carlet et Ding.

Plan

- Hypothèses de base ;
- Rappels sur les représentations linéaires de groupe ;
- Dual de la non linéarité parfaite au sens des translations à gauche ;
- Dual de la G -Non linéarité parfaite.

Plan

- Hypothèses de base ;
- Rappels sur les représentations linéaires de groupe ;
- Dual de la non linéarité parfaite au sens des translations à gauche ;
- Dual de la G -Non linéarité parfaite.

Plan

- Hypothèses de base ;
- Rappels sur les représentations linéaires de groupe ;
- Dual de la non linéarité parfaite au sens des translations à gauche ;
- Dual de la G -Non linéarité parfaite.

Plan

- Hypothèses de base ;
- Rappels sur les représentations linéaires de groupe ;
- Dual de la non linéarité parfaite au sens des translations à gauche ;
- Dual de la G -Non linéarité parfaite.

Plan

- Hypothèses de base ;
- Rappels sur les représentations linéaires de groupe ;
- Dual de la non linéarité parfaite au sens des translations à gauche ;
- Dual de la G -Non linéarité parfaite.

Hypothèses de base

Soit la donnée (G, H, X) avec

- G un groupe fini **non abélien** ;
- H un groupe fini commutatif ;
- X un ensemble fini non vide sur lequel G agit à gauche (au moins) **fidèlement**.

Hypothèses de base

Soit la donnée (G, H, X) avec

- G un groupe fini **non abélien** ;
- H un groupe fini commutatif ;
- X un ensemble fini non vide sur lequel G agit à gauche (au moins) **fidèlement**.

Hypothèses de base

Soit la donnée (G, H, X) avec

- G un groupe fini **non abélien** ;
- H un groupe fini commutatif ;
- X un ensemble fini non vide sur lequel G agit à gauche (au moins) **fidèlement**.

Hypothèses de base

Soit la donnée (G, H, X) avec

- G un groupe fini **non abélien** ;
- H un groupe fini commutatif ;
- X un ensemble fini non vide sur lequel G agit à gauche (au moins) **fidèlement**.

Rappels sur les représentations linéaires (1)

Définition

Soit V un \mathbb{C} -espace vectoriel de dimension finie $\dim_{\mathbb{C}}(V)$. Une **représentation linéaire (unitaire)** de G sur V est la donnée d'un homomorphisme de groupes $\rho : G \rightarrow \mathbb{U}(V)$.

Une représentation $\rho : G \rightarrow \mathbb{U}(V)$ est dite **irréductible** si les seuls sous-espaces stables de V par ρ sont V lui-même et $\{0_V\}$.

Rappels sur les représentations linéaires (1)

Définition

Soit V un \mathbb{C} -espace vectoriel de dimension finie $\dim_{\mathbb{C}}(V)$. Une **représentation linéaire (unitaire)** de G sur V est la donnée d'un homomorphisme de groupes $\rho : G \rightarrow \mathbb{U}(V)$.

Une représentation $\rho : G \rightarrow \mathbb{U}(V)$ est dite **irréductible** si les seuls sous-espaces stables de V par ρ sont V lui-même et $\{0_V\}$.

Rappels sur les représentations linéaires (2)

Définition

Deux représentations ρ_1 et ρ_2 d'un même groupe G respectivement sur les espaces vectoriels V_1 et V_2 sont **isomorphes** s'il existe $\Psi : V_1 \rightarrow V_2$ un isomorphisme d'espaces vectoriels tel que pour tout $g \in G$,

$$\Psi \circ \rho_1(g) = \rho_2(g) \circ \Psi .$$

Rappels sur les représentations linéaires (3)

On note \widehat{G} un système de représentants des classes d'équivalence (pour la relation d'isomorphisme) des représentations irréductibles de G .

Si G est commutatif alors \widehat{G} correspond bien au groupe dual de G .

Rappels sur les représentations linéaires (3)

On note \widehat{G} un système de représentants des classes d'équivalence (pour la relation d'isomorphisme) des représentations irréductibles de G .

Si G est commutatif alors \widehat{G} correspond bien au groupe dual de G .

