FPGAs et calcul dans les groupes finis

22 juin 2021

Groupes

- Définition : **G** ensemble, loi de composition interne •
  - associative : (a•b)•c = a•(b•c)
  - élément neutre a•1=1•a=a
  - inverse : $a \bullet a^{-1} = a^{-1} \bullet a = 1$

- Exemples classiques :
  - permutation sur n éléments S_n
  - permutation alternées sur n éléments A_n
  - matrices inversibles n×n sur F_q $M_n(F_q)$
  - entiers modulo n Z/nZ

  } Groupes finis

  - matrices inversibles n×n sur R, C $M_n(C), M_n(R)$ Groupes infinis

Conjugaison

- Définition : conjugué de a par b, $a^b := b^{-1}ab$
- H sous-groupe de G, $H^a := \{ b^a \mid b \in H \}$ est un groupe
- Classe de conjugaison de a dans G, $a^G := \{ a^b \mid b \in G \}$
- Classe de conjugaison de H dans G, $H^G := \{ H^b \mid b \in G \}$
- Si $H^G = \{H\}$, alors H est dit sous-groupe normal ou distingué de G, noté $H \triangleleft G$
- Alt. : Si $H \triangleleft G$ alors $\forall a \in H, \forall b \in G, a^b \in H$
- Si G ne possède pas de sous groupes normaux, G est dit simple
- Ex. : pour $n \geq 5$, A_n est simple $\Rightarrow$ Théorème d'Abel

Groupe normal et groupe quotient

- On suppose $H \lhd G$
- Classe latérale $aH:=\{ab \mid b \in H\}$
- Thm. Laplace : si G est fini, alors les classes latérales de H dans G ont toutes la même taille et forme une partition de G
- On a $ah_1bh_2=ab(b^{-1}h_1b)h_2=abh'_1h_2$ i.e. (aH)(bH)=abH
- La l.c.i. de G induit une l.c.i. sur les classes latérales de H.
- Axiomes de groupe respectés : le groupe construit est le groupe quotient K=G/H.
- G est un groupe extension de H. G admet une suite de composition, notée H.K

Isomorphisme et isoclinisme

- Morphisme de groupes: f:G $\rightarrow$H tel que f(ab)=f(a)f(b) et $f(a^{-1})=f(a)^{-1}$
- G et H sont isomorphes s'il existe un morphisme bijectif entre eux.
- G et H sont isocliniques s'ils ont une composition en série identique mais ne sont pas isomorphes.
- Exemple : S_n et $A_n \times 2$ sont de la forme $A_n.2$
- A_n et 2 sont des sous groupes normaux de $A_n \times 2$
- Seul A_n est un sous groupe normal de S_n

Classification des groupes finis simples

- Par récurrence, tous les groupes finis ont une série de composition où chaque facteur est un groupe fini simple.
- Les groupes finis simples sont exactement :
  - les groupes alternés A_n, $n \geq 5$
  - les groupes cycliques Z/pZ, p premier
  - les groupes linéaires classiques (unitaires, symplectiques, projectifs, orthogonaux)
  - les groupes de Lie exceptionnels ou tordus
  - les 26 groupes sporadiques
- Annoncé en 1983. Théorème monstrueux : 15000 + 1000 pages de démonstration

Démonstration complète ?

Groupes de permutations

- Thm. de Cayley : tout groupe fini est un groupe de permutation
- Ex : le groupe A_6 est généré par les permutations (1,2,3,4,5) et (4,5,6)
- Multiplier deux éléments $\Rightarrow$ Calculer l'image de chaque point
- Utilisation de chaînes de stabilisateur $\Rightarrow$ Quelques points suffisent
- Ex : M_{24} généré par (1,5)(2,14,7,12)(3,21)(4,17,16,11)(6,20,23,22)(9,10,15,13) et (1,19,15,8,20,23,24,9,14,11,5,10,22,13,2)(3,6,4)(7,16,12,17,18). Il suffit de calculer les images de 1 jusqu'à 7.

Groupes de matrices

- Tout groupe fini est un groupe de matrices : Cayley + matrices de permutations
- Multiplier deux éléments $\Rightarrow$ Multiplier deux matrices
- Ex : A_6 généré par $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ dans F_2
- Si G est généré par M_1 et M_2 avec $M_1v_1=v_1$ et $M_2v_2=v_2$, v_1,v_2 vecteurs non nuls alors $M \in G$, $Mv_1=v_1$, $Mv_2=v_2 \Rightarrow M=Id$
- On peut remplacer les produits de matrices par des produits matrice-vecteur

Matrices monomiales

- Cas particulier important
- Matrice monomiale : matrice avec exactement un coefficient non nul par ligne et par colonne
- Produit matrice-vecteur : permutation des coefficients du vecteur suivi d'une multiplication

Taille des représentations

Gpe	Mat	Perm	Taille
M_{11}	5	11	7920
M_{12}	10	12	95040
J_1	20	266	175560
M_{22}	10	22	443520
J_2	6	100	604800
M_{23}	11	23	10200960
HS	20	100	44352000
J_3	18	6156	50232960
M_{24}	11	24	244823040
McL	21	275	898128000
He	50	2058	4030387200
Ru	28	4060	145926144000
Suz	110	1782	448345497600

