La gazette du cnrs GDR Groupement de recherche
IM Informatique Mathématique

Edito

C'est un grand plaisir de vous présenter ce numéro 2 de la gazette du GDR IM. Nous aurions aimé vous le présenter plus tôt mais cette période bien délicate a beaucoup compliqué les choses. À ce sujet, nous espérons que vous allez toutes et tous aussi bien que possible.
Nous souhaitons à travers cette gazette montrer la vitalité de notre communauté, et la diversité et la richesse de ses problématiques. Nos remerciements vont bien entendu tout d'abord aux auteurs des articles, Thomas Fernique et Joris Van der Hoeven, aux personnes interviewées, Ludovic Patey et Marthe Bonamy, et à leurs intervieweurs Youssouf Oualhadj et Brigitte Vallée.
Cependant, pour passer d'une collection d'articles disparates à une gazette telle que celle-ci, un gros travail de mise en page est nécessaire : nous sommes très reconnaissants à Ines Klimann d'avoir commencé ce travail pour le numéro 1, et à Nicolas Schabanel d'avoir pris la relève pour le présent numéro.
La gazette du GDR IM ne peut se faire sans vous : nous sommes très preneurs de propositions d'articles et d'interviews, d'annonces, de suggestions.
Portez vous tou(te)s bien, et passez un excellent été.

Guillaume Theyssier et
Jean-Michel Muller
co-directeurs du GDR IM

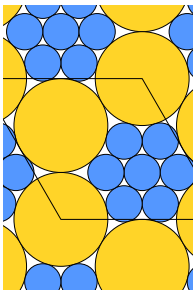
#2

Parue en juillet 2021

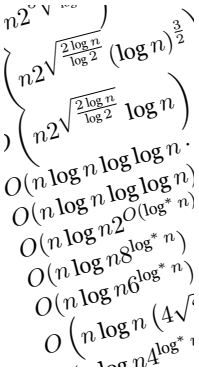
Entretiens

Articles

Empilements de Disques Triangulés
par Thomas Fernique



Comment disposer sur une table le plus possible de pièces sans qu'elles ne se chevauchent ? Si les pièces sont toutes identiques, on peut, par exemple, former une grille carrée. Environ 78% de la surface de la table sera alors recouverte. On peut en fait recouvrir plus de 90% de la table en formant une grille triangulaire. Peut-on faire mieux ? Et qu'en est-il s'il y a différentes pièces ?



Multiplier des entiers en temps $O(n \log n)$
par Joris van der Hoeven

Quelle est la meilleure façon de multiplier deux entiers ? Cette question, simple en apparence, est peut-être le plus ancien problème mathématique non résolu. Il a été démontré récemment que deux entiers de n chiffres peuvent être multipliés en temps $O(n \log n)$. L'existence d'un tel algorithme fut conjecturé en 1971 par Schönhage et Strassen. Ils émettaient également leurs doutes sur l'existence d'une méthode encore plus rapide, ce que l'on ignore toujours. Dans cet article, je présenterai brièvement une longue histoire et je poursuivrai avec un aperçu du nouvel algorithme.

Empilements de Disques Triangulés

Thomas Fernique

Chargé de recherches CNRS, LIPN

Comment disposer sur une table le plus possible de pièces sans qu'elles ne se chevauchent ? Si les pièces sont toutes identiques, on peut, par exemple, former une grille carrée (Fig. 1, à gauche). Environ 78% de la surface de la table sera alors recouverte. On peut en fait recouvrir plus de 90% de la table en formant une grille triangulaire (Fig. 1, au centre). Peut-on faire mieux ? Et qu'en est-il s'il y a différentes pièces (Fig. 1, à droite) ?

Sous ses dehors anecdotiques, cette question concerne en fait des domaines aussi variés que les codes correcteurs ou les sciences des matériaux et met en jeu des techniques typiques de l'informatique mathématique.