Rappels sur les représentations linéaires (4)

Définition

Soient $\varphi : G \rightarrow \mathbb{C}$ et $\rho \in \widehat{G}$ (associé à l'espace vectoriel V). On définit la **transformée de Fourier** de φ en ρ par

$$\widehat{\varphi}(\rho) = \sum_{x \in G} \varphi(x) \rho(x) \in \text{End}(V).$$

Dual de la non linéarité parfaite au sens des translations à gauche (1)

Rappel

Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** (à gauche) si pour tout $\alpha \in G^*$, sa dérivée (à gauche) $d_\alpha f$ est équilibrée.

Caractérisation duale

Une fonction $f : G \rightarrow H$ est parfaitement non linéaire (à gauche) si et seulement si $\forall \beta \in H^*$ et $\forall \rho \in \widehat{G}$ (associé à l'espace vectoriel V),

$$\widehat{(\chi_H^\beta \circ f(\rho))} \circ \widehat{(\chi_H^\beta \circ f(\rho))^*} = |G| Id_V.$$

Dual de la non linéarité parfaite au sens des translations à gauche (1)

Rappel

Une fonction $f : G \rightarrow H$ est **parfaitement non linéaire** (à gauche) si pour tout $\alpha \in G^*$, sa dérivée (à gauche) $d_\alpha f$ est équilibrée.

Caractérisation duale

Une fonction $f : G \rightarrow H$ est parfaitement non linéaire (à gauche) si et seulement si $\forall \beta \in H^*$ et $\forall \rho \in \widehat{G}$ (associé à l'espace vectoriel V),

$$\widehat{(\chi_H^\beta \circ f(\rho))} \circ \widehat{(\chi_H^\beta \circ f(\rho))^*} = |G| Id_V .$$

Dual de la non linéarité parfaite au sens des translations à gauche (2)

Par passage à la trace, on obtient

$$\| \widehat{\chi_H^\beta \circ f(\rho)} \|^2 = |G| \dim_{\mathbb{C}}(V) .$$

Question

Est-ce que si $\forall \rho \in \widehat{G}$, $\| \widehat{\chi_H^\beta \circ f(\rho)} \|^2 = |G| \dim_{\mathbb{C}}(V)$, f est parfaitement non linéaire au sens des translations à gauche ?

Dual de la non linéarité parfaite au sens des translations à gauche (2)

Par passage à la trace, on obtient

$$\| \widehat{\chi_H^\beta \circ f(\rho)} \|^2 = |G| \dim_{\mathbb{C}}(V) .$$

Question

Est-ce que si $\forall \rho \in \widehat{G}$, $\| \widehat{\chi_H^\beta \circ f(\rho)} \|^2 = |G| \dim_{\mathbb{C}}(V)$, f est parfaitement non linéaire au sens des translations à gauche ?

Dual de la non linéarité parfaite au sens des actions de groupe (1)

Rappel

Soient G un groupe fini non commutatif agissant fidèlement sur un ensemble fini non vide X et H un groupe fini abélien. Soit $f : X \rightarrow H$.

La fonction f est **G-parfaitement non linéaire** si $\forall g \in G^*$, $D_g f$ est équilibrée.

Problème

Déterminer la caractérisation duale de la G -non linéarité parfaite.

Dual de la non linéarité parfaite au sens des actions de groupe (1)

Rappel

Soient G un groupe fini non commutatif agissant fidèlement sur un ensemble fini non vide X et H un groupe fini abélien. Soit $f : X \rightarrow H$.

La fonction f est **G-parfaitement non linéaire** si $\forall g \in G^*$, $D_g f$ est équilibrée.

Problème

Déterminer la caractérisation duale de la G -non linéarité parfaite.

Dual de la non linéarité parfaite au sens des actions de groupe (2)

Caractérisation duale

Une fonction $f : X \rightarrow H$ est G -parfaitement non linéaire si et seulement si $\forall \beta \in H^*$ et $\forall \rho \in \widehat{G}$,

$$\frac{1}{|X|} \sum_{x \in X} (\widehat{\chi_H^\beta \circ f_x(\rho)}) \circ (\widehat{\chi_H^\beta \circ f_x(\rho)})^* = |G| Id_V .$$

Définition et Caractérisation combinatoire (1)

Définition

Soit G un groupe fini (abélien ou non) agissant à gauche (au moins) fidèlement sur un ensemble fini non vide X . Soit $D \subset X$. D est un **G - (v, k, λ) -ensemble à différences** de X si

- $v = |X|$;
- $k = |D|$;
- Pour chaque $g \in G^*$, l'équation $x = g \cdot y$ admet exactement λ solutions distinctes dans D^2 .