Gpe	Mat	Perm	Taille
$O'N$	154	122760	460815505920
Co_3	22	276	495766656000
Co_2	23	2300	42305421312000
Fi_{22}	77	3510	64561751654400
HN	132	1140000	273030912000000
Ly	111	8835156	51765179004000000
Th	248	143127000	90745943887872000
Fi_{23}	253	31671	4089470473293004800
Co_1	24	98280	4157776806543360000
J_4	112	173067389	86775571046077562880
Fi_{24}'	781	306936	1255205709190661721292800
B	4370	13571955000	4154781481226426191177580544000000
M	196884	97239461142009186000	808017424794512875886459904... 96171075700575436800000000

FPGA et mathématiques

- FPGA : essentiellement applications embarquées, prototypage de circuit
  - accélération librairie BigNum (Vuillemin & Morain)
  - génération partition ensemble (Butler & Sasao)
  - accélération d'opérateurs dans de multiples domaines : multiplication de matrices, graphes, séquences ADN, générateurs de bruit gaussien ...
- Alternatives accélération : GPUs, réseaux de CPUs
- Bien choisir l'application et bien choisir l'algorithme

Deux exemples

- Calcul du nombre de partitions de Goldbach $p+q=2n$
  - Convolution de la liste des nombres premiers par elle-même
  - Solution naïve : implémenter une convolution systolique sur FPGA
  - Solution plus efficace : calculer la convolution par transformée de Fourier sur CPU
  - Complexité : $O(n^2) \rightarrow O(n \log n)$
- Calcul distance minimale EQR(233)
  - Théorème de Chen
  - Enumération d'un nombre réduit de mots de code
  - Script VHDL difficile à maintenir et à modifier
  - Utilisation de GPUs plus appropriée

Permutations pour BM

- Détermination de deux permutations à 13571955000 points
- Action des générateurs de BM sur les classes latérales du centralisateur d'une involution x de type 2A de BM
- $C(x)=\{ h \mid xh=hx\}=\{h \mid x^h=x\}$ est un groupe
- $b \in aC(x) \Leftrightarrow ba^{-1} \in C(x) \Leftrightarrow x^{ba^{-1}}=x \Leftrightarrow x^b=x^a$
- u,v générateurs de BM
- On calcule toutes les classes latérales par algorithme glouton : x^w pour tout $w \in \{u,v\}^*$
- Les permutations sont déterminées par l'action de u et v sur les classes latérales

Identifier les classes de conjugaison de BM

- $x \in BM$: trouver un critère pour identifier la classe de conjugaison de x
- Exemple : x est de type 3B $\rightarrow$ x est d'ordre 3 et la taille de son centralisateur est la seconde parmi celles des éléments d'ordre 3
- 1ère solution : les matrices représentant $x - Id$ et $x^g - Id = g^{-1}xg - Id$ sont semblables et ont donc le même rang.
- 2ème solution : $tr(g^{-1}xg) = tr(g^{-1}gx) = tr(x)$. tr est un invariant de classe. Plusieurs représentations de BM sont nécessaires (modulo 2, 3, 5 ...)
- Pb : calculer le rang ou la trace $\rightarrow$ Complexité $O(n^3)$

Nouvelle méthode

- Si x à tester, calculer ord(xy) pour y bien choisi
- Exemple : dans M_{24}, deux classes d'involution 2A (11385) et 2B (31878)
- Deux classes d'élément d'ordre 3, 3A (226688) et 3B (485760)
- Si $x \in 2A$, ord(x.y3a) $\in$ {2 (896), 3 (5376), 4 (27776), 5 (28672), 6 (24192), 7 (43008), 8 (32256), 11 (21504), 12 (7168), 14 (21504), 15 (14336) }
- Si $x \in 2B$, ord(x.y3a) $\in$ {2 (320), 3 (448), 4 (7360), 6 (31680), 7 (2560), 8 (11520), 10 (30720), 11 (7680), 12 (42240), 14 (46080), 15 (15360), 21 (15360), 23 (15360)}
- Si ord(x)=2 et ord(x.y3a) = 5 alors $x \in 2A$. Proba=28672/226688≈0.13 par essai
- Si ord(x)=2 et ord(x.y3a) $\in$ { 10, 21, 23 } alors $x \in 2B$. Proba=61440/226688≈ 0.27 par essai.
- Méthode : On choisit g aléatoire, on calcule $y=y3a^g$, puis ord(xy) jqà réussite.

Perspectives

- Adapter et tester les trois méthodes sur BM et M
- Comparer méthodes + tester speedup FPGA
- Autres méthodes possibles : signatures, semi-présentation
- Autres applications :
  - Donner générateurs aux sous-groupes maximaux de BM et M
  - Tester derniers cas de sous-groupes maximaux de M
  - Faire une librairie de calcul dans les groupes sporadiques
  - Paralléliser les calculs dans les groupes de permutations
- Autres domaines :
  - Géométrie discrète : recherche d'unitaux, de géométrie discrète ...
  - Accélération de calcul : FastSPICE, recherche de trinomes irréductibles ...