1 Empilements de disques

Formellement, un *empilement de disques* (en anglais *circle packing*) est un ensemble de disques du plan d'intérieurs disjoints. Sa *densité* δ est la proportion du plan recouverte par les disques, définie par

$$\delta := \limsup_{n\to\infty} \frac{\text{surface du carré } [-n,n]^2 \text{ recouverte par les disques}}{\text{surface du carré } [-n,n]^2}.$$

Avec des disques tous identiques, la densité maximale est effectivement celle de l'empilement représenté Fig. 1, au centre, appelé *empilement hexagonal compact*. Bien qu'intuitif, ce résultat n'a été formellement prouvé que dans les années 1940. Le lecteur intéressé trouvera dans [2] une preuve élémentaire qui repose sur la notion de *triangulation de Delaunay*.

Avec deux tailles de disques, la densité maximale devient une fonction du ratio r de ces tailles. Il a été démontré dans les années 1960 qu'au delà d'un ratio $r_0 \approx 0.74$, il est impossible de faire plus dense qu'avec des disques tous identiques. Ainsi, la meilleure façon de disposer des pièces de 1 et 2 euros (ratio $\frac{93}{103} \approx 0.9$) sur une table est de juxtaposer deux empilements hexagonaux compacts, un pour chaque type de pièce. Il est parfois possible de faire mieux pour des ratios plus petits, mais il existe alors seulement 9 ratios pour lesquels la densité maximale est connue [1]. Ces ratios "magiques" sont des nombres algébriques qui permettent des empilements bien particuliers, dits *triangulés* car leur *graphe de contact* (le graphe reliant les centres des disques adjacents) est une triangulation (Fig. 2).

2 Empilement binaires triangulés

Ainsi, tous les ratios pour lesquels on connaît la densité maximale permettent des empilements triangulés. Inversement, si un ratio permet des empilements triangulés [1], alors la densité se trouve être maximisée par un tel empilement. C'est en effet un corollaire du fait que les 9 ratios illustrés Fig. 2 sont les seuls qui permettent un empilement triangulé à deux disques [5]. La preuve de ce résultat repose sur deux points :

1. Dans un empilement triangulé, la *couronne* d'un disque est la suite des tailles des disques qui lui sont tangents, ordonnés cycliquement. Dans le premier des 9 cas représentés Fig. 2, par exemple, chaque petit disque est entouré par 4 grands et 1 petit, *i.e.*, a une couronne $1111r$. Comme un petit disque est tangent à au plus 6 disques, deux tailles de disque permettent au plus 2^6 couronnes différentes. On peut en fait assez facilement se ramener à seulement 10 couronnes [2] : 11111, $1111r$, $111rr$, $11r1r$, $11rrr$, $1r1rr$, 1111, $111r$, $11rr$ et 111.
2. Considérons les triangles reliant le centre d'un petit disque aux centres de deux disques consécutifs de sa couronne : la somme de leurs angles en le centre du petit disque vaut 2π. Par exemple, toujours pour le premier des 9 cas représentés Fig. 2 :

$$3 \times \widehat{1r1} + 2 \times \widehat{1rr} = 2\pi,$$

où $\widehat{ijk}$ représente l'angle en j dans le triangle reliant les centres de disques mutuellement tangents de rayons i, j et k. Prendre le cosinus de chaque membre permet, après quelques manipulations trigonométriques classiques,

1. Autre que le cas dégénéré d'un empilement hexagonal compact, toujours possible en n'utilisant qu'une taille de disque.
2. La couronne $rrrrrr$, toujours possible, est éliminée car s'il n'y a qu'elle dans l'empilement, alors c'est l'empilement compact hexagonal.

Figure 1 – Quelques façons de placer des pièces sur une table.

d'en déduire une équation algébrique sur r, soit dans l'exemple ci-dessus :

$$r^4 - 10r^2 - 8r + 9 = 0.$$

On peut donc calculer, pour chacune des 10 couronnes de petit disque possible, la valeur algébrique de r qu'elle impose, puis en déduire toutes les couronnes possibles et enfin chercher un empilement compatible avec ces couronnes. Tout ça se fait assez facilement. Le seul cas éliminé est la couronne 11111, qui caractérise un ratio ne permettant pas de former une couronne autour d'un grand disque. Les 9 cas restants sont ceux illustrés Fig. 2.

