Fonctions presque parfaitement non linéaires sur des groupes non abéliens

Laurent Poinsot

LIPN - UMR CNRS 7030
Université Paris-Nord XIII - Institut Galilée

Séminaire d'Informatique et Algèbre Appliquée - IMATH

Le 7 février 2012 à l'Université du Sud Toulon-Var

Table des matières

Table des matières

Ce travail est tiré de :

Non-Boolean almost perfect nonlinear functions on non-Abelian groups,

Laurent Poinsot et Alexander Pott,
International Journal of Foundations of Computer Science, volume 22, numéro 6, pages 1351–1367, 2011.

Ce travail est tiré de :

Non-Boolean almost perfect nonlinear functions on non-Abelian groups,

Laurent Poinsot et Alexander Pott,
International Journal of Foundations of Computer Science, volume 22, numéro 6, pages 1351–1367, 2011.

Voir également :

Non Abelian bent functions,

Laurent Poinsot,
Cryptography and Communications, volume 4, numéro 1, pages 1–23, 2012.

La plupart des résultats au sujet de la non linéarité cryptographique (non linéarité parfaite, presque parfaite, fonctions maximalement non linéaires, fonctions courbes, presque courbes, *etc.*) relèvent des fonctions booléennes.

La plupart des résultats au sujet de la non linéarité cryptographique (non linéarité parfaite, presque parfaite, fonctions maximalement non linéaires, fonctions courbes, presque courbes, *etc.*) relèvent des fonctions booléennes.

Autrement dit, ils concernent les fonctions $f : G \to H$ où G, H sont deux groupes abéliens finis qui se trouvent être des $\mathbb{Z}_2$-modules, *i.e.*, tout élément non trivial est d'ordre deux.

La plupart des résultats au sujet de la non linéarité cryptographique (non linéarité parfaite, presque parfaite, fonctions maximalement non linéaires, fonctions courbes, presque courbes, *etc.*) relèvent des fonctions booléennes.

Autrement dit, ils concernent les fonctions $f : G \to H$ où G, H sont deux groupes abéliens finis qui se trouvent être des $\mathbb{Z}_2$-modules, *i.e.*, tout élément non trivial est d'ordre deux. Ces groupes sont appelés les 2-groupes abéliens élémentaires.

La plupart des résultats au sujet de la non linéarité cryptographique (non linéarité parfaite, presque parfaite, fonctions maximalement non linéaires, fonctions courbes, presque courbes, *etc.*) relèvent des fonctions booléennes.

Autrement dit, ils concernent les fonctions $f : G \to H$ où G, H sont deux groupes abéliens finis qui se trouvent être des $\mathbb{Z}_2$-modules, *i.e.*, tout élément non trivial est d'ordre deux. Ces groupes sont appelés les 2-groupes abéliens élémentaires.

Même si ces groupes paraissent très naturels en cryptographie, *a priori* aucune règle nous interdit d'utiliser des groupes plus compliqués voire même non abéliens.

La plupart des résultats au sujet de la non linéarité cryptographique (non linéarité parfaite, presque parfaite, fonctions maximalement non linéaires, fonctions courbes, presque courbes, *etc.*) relèvent des fonctions booléennes.

Autrement dit, ils concernent les fonctions $f : G \to H$ où G, H sont deux groupes abéliens finis qui se trouvent être des $\mathbb{Z}_2$-modules, *i.e.*, tout élément non trivial est d'ordre deux. Ces groupes sont appelés les 2-groupes abéliens élémentaires.

Même si ces groupes paraissent très naturels en cryptographie, *a priori* aucune règle nous interdit d'utiliser des groupes plus compliqués voire même non abéliens.

L'objectif de cet exposé est de discuter ces notions standards dans le cadre non commutatif.

Table des matières

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Elles mesurent la résistance de ces cryptosystèmes essentiellement face à deux attaques :

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Elles mesurent la résistance de ces cryptosystèmes essentiellement face à deux attaques : l'attaque différentielle et l'attaque linéaire.

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Elles mesurent la résistance de ces cryptosystèmes essentiellement face à deux attaques : l'attaque différentielle et l'attaque linéaire.

Soit donc E un tel cryptosystème :

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Elles mesurent la résistance de ces cryptosystèmes essentiellement face à deux attaques : l'attaque différentielle et l'attaque linéaire.

Soit donc E un tel cryptosystème : $C = E(M, K)$ désigne alors le message chiffré obtenu à partir du message clair M et d'une clef K.

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Elles mesurent la résistance de ces cryptosystèmes essentiellement face à deux attaques : l'attaque différentielle et l'attaque linéaire.

Soit donc E un tel cryptosystème : $C = E(M, K)$ désigne alors le message chiffré obtenu à partir du message clair M et d'une clef K. On suppose par ailleurs que M, C et K sont des blocs de bits

Cadre général de la non linéarité

Les diverses mesures de non linéarité en cryptographie ont pour cadre général l'étude de la sécurité des systèmes de chiffrement à clef secrète.

Elles mesurent la résistance de ces cryptosystèmes essentiellement face à deux attaques : l'attaque différentielle et l'attaque linéaire.

Soit donc E un tel cryptosystème : $C = E(M, K)$ désigne alors le message chiffré obtenu à partir du message clair M et d'une clef K. On suppose par ailleurs que M, C et K sont des blocs de bits (de sorte que l'on peut appliquer l'opération $\oplus$ de ou-exclusif).

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

L'objectif de l'attaquant est de découvrir (des bits de) la clef de chiffrement employée K.

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

L'objectif de l'attaquant est de découvrir (des bits de) la clef de chiffrement employée K.

Cette attaque repose sur le principe suivant : on suppose que $E(M, K) = S(M \oplus K)$ où S est une application non linéaire.

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

L'objectif de l'attaquant est de découvrir (des bits de) la clef de chiffrement employée K.

Cette attaque repose sur le principe suivant : on suppose que $E(M, K) = S(M \oplus K)$ où S est une application non linéaire. Remarquons que si $M \oplus M' = \alpha$, alors $(M \oplus K) \oplus (M' \oplus K) = \alpha$,

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

L'objectif de l'attaquant est de découvrir (des bits de) la clef de chiffrement employée K.

Cette attaque repose sur le principe suivant : on suppose que $E(M, K) = S(M \oplus K)$ où S est une application non linéaire. Remarquons que si $M \oplus M' = \alpha$, alors $(M \oplus K) \oplus (M' \oplus K) = \alpha$, autrement dit la somme avec la clef n'a aucune influence sur la différence en entrée.

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

L'objectif de l'attaquant est de découvrir (des bits de) la clef de chiffrement employée K.

Cette attaque repose sur le principe suivant : on suppose que $E(M, K) = S(M \oplus K)$ où S est une application non linéaire. Remarquons que si $M \oplus M' = \alpha$, alors $(M \oplus K) \oplus (M' \oplus K) = \alpha$, autrement dit la somme avec la clef n'a aucune influence sur la différence en entrée.

Une différentielle (α, β) représente une différence en entrée $M \oplus M' = \alpha$, et une différence en sortie $C \oplus C' = \beta$ (C, C' sont les chiffrés de M, M' avec la même clef).

Principe général de l'attaque différentielle

L'attaque différentielle a été découverte par Biham et Shamir, et utilisée pour attaquer des procédés de chiffrement par blocs itérés (dont le DES et l'AES).

L'objectif de l'attaquant est de découvrir (des bits de) la clef de chiffrement employée K.

Cette attaque repose sur le principe suivant : on suppose que $E(M, K) = S(M \oplus K)$ où S est une application non linéaire. Remarquons que si $M \oplus M' = \alpha$, alors $(M \oplus K) \oplus (M' \oplus K) = \alpha$, autrement dit la somme avec la clef n'a aucune influence sur la différence en entrée.

Une différentielle (α, β) représente une différence en entrée $M \oplus M' = \alpha$, et une différence en sortie $C \oplus C' = \beta$ (C, C' sont les chiffrés de M, M' avec la même clef). Puisque E n'est pas linéaire, $\beta \neq \alpha$.

Associée à une telle différentielle (α, β), on introduit la probabilité conditionnelle :

$$P(E(M,K) \oplus E(M',K) = \beta \mid M \oplus M' = \alpha)$$

où M et K sont deux variables aléatoires indépendantes et uniformément distribuées.

Associée à une telle différentielle (α, β), on introduit la probabilité conditionnelle :

$$P(E(M,K) \oplus E(M',K) = \beta \mid M \oplus M' = \alpha)$$

où M et K sont deux variables aléatoires indépendantes et uniformément distribuées. L'attaquant calcule ces probabilités (en tirant au hasard M et K).

Associée à une telle différentielle (α, β), on introduit la probabilité conditionnelle :

$$P(E(M,K) \oplus E(M',K) = \beta \mid M \oplus M' = \alpha)$$

où M et K sont deux variables aléatoires indépendantes et uniformément distribuées. L'attaquant calcule ces probabilités (en tirant au hasard M et K).

Dans l'idéal, une telle probabilité est égale à $\frac{1}{2^n}$ où n est le nombre de bits d'un message chiffré.

Associée à une telle différentielle (α, β), on introduit la probabilité conditionnelle :

$$P(E(M,K) \oplus E(M',K) = \beta \mid M \oplus M' = \alpha)$$

où M et K sont deux variables aléatoires indépendantes et uniformément distribuées. L'attaquant calcule ces probabilités (en tirant au hasard M et K).

Dans l'idéal, une telle probabilité est égale à $\frac{1}{2^n}$ où n est le nombre de bits d'un message chiffré.

La cryptanalyse différentielle exploite un biais statistique obtenu lorsqu'une différence β particulière, pour une différence α fixée, apparaît avec une grande probabilité (supérieure à $\frac{1}{2^n}$).

Cette attaque est utilisée pour découvrir la clef utilisée au dernier tour d'un chiffrement itéré à r rondes.

Cette attaque est utilisée pour découvrir la clef utilisée au dernier tour d'un chiffrement itéré à r rondes.

Pour cela l'attaquant détermine une différentielle (α, β) dont la probabilité d'occurrence est élevée, et où β représente la différence en sortie du $r-1$-ème tour.

Cette attaque est utilisée pour découvrir la clef utilisée au dernier tour d'un chiffrement itéré à r rondes.

Pour cela l'attaquant détermine une différentielle (α, β) dont la probabilité d'occurrence est élevée, et où β représente la différence en sortie du $r-1$-ème tour.

Il tire au hasard un texte clair M et chiffre M et $M \oplus \alpha$ (il obtient C et C').