Définition et Caractérisation combinatoire (1)

Définition

Soit G un groupe fini (abélien ou non) agissant à gauche (au moins) fidèlement sur un ensemble fini non vide X . Soit $D \subset X$. D est un **G-(v, k, λ)-ensemble à différences** de X si

- $v = |X|$;
- $k = |D|$;
- Pour chaque $g \in G^*$, l'équation $x = g.y$ admet exactement λ solutions distinctes dans D^2 .

Définition et Caractérisation combinatoire (1)

Définition

Soit G un groupe fini (abélien ou non) agissant à gauche (au moins) fidèlement sur un ensemble fini non vide X . Soit $D \subset X$. D est un **G-(v, k, λ)-ensemble à différences** de X si

- $v = |X|$;
- $k = |D|$;
- Pour chaque $g \in G^*$, l'équation $x = g.y$ admet exactement λ solutions distinctes dans D^2 .

Définition et Caractérisation combinatoire (1)

Définition

Soit G un groupe fini (abélien ou non) agissant à gauche (au moins) fidèlement sur un ensemble fini non vide X . Soit $D \subset X$. D est un **G-(v, k, λ)-ensemble à différences** de X si

- $v = |X|$;
- $k = |D|$;
- Pour chaque $g \in G^*$, l'équation $x = g.y$ admet exactement λ solutions distinctes dans D^2 .

Définition et Caractérisation combinatoire (2)

Proposition

Soit G un groupe fini (abélien ou non) agissant à gauche (au moins) fidèlement sur un ensemble fini non vide X . Supposons en outre que $|X| \equiv 0 \pmod{4}$. Soit la fonction $f : X \rightarrow \mathbb{F}_2$.

- La fonction f est G -parfaitement non linéaire si et seulement si son support S_f est un G - (v, k, λ) -ensemble à différences de X tel que

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

- Si de plus l'action de G sur X est **régulière** alors la fonction f est G -parfaitement non linéaire si et seulement si son support S_f est un G - $(4n^2, 2n^2 \pm n, n(n \pm 1))$ -ensemble à différences de X (avec $|G| = |X| = 4n^2$).

Première construction (1)

Définition

Une **involution sans point fixe** de \mathbb{F}_2^m est une permutation σ telle que

- $\sigma^{-1} = \sigma$;
- $\forall x \in \mathbb{F}_2^m, \sigma(x) \neq x$.

Un **groupe d'involutions sans point fixe** G de \mathbb{F}_2^m est un sous-groupe de $S(\mathbb{F}_2^m)$ telle que tout élément de G^* est une involution sans point fixe.

Un groupe d'involutions sans point fixe de \mathbb{F}_2^m agit fidèlement sur \mathbb{F}_2^m .

Un groupe d'involutions sans point fixe d'ordre 2^n est isomorphe à \mathbb{F}_2^n .

Première construction (1)

Définition

Une **involution sans point fixe** de \mathbb{F}_2^m est une permutation σ telle que

- $\sigma^{-1} = \sigma$;
- $\forall x \in \mathbb{F}_2^m, \sigma(x) \neq x$.

Un **groupe d'involutions sans point fixe** G de \mathbb{F}_2^m est un sous-groupe de $S(\mathbb{F}_2^m)$ telle que tout élément de G^* est une involution sans point fixe.

Un groupe d'involutions sans point fixe de \mathbb{F}_2^m agit fidèlement sur \mathbb{F}_2^m .

Un groupe d'involutions sans point fixe d'ordre 2^n est isomorphe à \mathbb{F}_2^n .

Première construction (2)

Soit deux entiers m et n tel que $m \geq 2n$. Soit G un groupe d'involutions sans point fixe de \mathbb{F}_2^m d'ordre 2^{2n} . Alors pour tout $j \in \{0, \dots, 2^{m-2n}\}$, il existe un G - $(2^m, k_j, \lambda_j)$ -ensemble à différences de \mathbb{F}_2^m avec

- $k_j = (2^{2^{m-1}} - 2^{m-1})j + (2^{2^{m-1}} + 2^{m-1})(2^{m-2n} - j)$;
- $\lambda_j = (2^{2^{(m-1)}} - 2^{m-1})j + (2^{2^{(m-1)}} + 2^{m-1})(2^{m-2n} - j)$.

En particulier, pour chaque j , $2^m = 4(k_j - \lambda_j)$.