3 Empilements ternaires triangulés

Que se passe-t-il si on ajoute maintenant des disques de rayon $s \in]0, r[$? Dans [4], on montre qu'il y a alors exactement 164 paires (r, s) qui permettent un empilement triangulé de disques de rayons s, r et 1 (chaque cas est illustré dans l'article). Le schéma de preuve est le même que quand il n'y a que deux disques, mais sa mise en pratique est bien plus complexe. En particulier, l'outil informatique (programmation python et calcul avec SageMath [6]) joue un rôle crucial. Rentrer dans les détails dépasserait largement le cadre de cet article. Soulignons seulement quelques points :

1. Comme il y a deux rayons inconnus, il faut maintenant deux couronnes pour les caractériser. Le nombre de paires de couronnes à considérer est très grand. Des astuces combinatoires et arithmétiques [3] sont nécessaires pour éliminer un maximum de paires impossibles.
2. Les paires de couronnes restantes donnent des systèmes polynomiaux complexes (des polynômes de plusieurs milliers de termes ne sont pas rares). Beaucoup résistent aux techniques éprouvées de résolution comme les *bases de Gröbner*. Ici encore, il faut ruser pour éliminer.
3. Rien n'exclut *a priori* qu'un ensemble de couronnes puisse n'être compatible qu'avec des empilements apériodiques, ce qui pourrait rendre indécidable le problème de l'existence d'un empilement compatible. Cela s'est avéré ne pas arriver avec seulement trois tailles de disques.

Reste alors la question de la densité. Est-ce que, comme avec deux disques, si un triplet de disques permet un empilement triangulé, alors la densité des empilements de disques de ces tailles est maximisé par un empilement triangulé ? Quelques premiers cas encourageants ont été récemment traités…

4 Pour aller plus loin

Les mêmes questions se posent bien sûr pour $k \geq 4$ tailles de disques, ou bien pour des empilements de sphères en dimension $d \geq 3$ (les dimensions 3, 8 et 24 sont celles où l'on en sait le plus, du moins quand il n'y a qu'une seule taille de sphère [3]). Pourtant, ce qui m'intéresserait plus encore serait de faire un lien avec mes travaux sur les *pavages apériodiques* en trouvant k tailles de disques telles que les empilements les plus denses soient nécessairement apériodiques. Peut-être des empilements triangulés avec 4 tailles de disques ?

3. L'arithmétique d'intervalles, notamment, très utile pour éliminer des couronnes à partir d'encadrements des valeurs des rayons.