Cette attaque est utilisée pour découvrir la clef utilisée au dernier tour d'un chiffrement itéré à r rondes.

Pour cela l'attaquant détermine une différentielle (α, β) dont la probabilité d'occurrence est élevée, et où β représente la différence en sortie du $r-1$-ème tour.

Il tire au hasard un texte clair M et chiffre M et $M \oplus \alpha$ (il obtient C et C').

Il recherche ensuite toutes les clefs possibles K_r du dernier tour telles que $S_{K_r}^{-1}(C) \oplus S_{K_r}^{-1}(C') = \beta$, où S_K désigne l'application inversible $M \mapsto S(M \oplus K)$.

Cette attaque est utilisée pour découvrir la clef utilisée au dernier tour d'un chiffrement itéré à r rondes.

Pour cela l'attaquant détermine une différentielle (α, β) dont la probabilité d'occurrence est élevée, et où β représente la différence en sortie du $r-1$-ème tour.

Il tire au hasard un texte clair M et chiffre M et $M \oplus \alpha$ (il obtient C et C').

Il recherche ensuite toutes les clefs possibles K_r du dernier tour telles que $S_{K_r}^{-1}(C) \oplus S_{K_r}^{-1}(C') = \beta$, où S_K désigne l'application inversible $M \mapsto S(M \oplus K)$.

Après un certain nombre d'essais, il devine la clef K_r utilisée.

Pour présenter un niveau élevé de sécurité face à cette attaque, il faut que la composante non linéaire S de E «ressemble» le moins possible à une application linéaire.

Pour présenter un niveau élevé de sécurité face à cette attaque, il faut que la composante non linéaire S de E «ressemble» le moins possible à une application linéaire.

Dans l'idéal, S doit satisfaire :

Pour présenter un niveau élevé de sécurité face à cette attaque, il faut que la composante non linéaire S de E «ressemble» le moins possible à une application linéaire.

Dans l'idéal, S doit satisfaire :

$$| \{ x \in \mathbb{Z}_2^m : S(x \oplus \alpha) \oplus S(x) = \beta \} | = 2^{m-n}$$

quels que soient α non nul et β (m désigne le nombre de bits en entrée de S).

Pour présenter un niveau élevé de sécurité face à cette attaque, il faut que la composante non linéaire S de E «ressemble» le moins possible à une application linéaire.

Dans l'idéal, S doit satisfaire :

$$| \{ x \in \mathbb{Z}_2^m : S(x \oplus \alpha) \oplus S(x) = \beta \} | = 2^{m-n}$$

quels que soient α non nul et β (m désigne le nombre de bits en entrée de S). Dans ce cas, S est dite être parfaitement non linéaire.

Pour présenter un niveau élevé de sécurité face à cette attaque, il faut que la composante non linéaire S de E «ressemble» le moins possible à une application linéaire.

Dans l'idéal, S doit satisfaire :

$$| \{ x \in \mathbb{Z}_2^m : S(x \oplus \alpha) \oplus S(x) = \beta \} | = 2^{m-n}$$

quels que soient α non nul et β (m désigne le nombre de bits en entrée de S). Dans ce cas, S est dite être parfaitement non linéaire.

Cette notion étant très contraignante, il faut parfois l'affaiblir :

Pour présenter un niveau élevé de sécurité face à cette attaque, il faut que la composante non linéaire S de E «ressemble» le moins possible à une application linéaire.

Dans l'idéal, S doit satisfaire :

$$| \{ x \in \mathbb{Z}_2^m : S(x \oplus \alpha) \oplus S(x) = \beta \} | = 2^{m-n}$$

quels que soient α non nul et β (m désigne le nombre de bits en entrée de S). Dans ce cas, S est dite être parfaitement non linéaire.

Cette notion étant très contraignante, il faut parfois l'affaiblir : on obtient les fonctions presque parfaitement non linéaires.

Principe général de l'attaque linéaire

L'attaque linéaire a été découverte par Matsui et publiée en 1983.

Principe général de l'attaque linéaire

L'attaque linéaire a été découverte par Matsui et publiée en 1983.

Elle tire profit d'équations linéaires liant des bits des textes clair M, chiffré C et de la clef K.

Principe général de l'attaque linéaire

L'attaque linéaire a été découverte par Matsui et publiée en 1983.

Elle tire profit d'équations linéaires liant des bits des textes clair M, chiffré C et de la clef K.

Une telle équation linéaire générale prend la forme suivante :

$$M_{i_1} \oplus \cdots \oplus M_{i_r} \oplus C_{j_1} \oplus \cdots \oplus C_{j_s} = K_\ell \ .$$

Principe général de l'attaque linéaire

L'attaque linéaire a été découverte par Matsui et publiée en 1983.

Elle tire profit d'équations linéaires liant des bits des textes clair M, chiffré C et de la clef K.

Une telle équation linéaire générale prend la forme suivante :

$$M_{i_1} \oplus \cdots \oplus M_{i_r} \oplus C_{j_1} \oplus \cdots \oplus C_{j_s} = K_\ell \ .$$

Dans un cryptosystème idéal, K_ℓ devrait prendre la valeur 0 avec une probabilité de $\frac{1}{2}$.

Principe général de l'attaque linéaire

L'attaque linéaire a été découverte par Matsui et publiée en 1983.

Elle tire profit d'équations linéaires liant des bits des textes clair M, chiffré C et de la clef K.

Une telle équation linéaire générale prend la forme suivante :

$$M_{i_1} \oplus \cdots \oplus M_{i_r} \oplus C_{j_1} \oplus \cdots \oplus C_{j_s} = K_\ell \ .$$

Dans un cryptosystème idéal, K_ℓ devrait prendre la valeur 0 avec une probabilité de $\frac{1}{2}$.

En général, la partie non linéaire S d'un cryptosystème est elle-même constituée de boîtes-S mettant en relation certains bits du message clair, du chiffré et de la clef.

Principe général de l'attaque linéaire

L'attaque linéaire a été découverte par Matsui et publiée en 1983.

Elle tire profit d'équations linéaires liant des bits des textes clair M, chiffré C et de la clef K.

Une telle équation linéaire générale prend la forme suivante :

$$M_{i_1} \oplus \cdots \oplus M_{i_r} \oplus C_{j_1} \oplus \cdots \oplus C_{j_s} = K_\ell \ .$$

Dans un cryptosystème idéal, K_ℓ devrait prendre la valeur 0 avec une probabilité de $\frac{1}{2}$.

En général, la partie non linéaire S d'un cryptosystème est elle-même constituée de boîtes-S mettant en relation certains bits du message clair, du chiffré et de la clef. L'attaquant peut exploiter de telles relations linéaires afin de deviner certains bits de la clef secrète employée.

Les fonctions qui résistent le mieux à la cryptanalyse linéaire sont les fonctions courbes.

Les fonctions qui résistent le mieux à la cryptanalyse linéaire sont les fonctions courbes.

Comme la non linéarité parfaite, le concept de fonctions courbes est excessivement contraint.

Les fonctions qui résistent le mieux à la cryptanalyse linéaire sont les fonctions courbes.

Comme la non linéarité parfaite, le concept de fonctions courbes est excessivement contraint. On montre qu'en fait les deux notions sont équivalentes.

Les fonctions qui résistent le mieux à la cryptanalyse linéaire sont les fonctions courbes.

Comme la non linéarité parfaite, le concept de fonctions courbes est excessivement contraint. On montre qu'en fait les deux notions sont équivalentes.

Les fonctions sous-optimales vis-à-vis de la solidité face à l'attaque linéaire sont les fonctions presque courbes et maximalement non linéaires.

Table des matières

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs,

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative,

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative, d'ordre m et n respectivement.

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative, d'ordre m et n respectivement.

Une application $f : H \to K$ est dite parfaitement non linéaire

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative, d'ordre m et n respectivement.

Une application $f : H \to K$ est dite parfaitement non linéaire si pour chaque $a \in H$, $a \neq 1_H$, et pour chaque $b \in K$, la quantité

$$\delta_f(a, b) = |\{ g \in H : f(ag)(f(g))^{-1} = b \}|$$

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative, d'ordre m et n respectivement.

Une application $f : H \to K$ est dite parfaitement non linéaire si pour chaque $a \in H$, $a \neq 1_H$, et pour chaque $b \in K$, la quantité

$$\delta_f(a, b) = |\{ g \in H : f(ag)(f(g))^{-1} = b \}|$$

est constante, et donc $\delta_f(a, b) = \frac{m}{n}$.

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative, d'ordre m et n respectivement.

Une application $f : H \to K$ est dite parfaitement non linéaire si pour chaque $a \in H$, $a \neq 1_H$, et pour chaque $b \in K$, la quantité

$$\delta_f(a, b) = |\{ g \in H : f(ag)(f(g))^{-1} = b \}|$$

est constante, et donc $\delta_f(a, b) = \frac{m}{n}$.

L'article Highly nonlinear mappings de Claude Carlet et Cunsheng Ding (Journal of Complexity, volume 20, pages 205–244, 2004) constitue un état de l'art très complet sur ce sujet.

Fonctions parfaitement non linéaires

Soient H, K deux groupes finis commutatifs, en notation multiplicative, d'ordre m et n respectivement.

Une application $f : H \to K$ est dite parfaitement non linéaire si pour chaque $a \in H$, $a \neq 1_H$, et pour chaque $b \in K$, la quantité

$$\delta_f(a, b) = |\{ g \in H : f(ag)(f(g))^{-1} = b \}|$$

est constante, et donc $\delta_f(a, b) = \frac{m}{n}$.

L'article Highly nonlinear mappings de Claude Carlet et Cunsheng Ding (Journal of Complexity, volume 20, pages 205–244, 2004) constitue un état de l'art très complet sur ce sujet.

L'article Nonlinear functions in Abelian groups and relative difference sets d'Alexander Pott (Discrete Applied Mathematics, volume 138, pages 195–232, 2004) l'est également.

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Par ailleurs il n'y a pas de fonction parfaitement non linéaire si H et K sont deux 2-groupes abéliens élémentaires de même ordre.

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Par ailleurs il n'y a pas de fonction parfaitement non linéaire si H et K sont deux 2-groupes abéliens élémentaires de même ordre. En fait, il existe un résultat plus général.

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Par ailleurs il n'y a pas de fonction parfaitement non linéaire si H et K sont deux 2-groupes abéliens élémentaires de même ordre. En fait, il existe un résultat plus général.