Première construction (3)

Remarque

Pour $m \geq 2n$, il existe des groupes G d'involutions sans point fixe de \mathbb{F}_2^m d'ordre 2^n . Par exemple, si l'on considère les éléments α de \mathbb{F}_2^m pour lesquels les dernières $m - 2n$ coordonnées valent zéro. Alors les translations par de tels α constituent un groupe G approprié. Il en est de même ses groupes conjugués.

Première construction (4)

Cette construction permet d'exhiber des fonctions booléennes G -parfaitement non linéaires en particulier dans des cas où des fonctions courbes classiques n'existent pas. Supposons en effet que $m = 9$ et $n = 4$ donc $|\mathbb{F}_2^9| = 512$ et $|G| = 256$. Alors il existe des G -ensembles à différences dont les paramètres sont de la forme : $(512, 240, 112)$, $(512, 256, 128)$ ou $(512, 272, 144)$.

Seconde construction - Hyperplan (1)

Soient deux entiers m et n . Soit G un groupe d'involutions sans point fixe de \mathbb{F}_2^{2m+n} d'ordre 2^m . Alors il existe un G - $(2^{2m+n}, 2^n((2^{m-1} - 1)(2^m - 1) + 1), 2^n(2^{m-1} - 1)(2^{m-1} - 2))$ -ensemble à différences de \mathbb{F}_2^{2m+n} . En particulier les paramètres satisfont l'équation $v = 4(k - \lambda)$.

Seconde construction - Hyperplan (2)

Remarque

Si m et n sont des entiers **impairs** alors ni $f : \mathbb{F}_2^{2m+n} \rightarrow \mathbb{F}_2$ ni $f_x : G \simeq \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ (pour $x \in \mathbb{F}_2^{2m+n}$) ne peuvent être parfaitement non linéaires (ou courbes) au sens traditionnel.

- Fonctions booléennes courbes en dimensions impaires ;
- Cryptanalyse “différentielle” généralisée :
Soit une boîte-S $S : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$, alors on peut construire une involution sans point fixe $\sigma_S \in S(\mathbb{F}_2^6)$ telle que $\forall x \in \mathbb{F}_2^6$,

$$S(x) \oplus S(\sigma_S(x)) = (0, 0, 0, 0) .$$

- Fonctions booléennes courbes en dimensions impaires ;
- Cryptanalyse “différentielle” généralisée :
Soit une boîte-S $S : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$, alors on peut construire une involution sans point fixe $\sigma_S \in S(\mathbb{F}_2^6)$ telle que $\forall x \in \mathbb{F}_2^6$,

$$S(x) \oplus S(\sigma_S(x)) = (0, 0, 0, 0) .$$

- Fonctions booléennes courbes en dimensions impaires ;
- Cryptanalyse “différentielle” généralisée :

Soit une boîte-S $S : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$, alors on peut construire une involution sans point fixe $\sigma_S \in S(\mathbb{F}_2^6)$ telle que $\forall x \in \mathbb{F}_2^6$,

$$S(x) \oplus S(\sigma_S(x)) = (0, 0, 0, 0) .$$

- Fonctions booléennes courbes en dimensions impaires ;
- Cryptanalyse “différentielle” généralisée :
Soit une boîte-S $S : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$, alors on peut construire une involution sans point fixe $\sigma_S \in S(\mathbb{F}_2^6)$ telle que $\forall x \in \mathbb{F}_2^6$,

$$S(x) \oplus S(\sigma_S(x)) = (0, 0, 0, 0) .$$

Publications

- Actes de conférences internationales :
 - Avec S. Harari : *Generalized Boolean Bent Functions*, Indocrypt 2004 (Chennai, Inde) ;
 - Avec S. Harari : *Group Action-based Perfect NonLinearity (Extended Abstract)*, WCC 2005 (Bergen, Norvège) ;
- Articles dans des revues internationales :
 - Avec S. Harari : *Group Action-based Perfect NonLinearity*, GESTS International Transactions on Computer Science and Engineering, vol. 12, n. 1, Juin 2005 ;
 - Avec J. A. Davis : *G-perfect nonlinear functions and G-difference sets*, soumis à Design, Codes and Cryptography ;
- Future(s) soumission(s) : la partie non commutative de la G-non linéarité parfaite.

MERCI!
Allez l'OM!

tu-logo

ur-logo

MERCI!
Allez l'OM!

tu-logo

ur-logo