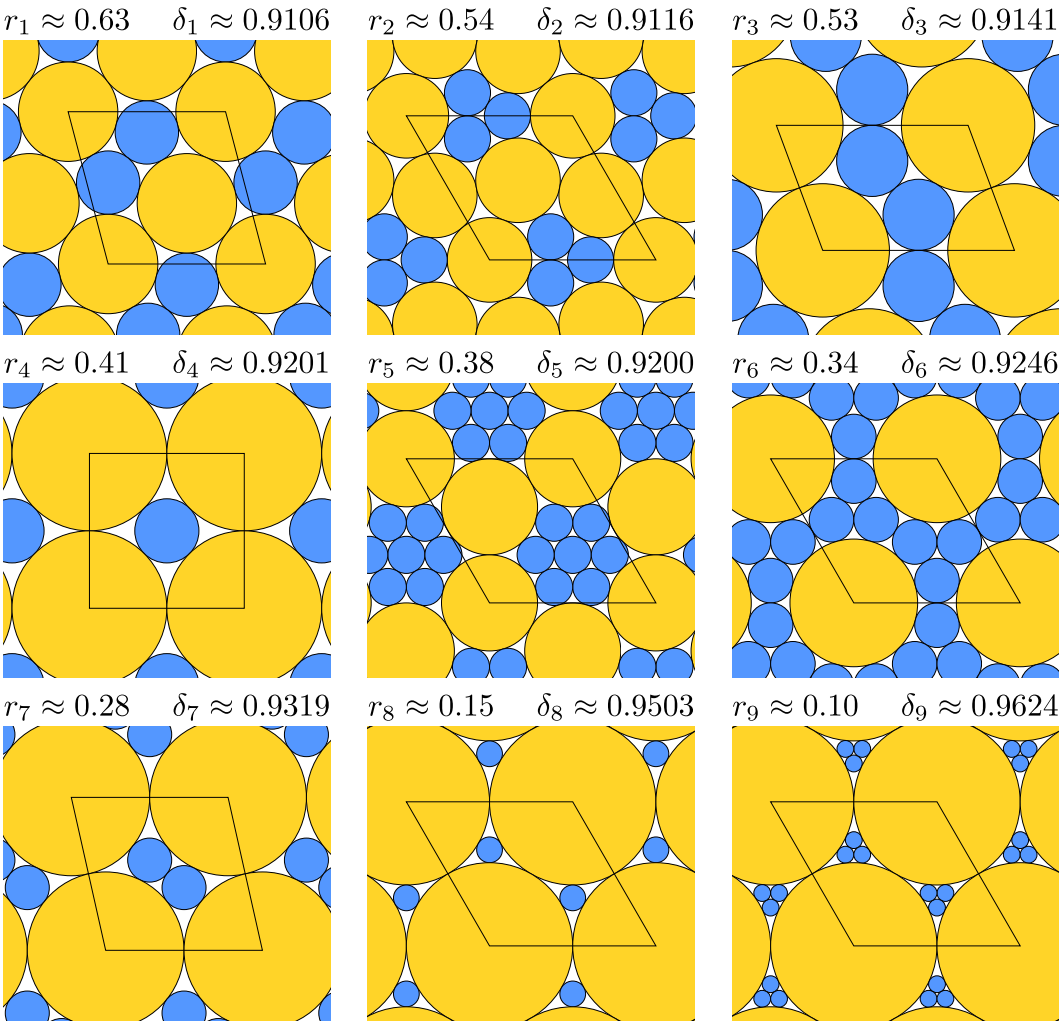


Figure 2 – Ratios pour lesquels la densité maximale est connue. Pour chacun, un empilement périodique (domaine fondamental en noir) qui atteint la densité maximale est représenté. Ces empilements sont tous triangulés.

Références

[1] N. Bédaride and Th. Fernique, *Density of binary disc packings : the 9 compact packings*, preprint, 2020.

[2] H.-Ch. Chang and L.-Ch. Wang, *A simple proof of Thue's theorem on circle packing*, preprint, 2010.

[3] H. Cohn, *A Conceptual breakthrough in sphere packing*, Notices of the AMS, 2017.

[4] Th. Fernique, A. Hashemi and O. Sizova, *Compact packings of the plane with three sizes of discs*, Discrete and Computational Geometry, 2020.

[5] T. Kennedy, *Compact packings of the plane with two sizes of discs*, Discrete and Computational Geometry, 2006.

[6] P. Zimmerman et al. *Calcul Mathématique avec Sage*. CreateSpace Independent Publishing Platform, 2013.

École jeunes chercheur.e.s

L'édition 2021, organizée par O. Blazy et P. Gaborit, a eu lieu virtuellement du 7 au 10 juin.
Un grand merci aux organisateurs d'avoir fait en sorte qu'elle ait lieu !

Toutes les informations sont disponibles à
`https://indico.math.cnrs.fr/event/6689/`

RENDEZ-VOUS À NICE POUR L'ÉDITION 2022 !

Entretien avec

Marthe Bonamy

Chargée de recherches CNRS au LaBRI

Conduit par Brigitte Vallée, le 25 mars 2021

Bonjour Marthe ! Tu pourrais commencer par nous raconter ton parcours, à tes débuts ? Comment t'es-tu orientée vers ta situation présente ?