Théorème (classique)

Soit H un groupe d'ordre $m = 2^a$, et soit K un groupe abélien d'ordre $n = 2^b$.

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Par ailleurs il n'y a pas de fonction parfaitement non linéaire si H et K sont deux 2-groupes abéliens élémentaires de même ordre. En fait, il existe un résultat plus général.

Théorème (classique)

Soit H un groupe d'ordre $m = 2^a$, et soit K un groupe abélien d'ordre $n = 2^b$. Aucune application parfaitement non linéaire n'existe si l'une des deux conditions est satisfaite

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Par ailleurs il n'y a pas de fonction parfaitement non linéaire si H et K sont deux 2-groupes abéliens élémentaires de même ordre. En fait, il existe un résultat plus général.

Théorème (classique)

Soit H un groupe d'ordre $m = 2^a$, et soit K un groupe abélien d'ordre $n = 2^b$. Aucune application parfaitement non linéaire n'existe si l'une des deux conditions est satisfaite

1. a est impair.

Résultats de non-existence

Clairement, si n ne divise pas m, alors il n'y a aucune fonction parfaitement non linéaire.

Par ailleurs il n'y a pas de fonction parfaitement non linéaire si H et K sont deux 2-groupes abéliens élémentaires de même ordre. En fait, il existe un résultat plus général.

Théorème (classique)

Soit H un groupe d'ordre $m = 2^a$, et soit K un groupe abélien d'ordre $n = 2^b$. Aucune application parfaitement non linéaire n'existe si l'une des deux conditions est satisfaite

1. a est impair.
2. a est pair, $a = 2s$, et $b \geq s + 1$.

Fonctions presque parfaitement non linéaires

Puisque les fonctions parfaitement non linéaires n'existent pas dans de nombreux (et intéressants) cas,

Fonctions presque parfaitement non linéaires

Puisque les fonctions parfaitement non linéaires n'existent pas dans de nombreux (et intéressants) cas, il faut se résoudre à relaxer les contraintes et considérer des formes plus faibles de non linéarité.

Fonctions presque parfaitement non linéaires

Puisque les fonctions parfaitement non linéaires n'existent pas dans de nombreux (et intéressants) cas, il faut se résoudre à relaxer les contraintes et considérer des formes plus faibles de non linéarité.

Soient H, K deux groupes abéliens finis (d'ordre m, n respectifs), et notons $G = H \times K$ leur produit direct.

Fonctions presque parfaitement non linéaires

Puisque les fonctions parfaitement non linéaires n'existent pas dans de nombreux (et intéressants) cas, il faut se résoudre à relaxer les contraintes et considérer des formes plus faibles de non linéarité.

Soient H, K deux groupes abéliens finis (d'ordre m, n respectifs), et notons $G = H \times K$ leur produit direct. Une application $f : H \to K$ est dite presque parfaitement non linéaire si

$$\sum_{(a,b)\in G} \delta_f(a,b)^2 \leq \sum_{(a,b)\in G} \delta_g(a,b)^2$$

pour toute application $g : H \to K$.

Fonctions presque parfaitement non linéaires

Puisque les fonctions parfaitement non linéaires n'existent pas dans de nombreux (et intéressants) cas, il faut se résoudre à relaxer les contraintes et considérer des formes plus faibles de non linéarité.

Soient H, K deux groupes abéliens finis (d'ordre m, n respectifs), et notons $G = H \times K$ leur produit direct. Une application $f : H \to K$ est dite presque parfaitement non linéaire si

$$\sum_{(a,b)\in G} \delta_f(a,b)^2 \leq \sum_{(a,b)\in G} \delta_g(a,b)^2$$

pour toute application $g : H \to K$.

Remarque

Les définitions de non linéarité parfaite et presque parfaite n'utilisent pas la commutativité des groupes et seront donc appliquées sans modification dans le contexte non commutatif.

Graphe d'une application

À chaque application $f : H \to K$ on associe son graphe $D_f \subseteq G$:

Graphe d'une application

À chaque application $f : H \to K$ on associe son graphe $D_f \subseteq G$:

$$D_f = \{ (g, f(g)) : g \in H \} .$$

Graphe d'une application

À chaque application $f : H \to K$ on associe son graphe $D_f \subseteq G$:

$$D_f = \{ (g, f(g)) : g \in H \} .$$

Cet ensemble joue un rôle important dans l'étude des propriétés de non linéarité des applications.

Graphe d'une application

À chaque application $f : H \to K$ on associe son graphe $D_f \subseteq G$:

$$D_f = \{ (g, f(g)) : g \in H \} .$$

Cet ensemble joue un rôle important dans l'étude des propriétés de non linéarité des applications.

Par exemple, f est parfaitement non linéaire si, et seulement si, son graphe est un $(m, n, m, \frac{m}{n})$-ensemble à différences dans G scindé relativement au sous-groupe distingué K.

Rappels : Les ensembles à différences

Soit G un groupe d'ordre v.

Rappels : Les ensembles à différences

Soit G un groupe d'ordre v. Supposons que K soit un sous-groupe distingué de G de cardinal n.

Rappels : Les ensembles à différences

Soit G un groupe d'ordre v. Supposons que K soit un sous-groupe distingué de G de cardinal n. Un ensemble $D \subseteq G$ de cardinal k est un (v, n, k, λ)-ensemble à différences relativement à K

Rappels : Les ensembles à différences

Soit G un groupe d'ordre v. Supposons que K soit un sous-groupe distingué de G de cardinal n. Un ensemble $D \subseteq G$ de cardinal k est un (v, n, k, λ)-ensemble à différences relativement à K si la liste des quotients xy^{-1} avec $x \neq y \in D$ contient chaque élément de G/K exactement λ fois,

Rappels : Les ensembles à différences

Soit G un groupe d'ordre v. Supposons que K soit un sous-groupe distingué de G de cardinal n. Un ensemble $D \subseteq G$ de cardinal k est un (v, n, k, λ)-ensemble à différences relativement à K si la liste des quotients xy^{-1} avec $x \neq y \in D$ contient chaque élément de G/K exactement λ fois, et aucun élément $z \in K$, $z \neq 1$, ne possède une telle écriture.

Rappels : Les ensembles à différences

Soit G un groupe d'ordre v. Supposons que K soit un sous-groupe distingué de G de cardinal n. Un ensemble $D \subseteq G$ de cardinal k est un (v, n, k, λ)-ensemble à différences relativement à K si la liste des quotients xy^{-1} avec $x \neq y \in D$ contient chaque élément de G/K exactement λ fois, et aucun élément $z \in K$, $z \neq 1$, ne possède une telle écriture.

Cet ensemble à différences est dit scindé si $G \cong H \times K$ pour un sous-groupe H de G.

L'algèbre d'un groupe

En général de telles structures combinatoires sont étudiées à l'aide de la notion d'algèbre d'un groupe.

L'algèbre d'un groupe

En général de telles structures combinatoires sont étudiées à l'aide de la notion d'algèbre d'un groupe.

Soient G un groupe et R un anneau commutatif et unitaire.

L'algèbre d'un groupe

En général de telles structures combinatoires sont étudiées à l'aide de la notion d'algèbre d'un groupe.

Soient G un groupe et R un anneau commutatif et unitaire. La R-algèbre du groupe G, notée $R[G]$, est définie comme le R-module librement engendré par G et muni de la multiplication étendant celle de G par bilinéarité.

L'algèbre d'un groupe

En général de telles structures combinatoires sont étudiées à l'aide de la notion d'algèbre d'un groupe.

Soient G un groupe et R un anneau commutatif et unitaire. La R-algèbre du groupe G, notée $R[G]$, est définie comme le R-module librement engendré par G et muni de la multiplication étendant celle de G par bilinéarité.

Plus précisément, ses éléments sont des sommes formelles $\sum_{g \in G} d_g g$ où les coefficients $d_g \in R$ sont tous nuls sauf un nombre au plus fini.

L'algèbre d'un groupe

En général de telles structures combinatoires sont étudiées à l'aide de la notion d'algèbre d'un groupe.

Soient G un groupe et R un anneau commutatif et unitaire. La R-algèbre du groupe G, notée $R[G]$, est définie comme le R-module librement engendré par G et muni de la multiplication étendant celle de G par bilinéarité.

Plus précisément, ses éléments sont des sommes formelles $\sum_{g \in G} d_g g$ où les coefficients $d_g \in R$ sont tous nuls sauf un nombre au plus fini.

- Addition : $\sum_{g \in G} d_g g + \sum_{g \in G} d'_g g = \sum_{g \in G} (d_g + d'_g) g$.

L'algèbre d'un groupe

En général de telles structures combinatoires sont étudiées à l'aide de la notion d'algèbre d'un groupe.

Soient G un groupe et R un anneau commutatif et unitaire. La R-algèbre du groupe G, notée $R[G]$, est définie comme le R-module librement engendré par G et muni de la multiplication étendant celle de G par bilinéarité.

Plus précisément, ses éléments sont des sommes formelles $\sum_{g\in G} d_g g$ où les coefficients $d_g \in R$ sont tous nuls sauf un nombre au plus fini.

- Addition : $\sum_{g\in G} d_g g + \sum_{g\in G} d'_g g = \sum_{g\in G} (d_g + d'_g) g.$

- Multiplication : $\left(\sum_{g\in G} d_g g\right)\left(\sum_{g\in G} d'_g g\right) = \sum_{g\in G}\left(\sum_{hk=g} d_h d'_k\right) g.$

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Lorsque $R = \mathbb{C}$, pour chaque $D \in \mathbb{C}[G]$, on définit $D^{(-1)} = \sum_{g \in G} \overline{d_g} g^{-1}$.

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Lorsque $R = \mathbb{C}$, pour chaque $D \in \mathbb{C}[G]$, on définit $D^{(-1)} = \sum_{g \in G} \overline{d_g} g^{-1}$.

(Attention : la notation est trompeuse car $D^{(-1)}$ n'est pas l'inverse de D.
L'opération $D \mapsto D^{(-1)}$ est une involution d'algèbre :
$(D + E)^{(-1)} = D^{(-1)} + E^{(-1)}$, et $(DE)^{(-1)} = E^{(-1)} D^{(-1)}$.)

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Lorsque $R = \mathbb{C}$, pour chaque $D \in \mathbb{C}[G]$, on définit $D^{(-1)} = \sum_{g \in G} \overline{d_g} g^{-1}$.

(Attention : la notation est trompeuse car $D^{(-1)}$ n'est pas l'inverse de D.
L'opération $D \mapsto D^{(-1)}$ est une involution d'algèbre :
$(D + E)^{(-1)} = D^{(-1)} + E^{(-1)}$, et $(DE)^{(-1)} = E^{(-1)} D^{(-1)}$.)

En particulier, si $f : H \to K$, et si $G = H \times K$, alors

$$D_f D_f^{(-1)} = \sum_{(a,b) \in G} \delta_f(a,b)(a,b) \in \mathbb{Z}[G] \subseteq \mathbb{C}[G] \ .$$

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Lorsque $R = \mathbb{C}$, pour chaque $D \in \mathbb{C}[G]$, on définit $D^{(-1)} = \sum_{g \in G} \overline{d_g} g^{-1}$.

(Attention : la notation est trompeuse car $D^{(-1)}$ n'est pas l'inverse de D. L'opération $D \mapsto D^{(-1)}$ est une involution d'algèbre : $(D + E)^{(-1)} = D^{(-1)} + E^{(-1)}$, et $(DE)^{(-1)} = E^{(-1)} D^{(-1)}$.)

En particulier, si $f : H \to K$, et si $G = H \times K$, alors

$$D_f D_f^{(-1)} = \sum_{(a,b) \in G} \delta_f(a,b)(a,b) \in \mathbb{Z}[G] \subseteq \mathbb{C}[G] \ .$$

Tout sous-ensemble fini $D \subseteq G$ peut être plongé dans $R[G]$ *via* sa fonction indicatrice $1_D(x) = 1$ si $x \in D$, $1_D(x) = 0$ si $x \notin D$

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Lorsque $R = \mathbb{C}$, pour chaque $D \in \mathbb{C}[G]$, on définit $D^{(-1)} = \sum_{g \in G} \overline{d_g} g^{-1}$.

(Attention : la notation est trompeuse car $D^{(-1)}$ n'est pas l'inverse de D. L'opération $D \mapsto D^{(-1)}$ est une involution d'algèbre : $(D + E)^{(-1)} = D^{(-1)} + E^{(-1)}$, et $(DE)^{(-1)} = E^{(-1)} D^{(-1)}$.)

En particulier, si $f : H \to K$, et si $G = H \times K$, alors

$$D_f D_f^{(-1)} = \sum_{(a,b) \in G} \delta_f(a,b)(a,b) \in \mathbb{Z}[G] \subseteq \mathbb{C}[G] \ .$$

Tout sous-ensemble fini $D \subseteq G$ peut être plongé dans $R[G]$ *via* sa fonction indicatrice $1_D(x) = 1$ si $x \in D$, $1_D(x) = 0$ si $x \notin D$ par

$$D \mapsto \sum_{g \in G} 1_D(g) g \ .$$

Remarque

En termes de catégories, $R[\cdot]$ est l'adjoint à gauche du foncteur d'oubli de la catégorie des R-algèbres dans celles des groupes.

Lorsque $R = \mathbb{C}$, pour chaque $D \in \mathbb{C}[G]$, on définit $D^{(-1)} = \sum_{g \in G} \overline{d_g} g^{-1}$.

(Attention : la notation est trompeuse car $D^{(-1)}$ n'est pas l'inverse de D. L'opération $D \mapsto D^{(-1)}$ est une involution d'algèbre : $(D + E)^{(-1)} = D^{(-1)} + E^{(-1)}$, et $(DE)^{(-1)} = E^{(-1)} D^{(-1)}$.)

En particulier, si $f : H \to K$, et si $G = H \times K$, alors

$$D_f D_f^{(-1)} = \sum_{(a,b) \in G} \delta_f(a,b)(a,b) \in \mathbb{Z}[G] \subseteq \mathbb{C}[G] \ .$$

Tout sous-ensemble fini $D \subseteq G$ peut être plongé dans $R[G]$ *via* sa fonction indicatrice $1_D(x) = 1$ si $x \in D$, $1_D(x) = 0$ si $x \notin D$ par

$$D \mapsto \sum_{g \in G} 1_D(g) g \ .$$

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$.

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. À cause de la torsion, les éléments $\chi(g)$, $g \in G$, appartiennent au cercle unité.

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. À cause de la torsion, les éléments $\chi(g)$, $g \in G$, appartiennent au cercle unité.

L'ensemble des caractères est un groupe abélien fini pour les opérations ponctuelles, appelé le groupe des caractères de G, et noté $\widehat{G}$.

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. À cause de la torsion, les éléments $\chi(g)$, $g \in G$, appartiennent au cercle unité.

L'ensemble des caractères est un groupe abélien fini pour les opérations ponctuelles, appelé le groupe des caractères de G, et noté $\widehat{G}$. Il se trouve être isomorphe à G.

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. À cause de la torsion, les éléments $\chi(g)$, $g \in G$, appartiennent au cercle unité.

L'ensemble des caractères est un groupe abélien fini pour les opérations ponctuelles, appelé le groupe des caractères de G, et noté $\widehat{G}$. Il se trouve être isomorphe à G.

Le caractère $\chi_0 : g \in G \mapsto 1$ est le caractère principal de G (identité du groupe $\widehat{G}$).

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. À cause de la torsion, les éléments $\chi(g)$, $g \in G$, appartiennent au cercle unité.

L'ensemble des caractères est un groupe abélien fini pour les opérations ponctuelles, appelé le groupe des caractères de G, et noté $\widehat{G}$. Il se trouve être isomorphe à G.

Le caractère $\chi_0 : g \in G \mapsto 1$ est le caractère principal de G (identité du groupe $\widehat{G}$).

Les caractères d'un groupe produit direct $G = H \times K$ sont donnés par $\chi = \chi_H \otimes \chi_K : (a, b) \in H \times K \mapsto \chi(a, b) = \chi_H(a)\chi_K(b)$ où χ_H parcourt $\widehat{H}$, χ_K parcourt $\widehat{K}$.

Groupe des caractères

Un caractère χ d'un groupe abélien fini G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. À cause de la torsion, les éléments $\chi(g)$, $g \in G$, appartiennent au cercle unité.

L'ensemble des caractères est un groupe abélien fini pour les opérations ponctuelles, appelé le groupe des caractères de G, et noté $\widehat{G}$. Il se trouve être isomorphe à G.

Le caractère $\chi_0 : g \in G \mapsto 1$ est le caractère principal de G (identité du groupe $\widehat{G}$).

Les caractères d'un groupe produit direct $G = H \times K$ sont donnés par $\chi = \chi_H \otimes \chi_K : (a, b) \in H \times K \mapsto \chi(a, b) = \chi_H(a)\chi_K(b)$ où χ_H parcourt $\widehat{H}$, χ_K parcourt $\widehat{K}$.

Un caractère $\chi \in \widehat{G}$ s'étend de manière naturelle (fonctorielle) en un homomorphisme d'algèbres de $\mathbb{C}[G]$ dans $\mathbb{C}$ par

$$\chi(D) = \sum_{g \in G} d_g \chi(g)$$

Fonctions maximalement non linéaires

En utilisant les caractères on peut introduire un autre critère de non linéarité

Fonctions maximalement non linéaires

En utilisant les caractères on peut introduire un autre critère de non linéarité : une fonction $f : H \to K$ est dite maximalement non linéaire si

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| \leq \max_{\chi_K \neq \chi_0} |\chi(D_g)|$$

pour tout $g : H \to K$,

Fonctions maximalement non linéaires

En utilisant les caractères on peut introduire un autre critère de non linéarité : une fonction $f : H \to K$ est dite maximalement non linéaire si

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| \leq \max_{\chi_K \neq \chi_0} |\chi(D_g)|$$

pour tout $g : H \to K$, ou de façon équivalente,

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| = \min_{g \in H \to K} \max_{\chi_K \neq \chi_0} |\chi(D_g)| \ .$$

Fonctions maximalement non linéaires

En utilisant les caractères on peut introduire un autre critère de non linéarité : une fonction $f : H \to K$ est dite maximalement non linéaire si

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| \leq \max_{\chi_K \neq \chi_0} |\chi(D_g)|$$

pour tout $g : H \to K$, ou de façon équivalente,

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| = \min_{g \in H \to K} \max_{\chi_K \neq \chi_0} |\chi(D_g)| \ .$$

La valeur $\sqrt{|H|}$ est un minorant pour la quantité $\max_{\chi_K \neq \chi_0} |\chi(D_f)|$.

Fonctions maximalement non linéaires

En utilisant les caractères on peut introduire un autre critère de non linéarité : une fonction $f : H \to K$ est dite maximalement non linéaire si

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| \leq \max_{\chi_K \neq \chi_0} |\chi(D_g)|$$

pour tout $g : H \to K$, ou de façon équivalente,

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| = \min_{g \in H \to K} \max_{\chi_K \neq \chi_0} |\chi(D_g)| \ .$$

La valeur $\sqrt{|H|}$ est un minorant pour la quantité $\max_{\chi_K \neq \chi_0} |\chi(D_f)|$. Une fonction qui atteint cette borne est dite courbe.

Fonctions maximalement non linéaires

En utilisant les caractères on peut introduire un autre critère de non linéarité : une fonction $f : H \to K$ est dite maximalement non linéaire si

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| \leq \max_{\chi_K \neq \chi_0} |\chi(D_g)|$$

pour tout $g : H \to K$, ou de façon équivalente,

$$\max_{\chi_K \neq \chi_0} |\chi(D_f)| = \min_{g \in H \to K} \max_{\chi_K \neq \chi_0} |\chi(D_g)| \ .$$

La valeur $\sqrt{|H|}$ est un minorant pour la quantité $\max_{\chi_K \neq \chi_0} |\chi(D_f)|$. Une fonction qui atteint cette borne est dite courbe.

Un résultat classique énonce qu'une fonction est courbe si, et seulement si, elle est parfaitement non linéaire.

Comme la non linéarité parfaite, la notion d'application presque parfaitement non linéaire peut s'exprimer à l'aide des caractères.

Comme la non linéarité parfaite, la notion d'application presque parfaitement non linéaire peut s'exprimer à l'aide des caractères.

Théorème (classique)

Soient H, K deux groupes abéliens finis.

Comme la non linéarité parfaite, la notion d'application presque parfaitement non linéaire peut s'exprimer à l'aide des caractères.

Théorème (classique)

Soient H, K deux groupes abéliens finis. Une fonction $f : H \to K$ est presque parfaitement non linéaire si, et seulement si,

$$\sum_{\chi \in \widehat{G}} |\chi(D_f)|^4 \leq \sum_{\chi \in \widehat{G}} |\chi(D_g)|^4$$

quel que soit $g : H \to K$.