En seconde, l'école ne m'intéressait pas vraiment, mais les matières littéraires m'attiraient, et je lisais énormément. Je ne travaillais pas beaucoup, et j'avais un niveau moyen.
En première, la professeure de mathématiques a mentionné que si les théorèmes vus en cours étaient "vieux", de nouveaux théorèmes étaient encore prouvés de nos jours. Cela m'a ouvert des horizons nouveaux. Par la suite, j'étais en filière S, et je me suis orientée naturellement vers des classes préparatoires, avec, dans un coin de ma tête, l'idée naïve mais tenace de devenir chercheuse en mathématiques.
Mes débuts en classe de math-sup ont été difficiles ; je n'avais jamais été réellement confrontée aux difficultés scolaires et, là, j'étais vraiment en queue de classe, au moins en mathématiques. À côté, l'introduction à l'informatique me plaisait beaucoup. Là, mon professeur de maths, Grégoire Taviot, a cru en moi et m'a encouragée à changer en profondeur ma façon de travailler. Sur ses conseils, j'ai fait le pari d'arrêter de prendre des notes en cours mais de tout inspecter et assimiler pendant le cours, quitte à sortir de cours épuisée et passer mes soirées à récupérer. Ça a tout changé, et je me surprends encore maintenant à appliquer parfois cette approche du "tout ou rien" à certaines étapes importantes d'un projet. C'était une leçon très importante au-delà de l'aspect scolaire ; il vaut mieux accepter les forces et faiblesses de son profil que d'essayer de suivre d'autres modèles.

Et après ?

J'ai intégré l'ENS de Lyon. Nous étions très peu de filles dans le département Informatique, ce qui donnait un statut un peu particulier. J'y trouvais des côtés positifs comme négatifs, mais j'essayais d'y voir surtout les côtés positifs. Je voulais au départ suivre un cursus équilibré entre les mathématiques et l'informatique, mais progressivement, je me suis plus fermement dirigée vers l'informatique théorique. J'aimais bien les cours donnés à l'école, je choisissais toujours les cours d'informatique-la-plus-théorique, mais malheureusement la théorie et l'algorithmique de graphes n'y étaient pas aussi développés que maintenant.

J'ai découvert ce domaine lors d'une école d'hiver organisée par l'ENS (une super initiative, je trouve) : Louis Esperet est venu de Grenoble faire un cours sur la coloration de graphes, et j'étais tout de suite très enthousiaste. Dans notre cursus, nous devions faire un stage d'été à l'étranger, et Louis m'a suggéré un stage à Durham. L'expérience m'a confortée dans mon affection pour les questions de graphes.
Au retour de ce stage, j'ai rencontré Alexandre Pinlou, et j'ai décidé de faire une thèse à Montpellier en co-direction avec lui et Benjamin Lévêque. J'ai beaucoup aimé mes années de thèse, des années de découverte ; mon co-bureau, Nicolas Bousquet, qui avait un an d'ancienneté de plus que moi en thèse, y a joué un grand rôle : grand frère en recherche, c'était de fait presque un troisième directeur. C'était extrêmement précieux d'avoir quelqu'un avec qui discuter au quotidien tant de recherche que des inquiétudes liées à la thèse. Je mesure ma chance d'avoir été si bien entourée. Alexandre était, sur beaucoup d'aspects, exactement le directeur de thèse qu'il me fallait. Je pense d'ailleurs que nous devrions refaire un projet ensemble !

Ça peut sembler niais, mais le jour où j'ai su que j'avais un poste de chercheuse au CNRS a été l'un des plus beaux jours de ma vie. Cela me semblait presque inconcevable : j'avais, dès ce jour-là, l'assurance à vie de pouvoir continuer à faire de la recherche.