Comme la non linéarité parfaite, la notion d'application presque parfaitement non linéaire peut s'exprimer à l'aide des caractères.

Théorème (classique)

Soient H, K deux groupes abéliens finis. Une fonction $f : H \to K$ est presque parfaitement non linéaire si, et seulement si,

$$\sum_{\chi \in \widehat{G}} |\chi(D_f)|^4 \leq \sum_{\chi \in \widehat{G}} |\chi(D_g)|^4$$

quel que soit $g : H \to K$.

Cette caractérisation n'est possible que dans le contexte commutatif.

Comme la non linéarité parfaite, la notion d'application presque parfaitement non linéaire peut s'exprimer à l'aide des caractères.

Théorème (classique)

Soient H, K deux groupes abéliens finis. Une fonction $f : H \to K$ est presque parfaitement non linéaire si, et seulement si,

$$\sum_{\chi \in \widehat{G}} |\chi(D_f)|^4 \leq \sum_{\chi \in \widehat{G}} |\chi(D_g)|^4$$

quel que soit $g : H \to K$.

Cette caractérisation n'est possible que dans le contexte commutatif. Un théorème similaire sera donné ultérieurement dans le cadre non commutatif.

Table des matières

Une représentation (linéaire) d'un groupe fini G est un couple (ρ, V) où V est un espace vectoriel complexe de dimension finie et ρ est un homomorphisme de groupes de G dans le groupe linéaire $\mathrm{GL}(V)$ de V.

Une représentation (linéaire) d'un groupe fini G est un couple (ρ, V) où V est un espace vectoriel complexe de dimension finie et ρ est un homomorphisme de groupes de G dans le groupe linéaire $\mathrm{GL}(V)$ de V. On notera parfois V_ρ l'espace sur lequel agit la représentation ρ, de sorte que l'on pourra dire que ρ est une représentation de G.

Une représentation (linéaire) d'un groupe fini G est un couple (ρ, V) où V est un espace vectoriel complexe de dimension finie et ρ est un homomorphisme de groupes de G dans le groupe linéaire $\mathrm{GL}(V)$ de V. On notera parfois V_ρ l'espace sur lequel agit la représentation ρ, de sorte que l'on pourra dire que ρ est une représentation de G.

La dimension $\dim \rho$ de la représentation (ρ, V) est définie comme la dimension de V sur $\mathbb{C}$.

Une représentation (linéaire) d'un groupe fini G est un couple (ρ, V) où V est un espace vectoriel complexe de dimension finie et ρ est un homomorphisme de groupes de G dans le groupe linéaire $\mathrm{GL}(V)$ de V. On notera parfois V_ρ l'espace sur lequel agit la représentation ρ, de sorte que l'on pourra dire que ρ est une représentation de G.

La dimension $\dim \rho$ de la représentation (ρ, V) est définie comme la dimension de V sur $\mathbb{C}$.

Deux représentations $(\rho_1, V_1), (\rho_2, V_2)$ d'un même groupe G sont dites équivalentes s'il existe un isomorphisme linéaire $T : V_1 \to V_2$ tel que pour tout $g \in G$,

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

Une représentation (linéaire) d'un groupe fini G est un couple (ρ, V) où V est un espace vectoriel complexe de dimension finie et ρ est un homomorphisme de groupes de G dans le groupe linéaire $\mathrm{GL}(V)$ de V. On notera parfois V_ρ l'espace sur lequel agit la représentation ρ, de sorte que l'on pourra dire que ρ est une représentation de G.

La dimension $\dim \rho$ de la représentation (ρ, V) est définie comme la dimension de V sur $\mathbb{C}$.

Deux représentations $(\rho_1, V_1), (\rho_2, V_2)$ d'un même groupe G sont dites équivalentes s'il existe un isomorphisme linéaire $T : V_1 \to V_2$ tel que pour tout $g \in G$,

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

(Autrement dit, T est un isomorphisme linéaire et est G-équivariante relativement aux actions de G sur V_1 et sur V_2.)

Soient (ρ, V) une représentation de G, et W un sous-espace de V.

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Une représentation (ρ, V) de G est dite irréductible si les seuls sous-espaces de V invariants pas ρ sont (0) et V lui-même.

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Une représentation (ρ, V) de G est dite irréductible si les seuls sous-espaces de V invariants pas ρ sont (0) et V lui-même.

On note $\tilde{G}$ un système de représentants de représentations irréductibles (pour la relation d'équivalence).

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Une représentation (ρ, V) de G est dite irréductible si les seuls sous-espaces de V invariants pas ρ sont (0) et V lui-même.

On note $\tilde{G}$ un système de représentants de représentations irréductibles (pour la relation d'équivalence). Autrement dit, quels que soient $\rho_1, \rho_2 \in \tilde{G}$, ρ_i est irréductible, et si $\rho_1 \neq \rho_2$, alors ρ_1 et ρ_2 sont non équivalentes.

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Une représentation (ρ, V) de G est dite irréductible si les seuls sous-espaces de V invariants pas ρ sont (0) et V lui-même.

On note $\tilde{G}$ un système de représentants de représentations irréductibles (pour la relation d'équivalence). Autrement dit, quels que soient $\rho_1, \rho_2 \in \tilde{G}$, ρ_i est irréductible, et si $\rho_1 \neq \rho_2$, alors ρ_1 et ρ_2 sont non équivalentes.

Si G est un groupe abélien, alors $\tilde{G}$ n'est autre que $\widehat{G}$.

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Une représentation (ρ, V) de G est dite irréductible si les seuls sous-espaces de V invariants pas ρ sont (0) et V lui-même.

On note $\tilde{G}$ un système de représentants de représentations irréductibles (pour la relation d'équivalence). Autrement dit, quels que soient $\rho_1, \rho_2 \in \tilde{G}$, ρ_i est irréductible, et si $\rho_1 \neq \rho_2$, alors ρ_1 et ρ_2 sont non équivalentes.

Si G est un groupe abélien, alors $\tilde{G}$ n'est autre que $\widehat{G}$.

Les représentations de dimension un de G sont en bijection avec les caractères de l'abélianisé $G/[G, G]$ de G ($[G, G]$ est le groupe dérivé de G engendré par les commutateurs $ghg^{-1}h^{-1}$).

Soient (ρ, V) une représentation de G, et W un sous-espace de V. W est dit invariant par ρ si $\rho(g)(W) \subseteq W$ (et donc $\rho(g)(W) = W$) pour tout $g \in G$.

Une représentation (ρ, V) de G est dite irréductible si les seuls sous-espaces de V invariants pas ρ sont (0) et V lui-même.

On note $\tilde{G}$ un système de représentants de représentations irréductibles (pour la relation d'équivalence). Autrement dit, quels que soient $\rho_1, \rho_2 \in \tilde{G}$, ρ_i est irréductible, et si $\rho_1 \neq \rho_2$, alors ρ_1 et ρ_2 sont non équivalentes.

Si G est un groupe abélien, alors $\tilde{G}$ n'est autre que $\widehat{G}$.

Les représentations de dimension un de G sont en bijection avec les caractères de l'abélianisé $G/[G, G]$ de G ($[G, G]$ est le groupe dérivé de G engendré par les commutateurs $ghg^{-1}h^{-1}$).

La représentation $(\rho_0, \mathbb{C})$ qui envoie $g \in G$ sur 1 est appelée la représentation principale de G.

Remarque sur la théorie des ensembles

La notion d'équivalence entre représentations d'un même groupe fini définit une relation d'équivalence sur la classe propre (ce n'est pas un ensemble !) de toutes les représentations linéaires de G.

Remarque sur la théorie des ensembles

La notion d'équivalence entre représentations d'un même groupe fini définit une relation d'équivalence sur la classe propre (ce n'est pas un ensemble !) de toutes les représentations linéaires de G. On peut par contre montrer qu'une classe contenant un représentant, et un seul, de chaque classe d'équivalence est un ensemble

Remarque sur la théorie des ensembles

La notion d'équivalence entre représentations d'un même groupe fini définit une relation d'équivalence sur la classe propre (ce n'est pas un ensemble !) de toutes les représentations linéaires de G. On peut par contre montrer qu'une classe contenant un représentant, et un seul, de chaque classe d'équivalence est un ensemble et même un ensemble fini si on ne s'intéresse qu'aux représentations irréductibles : son cardinal est égal au nombre de classes de conjugaison de G.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

- Produit tensoriel : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

- Produit tensoriel : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ par
$(\rho_1 \otimes \rho_2)(g)(v \otimes w) = \rho_1(g)(v) \otimes \rho_2(g)(w)$.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

- Produit tensoriel : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ par
$(\rho_1 \otimes \rho_2)(g)(v \otimes w) = \rho_1(g)(v) \otimes \rho_2(g)(w)$.

Soit $G = H \times K$.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

- Produit tensoriel : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ par
$(\rho_1 \otimes \rho_2)(g)(v \otimes w) = \rho_1(g)(v) \otimes \rho_2(g)(w)$.

Soit $G = H \times K$. Toutes les représentations irréductibles (et elles seules) de G sont équivalentes à un produit tensoriel $\rho_H \otimes \rho_K$ de représentations irréductibles de H et de K.

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

- Produit tensoriel : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ par
$(\rho_1 \otimes \rho_2)(g)(v \otimes w) = \rho_1(g)(v) \otimes \rho_2(g)(w)$.

Soit $G = H \times K$. Toutes les représentations irréductibles (et elles seules) de G sont équivalentes à un produit tensoriel $\rho_H \otimes \rho_K$ de représentations irréductibles de H et de K.

Les (classes d'équivalence de) représentations irréductibles forment les «briques de bases» pour construire, à partir des deux opérations, toutes les représentations linéaires de dimension finie d'un groupe

Opérations sur les représentations

- Somme directe : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ par
$(\rho_1 \oplus \rho_2)(g)(v + w) = \rho_1(g)(v) + \rho_2(g)(w)$.

- Produit tensoriel : Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G.
On définit $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ par
$(\rho_1 \otimes \rho_2)(g)(v \otimes w) = \rho_1(g)(v) \otimes \rho_2(g)(w)$.

Soit $G = H \times K$. Toutes les représentations irréductibles (et elles seules) de G sont équivalentes à un produit tensoriel $\rho_H \otimes \rho_K$ de représentations irréductibles de H et de K.

Les (classes d'équivalence de) représentations irréductibles forment les «briques de bases» pour construire, à partir des deux opérations, toutes les représentations linéaires de dimension finie d'un groupe : l'anneau (de Grothendieck) des représentations de G est librement engendré par les représentations irréductibles.

Une représentation (ρ, V) est dite unitaire si quels que soient $g \in G$, $\rho(g^{-1}) = \rho(g)^*$ où $*$ désigne l'adjoint d'un opérateur par rapport à un produit scalaire.

Une représentation (ρ, V) est dite unitaire si quels que soient $g \in G$, $\rho(g^{-1}) = \rho(g)^*$ où $*$ désigne l'adjoint d'un opérateur par rapport à un produit scalaire. On peut montrer que toute représentation (ρ, V) est équivalente à une représentation unitaire.

Une représentation (ρ, V) est dite unitaire si quels que soient $g \in G$, $\rho(g^{-1}) = \rho(g)^*$ où $*$ désigne l'adjoint d'un opérateur par rapport à un produit scalaire. On peut montrer que toute représentation (ρ, V) est équivalente à une représentation unitaire.

Convention : À partir de maintenant on suppose que $\tilde{G}$ est un système de représentations irréductibles unitaires.

Une représentation (ρ, V) de G peut être étendue en un homomorphisme d'algèbres de $\mathbb{C}[G]$ dans $\mathrm{End}(V)$ par

$$\rho(D) = \sum_{g \in G} d_g \rho(g)$$

où $D = \sum_{g \in G} d_g g$.

Une représentation (ρ, V) de G peut être étendue en un homomorphisme d'algèbres de $\mathbb{C}[G]$ dans $\mathrm{End}(V)$ par

$$\rho(D) = \sum_{g \in G} d_g \rho(g)$$

où $D = \sum_{g \in G} d_g g$.

On montre que $\rho(G) = 0_V$ si $\rho \neq \rho_0$, et $\rho_0(G) = |G|$.

La transformée de Fourier

Pour $D \in \mathbb{C}[G]$, on peut définir sa transformée de Fourier par

$$\tilde{D} = (\rho(D))_{\rho \in \tilde{G}} \in \bigoplus_{\rho \in \tilde{G}} \mathrm{End}(V_\rho)$$

où V_ρ désigne l'espace vectoriel sur lequel ρ agit.

La transformée de Fourier

Pour $D \in \mathbb{C}[G]$, on peut définir sa transformée de Fourier par

$$\tilde{D} = (\rho(D))_{\rho \in \tilde{G}} \in \bigoplus_{\rho \in \tilde{G}} \mathrm{End}(V_\rho)$$

où V_ρ désigne l'espace vectoriel sur lequel ρ agit.

La transformation de Fourier est l'application $\mathcal{F} : \mathbb{C}[G] \to \bigoplus_{\rho \in \tilde{G}} \mathrm{End}(V)$ telle que $\mathcal{F}(D) = \tilde{D}$.

Table des matières

Formule d'inversion de Fourier et l'égalité de Parseval

Soit G un groupe fini (pas nécessairement commutatif).

Formule d'inversion de Fourier et l'égalité de Parseval

Soit G un groupe fini (pas nécessairement commutatif). Soit $D = \sum_{g \in G} d_g g \in \mathbb{C}[G]$.

Formule d'inversion de Fourier et l'égalité de Parseval

Soit G un groupe fini (pas nécessairement commutatif). Soit $D = \sum_{g \in G} d_g g \in \mathbb{C}[G]$.

1. Formule d'inversion de Fourier : $d_g = \frac{1}{|G|} \sum_{\rho \in \tilde{G}} tr(\rho(D) \circ \rho(g^{-1}))$

   où tr désigne la trace d'un opérateur.

Formule d'inversion de Fourier et l'égalité de Parseval

Soit G un groupe fini (pas nécessairement commutatif). Soit $D = \sum_{g \in G} d_g g \in \mathbb{C}[G]$.

1. Formule d'inversion de Fourier : $d_g = \frac{1}{|G|} \sum_{\rho \in \tilde{G}} tr(\rho(D) \circ \rho(g^{-1}))$

   où tr désigne la trace d'un opérateur.

2. Égalité de Parseval : $\sum_{g \in G} |d_g|^2 = \frac{1}{|G|} \sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D)\|^2$

   où $\|T\|$ est la norme de Frobénius d'un opérateur linéaire donnée par $\|T\|^2 = tr(T \circ T^*)$.

Formule d'inversion de Fourier et l'égalité de Parseval

Soit G un groupe fini (pas nécessairement commutatif). Soit $D = \sum_{g \in G} d_g g \in \mathbb{C}[G]$.

1. Formule d'inversion de Fourier : $d_g = \frac{1}{|G|} \sum_{\rho \in \tilde{G}} tr(\rho(D) \circ \rho(g^{-1}))$

   où tr désigne la trace d'un opérateur.

2. Égalité de Parseval : $\sum_{g \in G} |d_g|^2 = \frac{1}{|G|} \sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D)\|^2$

   où $\|T\|$ est la norme de Frobénius d'un opérateur linéaire donnée par $\|T\|^2 = tr(T \circ T^*)$. (On utilise ici le fait que les représentants choisis pour former $\tilde{G}$ sont unitaires.)

En utilisant les représentations de groupe, il est possible d'obtenir une caractérisation des fonctions presque parfaitement non linéaires.

En utilisant les représentations de groupe, il est possible d'obtenir une caractérisation des fonctions presque parfaitement non linéaires.

Théorème

Soient H, K deux groupes finis.

En utilisant les représentations de groupe, il est possible d'obtenir une caractérisation des fonctions presque parfaitement non linéaires.

Théorème

Soient H, K deux groupes finis. Soit $G = H \times K$.

En utilisant les représentations de groupe, il est possible d'obtenir une caractérisation des fonctions presque parfaitement non linéaires.

Théorème

Soient H, K deux groupes finis. Soit $G = H \times K$. Une application $f : H \to K$ est presque parfaitement non linéaire si, et seulement si,

$$\sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_f)\|^4 \leq \sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_g)\|^4$$

pour tout $g : H \to K$.

En utilisant les représentations de groupe, il est possible d'obtenir une caractérisation des fonctions presque parfaitement non linéaires.

Théorème

Soient H, K deux groupes finis. Soit $G = H \times K$. Une application $f : H \to K$ est presque parfaitement non linéaire si, et seulement si,

$$\sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_f)\|^4 \leq \sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_g)\|^4$$

pour tout $g : H \to K$.

Rappelons que dans le cas commutatif, nous avions : Une fonction $f : H \to K$ est presque parfaitement non linéaire si, et seulement si,

$$\sum_{\chi \in \widehat{G}} |\chi(D_f)|^4 \leq \sum_{\chi \in \widehat{G}} |\chi(D_g)|^4$$

quel que soit $g : H \to K$.

Preuve :

Nous avons $D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b)$.

Preuve :

Nous avons $D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b)$. De sorte que par l'égalité de Parseval, nous obtenons :

$$\sum_{(a,b)\in G} \delta_f(a,b)^2 \quad = \quad \frac{1}{|G|} \sum_{\rho\in\tilde{G}} \dim \rho \|\rho(D_f D_f^{(-1)})\|^2$$

Preuve :

Nous avons $D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b)$. De sorte que par l'égalité de Parseval, nous obtenons :

$$\begin{aligned}\sum_{(a,b)\in G} \delta_f(a,b)^2 &= \frac{1}{|G|}\sum_{\rho\in\tilde{G}} \dim\rho \|\rho(D_f D_f^{(-1)})\|^2 \\ &= \frac{1}{|G|}\sum_{\rho\in\tilde{G}} \dim\rho \|\rho(D_f)\circ\rho(D_f)^*\|^2\end{aligned}$$

Preuve :

Nous avons $D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b)$. De sorte que par l'égalité de Parseval, nous obtenons :

$$\begin{aligned}
\sum_{(a,b)\in G} \delta_f(a,b)^2 &= \frac{1}{|G|} \sum_{\rho\in\tilde{G}} \dim \rho \|\rho(D_f D_f^{(-1)})\|^2 \\
&= \frac{1}{|G|} \sum_{\rho\in\tilde{G}} \dim \rho \|\rho(D_f) \circ \rho(D_f)^*\|^2 \\
&= \frac{1}{|G|} \sum_{\rho\in\tilde{G}} \dim \rho \|\rho(D_f)\|^4 \ .
\end{aligned}$$

Preuve :

Nous avons $D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b)$. De sorte que par l'égalité de Parseval, nous obtenons :

$$\begin{aligned}\sum_{(a,b)\in G} \delta_f(a,b)^2 &= \frac{1}{|G|}\sum_{\rho\in\tilde{G}} \dim\rho \|\rho(D_f D_f^{(-1)})\|^2 \\ &= \frac{1}{|G|}\sum_{\rho\in\tilde{G}} \dim\rho \|\rho(D_f)\circ\rho(D_f)^*\|^2 \\ &= \frac{1}{|G|}\sum_{\rho\in\tilde{G}} \dim\rho \|\rho(D_f)\|^4 \ .\end{aligned}$$

Puisqu'une fonction $f : H \to K$ est presque parfaitement non linéaire si, et seulement si, quel que soit $g : H \to K$ tel que

$$\sum_{(a,b)\in G} \delta_f(a,b)^2 \leq \sum_{(a,b)\in G} \delta_g(a,b)^2 \ ,$$

cela conclut la preuve.

Fonctions maximalement non linéaires

On peut employer les représentations de groupe pour établir un critère similaire de non linéarité maximale dans le cadre non commutatif.

Fonctions maximalement non linéaires

On peut employer les représentations de groupe pour établir un critère similaire de non linéarité maximale dans le cadre non commutatif.

Soient H, K deux groupes finis d'ordre m et n respectivement, et $f : H \to K$.

Fonctions maximalement non linéaires

On peut employer les représentations de groupe pour établir un critère similaire de non linéarité maximale dans le cadre non commutatif.

Soient H, K deux groupes finis d'ordre m et n respectivement, et $f : H \to K$.

Pour certaines représentations $\rho = \rho_H \otimes \rho_K \in \widetilde{H \times K}$, les valeurs de $\rho(D_f)$ sont connues.

Fonctions maximalement non linéaires

On peut employer les représentations de groupe pour établir un critère similaire de non linéarité maximale dans le cadre non commutatif.

Soient H, K deux groupes finis d'ordre m et n respectivement, et $f : H \to K$.

Pour certaines représentations $\rho = \rho_H \otimes \rho_K \in \widetilde{H \times K}$, les valeurs de $\rho(D_f)$ sont connues.

- $\rho_0(D_f) = m$.

Fonctions maximalement non linéaires

On peut employer les représentations de groupe pour établir un critère similaire de non linéarité maximale dans le cadre non commutatif.

Soient H, K deux groupes finis d'ordre m et n respectivement, et $f : H \to K$.

Pour certaines représentations $\rho = \rho_H \otimes \rho_K \in \widetilde{H \times K}$, les valeurs de $\rho(D_f)$ sont connues.

- $\rho_0(D_f) = m$.

- $\rho(D_f) = 0_V$ si $\rho = \rho_H \otimes \rho_0$, et (ρ_H, V) n'est pas la représentation principale de H.

En effet,

$$\rho_0(D_f) \quad = \quad \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_0(a,b)$$

En effet,

$$\begin{aligned}\rho_0(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_0(a,b) \\ &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\end{aligned}$$

En effet,

$$\begin{aligned}
\rho_0(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_0(a,b) \\
&= \sum_{(a,b)\in G} 1_{D_f}(a,b) \\
&= |D_f|
\end{aligned}$$

En effet,

$$\begin{aligned}
\rho_0(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_0(a,b) \\
&= \sum_{(a,b)\in G} 1_{D_f}(a,b) \\
&= |D_f| \\
&= |H|
\end{aligned}$$

En effet,

$$\begin{aligned}
\rho_0(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_0(a,b) \\
&= \sum_{(a,b)\in G} 1_{D_f}(a,b) \\
&= |D_f| \\
&= |H| \\
&= m\ .
\end{aligned}$$

Supposons que $\rho = \rho_H \otimes \rho_0$ avec (ρ_H, V) non principale de H.

Supposons que $\rho = \rho_H \otimes \rho_0$ avec (ρ_H, V) non principale de H. Alors on a :

$$\rho(D_f) \quad = \quad \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_H(a) \otimes \rho_0(b)$$

Supposons que $\rho = \rho_H \otimes \rho_0$ avec (ρ_H, V) non principale de H. Alors on a :

$$\begin{aligned} \rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_H(a) \otimes \rho_0(b) \\ &= \sum_{a\in H} \rho_H(a) \otimes \rho_0(f(a)) \end{aligned}$$

Supposons que $\rho = \rho_H \otimes \rho_0$ avec (ρ_H, V) non principale de H. Alors on a :

$$\begin{aligned}
\rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_H(a) \otimes \rho_0(b) \\
&= \sum_{a\in H} \rho_H(a) \otimes \rho_0(f(a)) \\
&= \sum_{a\in H} \rho_H(a) \text{ (car } V \otimes \mathbb{C} \cong V)
\end{aligned}$$

Supposons que $\rho = \rho_H \otimes \rho_0$ avec (ρ_H, V) non principale de H. Alors on a :

$$\begin{aligned}
\rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_H(a) \otimes \rho_0(b) \\
&= \sum_{a\in H} \rho_H(a) \otimes \rho_0(f(a)) \\
&= \sum_{a\in H} \rho_H(a) \text{ (car } V \otimes \mathbb{C} \cong V) \\
&= \rho_H(H)
\end{aligned}$$

Supposons que $\rho = \rho_H \otimes \rho_0$ avec (ρ_H, V) non principale de H. Alors on a :

$$\begin{aligned}
\rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_H(a) \otimes \rho_0(b) \\
&= \sum_{a\in H} \rho_H(a) \otimes \rho_0(f(a)) \\
&= \sum_{a\in H} \rho_H(a) \text{ (car } V \otimes \mathbb{C} \cong V) \\
&= \rho_H(H) \\
&= 0_V \ .
\end{aligned}$$

L'égalité de Parseval suggère, par analogie au cas commutatif, de dire que $f : H \to K$ est maximalement non linéaire si la valeur de $\sqrt{\dim \rho}\|\rho(D_f)\|$ est la plus petite possible,

L'égalité de Parseval suggère, par analogie au cas commutatif, de dire que $f : H \to K$ est maximalement non linéaire si la valeur de $\sqrt{\dim \rho}\|\rho(D_f)\|$ est la plus petite possible, soit en d'autres termes,

$$\max_{\rho_K \neq \rho_0} \sqrt{\dim \rho}\|\rho(D_f)\| \leq \max_{\rho_K \neq \rho_0} \sqrt{\dim \rho}\|\rho(D_g)\|$$

pour tout $g : H \to K$ (d'après les valeurs connues de $\rho(D_f)$).

Il est possible d'exhiber un minorant pour la quantité $\max \sqrt{\dim \rho} \|\rho(D_f)\|$.

Il est possible d'exhiber un minorant pour la quantité $\max \sqrt{\dim \rho} \|\rho(D_f)\|$.

Théorème

Soit $f : H \to K$, K non trivial.

Il est possible d'exhiber un minorant pour la quantité $\max \sqrt{\dim \rho}\|\rho(D_f)\|$.

Théorème

Soit $f : H \to K$, K non trivial. Alors :

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)} \ .$$

Il est possible d'exhiber un minorant pour la quantité $\max \sqrt{\dim \rho}\|\rho(D_f)\|$.

Théorème

Soit $f : H \to K$, K non trivial. Alors :

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)} \ .$$

On remarque que si H, K sont des groupes abéliens, alors $\dim \rho = 1$, $|\tilde{H}| = |H|$, $|\tilde{K}| = |K|$.

Il est possible d'exhiber un minorant pour la quantité $\max \sqrt{\dim \rho}\|\rho(D_f)\|$.

Théorème

Soit $f : H \to K$, K non trivial. Alors :

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)} \ .$$

On remarque que si H, K sont des groupes abéliens, alors $\dim \rho = 1$, $|\tilde{H}| = |H|$, $|\tilde{K}| = |K|$. De sorte que l'on récupère $\max_{\rho_K \neq \rho_0} \|\rho(D_f)\|^2 \geq m$, soit la borne inférieure définissant les fonctions courbes.

Preuve

De l'égalité de Parseval, appliquée à D_f, nous tirons que :

$$\frac{1}{|G|}\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=\sum_{(a,b)\in G}1_{D_f}(a,b)^2=m\ .$$

Preuve

De l'égalité de Parseval, appliquée à D_f, nous tirons que :

$$\frac{1}{|G|}\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=\sum_{(a,b)\in G}1_{D_f}(a,b)^2=m\ .$$

Ainsi, $\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=|G|m=m^2n\ .$

Preuve

De l'égalité de Parseval, appliquée à D_f, nous tirons que :

$$\frac{1}{|G|}\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=\sum_{(a,b)\in G}1_{D_f}(a,b)^2=m\ .$$

Ainsi, $\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=|G|m=m^2n$. Nous connaissons certaines des valeurs de $\rho(D_f)$ de façon que :

$$\sum_{\rho_K\neq\rho_0}\dim\rho\|\rho(D_f)\|^2\ =\ \sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2-\sum_{\rho_K=\rho_0}\dim\rho\|\rho(D_f)\|^2$$

Preuve

De l'égalité de Parseval, appliquée à D_f, nous tirons que :

$$\frac{1}{|G|}\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=\sum_{(a,b)\in G}1_{D_f}(a,b)^2=m\ .$$

Ainsi, $\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=|G|m=m^2n$. Nous connaissons certaines des valeurs de $\rho(D_f)$ de façon que :

$$\begin{aligned}\sum_{\rho_K\neq\rho_0}\dim\rho\|\rho(D_f)\|^2 &= \sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2-\sum_{\rho_K=\rho_0}\dim\rho\|\rho(D_f)\|^2\\ &= m^2n-\underbrace{\dim\rho_0\|\rho_0(D_f)\|^2}_{=m^2}\\ &\quad-\underbrace{\sum_{\rho_K=\rho_0,\ \rho\neq\rho_0}\dim\rho\|\rho(D_f)\|^2}_{=0}\end{aligned}$$

Preuve

De l'égalité de Parseval, appliquée à D_f, nous tirons que :

$$\frac{1}{|G|}\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=\sum_{(a,b)\in G}1_{D_f}(a,b)^2=m\ .$$

Ainsi, $\sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2=|G|m=m^2n$. Nous connaissons certaines des valeurs de $\rho(D_f)$ de façon que :

$$\begin{aligned}\sum_{\rho_K\neq\rho_0}\dim\rho\|\rho(D_f)\|^2 &= \sum_{\rho\in\tilde{G}}\dim\rho\|\rho(D_f)\|^2-\sum_{\rho_K=\rho_0}\dim\rho\|\rho(D_f)\|^2\\ &= m^2n-\underbrace{\dim\rho_0\|\rho_0(D_f)\|^2}_{=m^2}\\ &\quad-\underbrace{\sum_{\rho_K=\rho_0,\ \rho\neq\rho_0}\dim\rho\|\rho(D_f)\|^2}_{=0}\\ &= m^2(n-1)\ .\end{aligned}$$

Preuve (suite)

Le nombre de représentations de G principales sur K est $|\tilde{H}|$.

Preuve (suite)

Le nombre de représentations de G principales sur K est $|\tilde{H}|$. Donc il y a $|\tilde{G}| - |\tilde{H}|$ représentations de G non principales sur K.

Preuve (suite)

Le nombre de représentations de G principales sur K est $|\tilde{H}|$. Donc il y a $|\tilde{G}| - |\tilde{H}|$ représentations de G non principales sur K. Mais $|\tilde{G}| = |\tilde{H}||\tilde{K}|$.

Preuve (suite)

Le nombre de représentations de G principales sur K est $|\tilde{H}|$. Donc il y a $|\tilde{G}| - |\tilde{H}|$ représentations de G non principales sur K. Mais $|\tilde{G}| = |\tilde{H}||\tilde{K}|$. Il en résulte donc que

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)} \ .$$

Preuve (suite)

Le nombre de représentations de G principales sur K est $|\tilde{H}|$. Donc il y a $|\tilde{G}| - |\tilde{H}|$ représentations de G non principales sur K. Mais $|\tilde{G}| = |\tilde{H}||\tilde{K}|$. Il en résulte donc que

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)} \ .$$

Remarque

La preuve précédente montre également que

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)}$$

si, et seulement si,

$$\forall \rho_K \neq \rho_0, \ \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{\dim \rho |\tilde{H}|(|\tilde{K}|-1)} \ .$$

Preuve (suite)

Le nombre de représentations de G principales sur K est $|\tilde{H}|$. Donc il y a $|\tilde{G}| - |\tilde{H}|$ représentations de G non principales sur K. Mais $|\tilde{G}| = |\tilde{H}||\tilde{K}|$. Il en résulte donc que

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)} \ .$$

Remarque

La preuve précédente montre également que

$$\max_{\rho_K \neq \rho_0} \dim \rho \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{|\tilde{H}|(|\tilde{K}|-1)}$$

si, et seulement si,

$$\forall \rho_K \neq \rho_0, \ \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{\dim \rho |\tilde{H}|(|\tilde{K}|-1)} \ .$$

Une application atteignant cette borne inférieure est appelée courbe.

Aperçu des notions de non linéarité dans le cadre non commutatif

- Fonctions minimisant $\sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_f)\|^4$: fonctions presque parfaitement non linéaires.

Aperçu des notions de non linéarité dans le cadre non commutatif

- Fonctions minimisant $\sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_f)\|^4$: fonctions presque parfaitement non linéaires.

- Fonctions minimisant $\max_{\rho_K \neq \rho_0} \sqrt{\dim \rho} \|\rho(D_f)\|$: fonctions maximalement non linéaires.

Aperçu des notions de non linéarité dans le cadre non commutatif

- Fonctions minimisant $\sum_{\rho \in \tilde{G}} \dim \rho \|\rho(D_f)\|^4$: fonctions presque parfaitement non linéaires.

- Fonctions minimisant $\max_{\rho_K \neq \rho_0} \sqrt{\dim \rho} \|\rho(D_f)\|$: fonctions maximalement non linéaires.

- Fonctions telles que quel que soit $\rho_K \neq \rho_0$, $\|\rho(D_f)\|^2 = \frac{m^2(n-1)}{\dim \rho |\tilde{H}|(|\tilde{K}|-1)}$: fonctions courbes.

Quelques résultats obtenus avec GAP : Non linéarité de fonctions entre deux groupes d'ordre 6

H	K	$\min_{g\,:\,H\to K} \sum_{\rho\in\tilde{G}} \dim\ \rho \|\rho(D_g)\|^4$	$\min_{g\,:\,H\to K} \max_{\rho_K\neq\rho_0} \sqrt{\dim\ \rho}\|\rho(D_g)\|$
$\mathfrak{S}_3$	$\mathbb{Z}_6$	2376	4
$\mathbb{Z}_6$	$\mathfrak{S}_3$	3972	$4\sqrt{2}$
$\mathfrak{S}_3$	$\mathfrak{S}_3$	3552	$2\sqrt{14}$
$\mathbb{Z}_6$	$\mathbb{Z}_6$	2808	$2\sqrt{3}$

Quelques résultats obtenus avec GAP : Non linéarité de fonctions entre deux groupes d'ordre 6

H	K	$\min_{g:\, H\to K} \sum_{\rho\in\tilde{G}} \dim\ \rho \|\rho(D_g)\|^4$	$\min_{g:\, H\to K} \max_{\rho_K\neq\rho_0} \sqrt{\dim\ \rho}\|\rho(D_g)\|$
$\mathfrak{S}_3$	$\mathbb{Z}_6$	2376	4
$\mathbb{Z}_6$	$\mathfrak{S}_3$	3972	$4\sqrt{2}$
$\mathfrak{S}_3$	$\mathfrak{S}_3$	3552	$2\sqrt{14}$
$\mathbb{Z}_6$	$\mathbb{Z}_6$	2808	$2\sqrt{3}$

On remarque que la mesure de non linéarité presque parfaite est de loin la meilleure dans le cas $(H, K) = (\mathfrak{S}_3, \mathbb{Z}_6)$ et non dans le cas abélien.

Quelques résultats obtenus avec GAP : Non linéarité de fonctions entre deux groupes d'ordre 6

H	K	$\min_{g:\, H\to K} \sum_{\rho\in\tilde{G}} \dim\ \rho \|\rho(D_g)\|^4$	$\min_{g:\, H\to K} \max_{\rho_K\neq\rho_0} \sqrt{\dim\ \rho}\|\rho(D_g)\|$
$\mathfrak{S}_3$	$\mathbb{Z}_6$	2376	4
$\mathbb{Z}_6$	$\mathfrak{S}_3$	3972	$4\sqrt{2}$
$\mathfrak{S}_3$	$\mathfrak{S}_3$	3552	$2\sqrt{14}$
$\mathbb{Z}_6$	$\mathbb{Z}_6$	2808	$2\sqrt{3}$

On remarque que la mesure de non linéarité presque parfaite est de loin la meilleure dans le cas $(H, K) = (\mathfrak{S}_3, \mathbb{Z}_6)$ et non dans le cas abélien. De plus, toujours lorsque $(H, K) = (\mathfrak{S}_3, \mathbb{Z}_6)$, toute fonction presque parfaitement non linéaire est également maximalement non linéaire.

Quelques résultats obtenus avec GAP : Non linéarité de fonctions entre deux groupes d'ordre 6

H	K	$\min_{g:\, H\to K} \sum_{\rho\in\tilde{G}} \dim\ \rho \|\rho(D_g)\|^4$	$\min_{g:\, H\to K} \max_{\rho_K\neq\rho_0} \sqrt{\dim\ \rho}\|\rho(D_g)\|$
$\mathfrak{S}_3$	$\mathbb{Z}_6$	2376	4
$\mathbb{Z}_6$	$\mathfrak{S}_3$	3972	$4\sqrt{2}$
$\mathfrak{S}_3$	$\mathfrak{S}_3$	3552	$2\sqrt{14}$
$\mathbb{Z}_6$	$\mathbb{Z}_6$	2808	$2\sqrt{3}$

On remarque que la mesure de non linéarité presque parfaite est de loin la meilleure dans le cas $(H, K) = (\mathfrak{S}_3, \mathbb{Z}_6)$ et non dans le cas abélien. De plus, toujours lorsque $(H, K) = (\mathfrak{S}_3, \mathbb{Z}_6)$, toute fonction presque parfaitement non linéaire est également maximalement non linéaire. Dans tous les autres cas, aucune fonction presque parfaitement non linéaire n'est maximalement non linéaire.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants :

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Par contre il y a au moins une fonction courbe $f : \mathfrak{S}_3 \to \mathbb{Z}_3$.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Par contre il y a au moins une fonction courbe $f : \mathfrak{S}_3 \to \mathbb{Z}_3$. En effet on peut vérifier que l'application f donnée par
$f(id) = f((1,2)) = f((2,3)) = f((1,3)) = 0$ et
$f((1,2,3)) = f((1,3,2)) = 1$ est courbe,

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Par contre il y a au moins une fonction courbe $f : \mathfrak{S}_3 \to \mathbb{Z}_3$. En effet on peut vérifier que l'application f donnée par
$f(id) = f((1,2)) = f((2,3)) = f((1,3)) = 0$ et
$f((1,2,3)) = f((1,3,2)) = 1$ est courbe, ce qui signifie que
$\sqrt{\dim \rho}\|\rho(D_f)\| = 2\sqrt{3}$ pour tout $\rho_{\mathbb{Z}_3} \neq \rho_0$.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Par contre il y a au moins une fonction courbe $f : \mathfrak{S}_3 \to \mathbb{Z}_3$. En effet on peut vérifier que l'application f donnée par
$f(id) = f((1,2)) = f((2,3)) = f((1,3)) = 0$ et
$f((1,2,3)) = f((1,3,2)) = 1$ est courbe, ce qui signifie que
$\sqrt{\dim \rho}\|\rho(D_f)\| = 2\sqrt{3}$ pour tout $\rho_{\mathbb{Z}_3} \neq \rho_0$.

En effet, le groupe symétrique $\mathfrak{S}_3$ possède deux représentations de dimension un (la représentation principale et le signature), et une représentation de dimension deux.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Par contre il y a au moins une fonction courbe $f : \mathfrak{S}_3 \to \mathbb{Z}_3$. En effet on peut vérifier que l'application f donnée par
$f(id) = f((1,2)) = f((2,3)) = f((1,3)) = 0$ et
$f((1,2,3)) = f((1,3,2)) = 1$ est courbe, ce qui signifie que
$\sqrt{\dim \rho}\|\rho(D_f)\| = 2\sqrt{3}$ pour tout $\rho_{\mathbb{Z}_3} \neq \rho_0$.

En effet, le groupe symétrique $\mathfrak{S}_3$ possède deux représentations de dimension un (la représentation principale et le signature), et une représentation de dimension deux. Ainsi $\frac{|\mathfrak{S}_3|^2(|\mathbb{Z}_3|-1)}{|\tilde{\mathfrak{S}}_3|(|\tilde{\mathbb{Z}}_3|-1)} = 12$, de sorte que nous avons $\sqrt{\dim \rho}\|\rho(D_f)\| = 2\sqrt{3}$ pour toute représentation irréductible $\rho = \rho_{\mathfrak{S}_3} \otimes \rho_{\mathbb{Z}_3}$ telle que $\rho_{\mathbb{Z}_3}$ est non principale.

Une recherche exhaustive de fonctions courbes de $\mathfrak{S}_3$ dans un groupe K tel que $1 < |K| \leq 5$ a également été menée. Notons que la notion de fonctions courbes fait sens même si $|K|$ ne divise pas $|\mathfrak{S}_3| = 6$ contrairement au cas commutatif. Les résultats obtenus sont les suivants : tout d'abord il n'y a aucune fonction courbe si $N \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5\}$.

Par contre il y a au moins une fonction courbe $f : \mathfrak{S}_3 \to \mathbb{Z}_3$. En effet on peut vérifier que l'application f donnée par
$f(id) = f((1,2)) = f((2,3)) = f((1,3)) = 0$ et
$f((1,2,3)) = f((1,3,2)) = 1$ est courbe, ce qui signifie que
$\sqrt{\dim \rho}\|\rho(D_f)\| = 2\sqrt{3}$ pour tout $\rho_{\mathbb{Z}_3} \neq \rho_0$.

En effet, le groupe symétrique $\mathfrak{S}_3$ possède deux représentations de dimension un (la représentation principale et le signature), et une représentation de dimension deux. Ainsi $\frac{|\mathfrak{S}_3|^2(|\mathbb{Z}_3|-1)}{|\tilde{\mathfrak{S}}_3|(|\tilde{\mathbb{Z}}_3|-1)} = 12$, de sorte que nous avons $\sqrt{\dim \rho}\|\rho(D_f)\| = 2\sqrt{3}$ pour toute représentation irréductible $\rho = \rho_{\mathfrak{S}_3} \otimes \rho_{\mathbb{Z}_3}$ telle que $\rho_{\mathbb{Z}_3}$ est non principale. Par contre f n'est pas parfaitement non linéaire !