Pour des raisons de calendrier, je n'avais à ce moment-là pas encore eu l'occasion de candidater à des postes de Maître de Conférences, mais c'était bien sûr une carrière que j'envisageais également. J'aimais bien (et j'aime toujours bien) l'activité d'enseignement, et le contact avec les étudiants. Je préférais un poste au CNRS car je m'inquiétais de réussir à jongler entre les rôles d'enseignante et de chercheuse. Que ce soit en contraintes d'emploi du temps (difficile d'improviser des visites de recherche ou conférences) ou en charge mentale. C'est un bémol de mon style de recherche : j'apprécie de pouvoir me plonger dans un problème en oubliant tout le reste. Ceci dit, je garde le contact avec quelques anciens étudiants, et je continue à

enseigner quelques cours de M2. Ceux-ci représentent une fraction minime du service d'un MdC, et pourtant ils suffisent à mettre mon organisation à rude épreuve.

Et ta recherche ? Tu travailles en "graphes". Peux-tu nous en dire plus ? Comment aimes-tu travailler ?

Si on sépare la thématique des graphes grossièrement en deux (théorie des graphes, et algorithmique des graphes), alors, c'est la première des deux thématiques que j'ai découverte en premier et celle qui m'accroche toujours le plus. Mais, progressivement, en particulier lors d'un séjour en Pologne, j'ai découvert le versant algorithmique ; je reste essentiellement branchée sur le versant "théorie des graphes", mais l'algorithmique est un débouché formidable pour ce versant-là : quand on me parle d'un problème d'algorithmique, j'ai un petit traducteur interne (et parfois externe) qui me le transpose en problème de théorie des graphes, et, là, cela commence à me passionner...
En temps normal, (en dehors de la crise sanitaire), j'aime voyager et rendre visite à des collaborateurs étrangers, mais, surtout, j'invite de nombreux chercheurs à Bordeaux, pour travailler avec eux.
J'aime bien me concentrer sur un problème assez précis, sur une semaine ou deux. Cependant, quand j'ai l'impression d'avoir épuisé toutes mes idées, je n'hésite pas à tourner la page et changer de problème. Derrière mes résultats publiés il y a un nombre bien plus grand de problèmes que j'ai attaqués et qui m'ont résisté. Certains me suivent et j'attends simplement une nouvelle idée ou un nouvel outil, d'autres sont oubliés depuis longtemps.
J'ai un peu le même état d'esprit avec les doctorants que je co-encadre (deux thèses soutenues, deux thèses en cours, et un stagiaire M2 dont j'espère qu'il va obtenir un financement pour rester en thèse) : si le sujet n'évolue pas bien au bout d'un certain temps, je leur suggère assez vite un autre angle d'attaque, ou même, souvent, un autre problème. Le risque est souvent de les submerger en les impliquant dans trop de projets différents. J'essaye d'être vigilante à ce niveau. L'encadrement de thèses est l'un des aspects du métier que j'aime le plus, et, en tout cas ; une grande source de satisfaction. Ça peut aussi être très prenant, et, de plus, difficile à prévoir, car les besoins en attention dépendent des étudiants et varient avec l'évolution de la thèse. Pour cette raison, je ne m'engage pas auprès de plus d'un nouveau doctorant par an.
J'aime beaucoup travailler en groupe, devant un tableau. J'ai même du mal à faire de la recherche en solitaire. Quand je commence à avoir des questions ou des idées, mon premier réflexe est de chercher quelqu'un à qui en parler. J'ai tendance à réfléchir à voix haute, et dire beaucoup de choses fausses. Pour autant, j'ai besoin de les dire pour comprendre en quoi elles sont fausses, et trouver à tâtons le chemin. Je préviens mes nouveaux collaborateurs de ce tic de fonctionnement. À la fois pour m'assurer qu'ils ne me fassent pas trop confiance quand je propose une approche, et pour qu'ils gardent un peu espoir dans le fait que je vais peut-être finir par dire quelque chose d'utile.
Je n'ai pas de plan de recherche à proprement parler, ni vraiment de problème phare que j'aimerais résoudre. Le fait que je change souvent de problème me place plutôt dans une démarche où je suis vite influencée par les problèmes que j'entends en conférence ou que des collaborateurs (notamment au LaBRI) me proposent. Le séminaire hebdomadaire de l'équipe bordelaise me tient beaucoup à coeur, notamment à ce titre. De façon amusante, je m'aperçois souvent qu'il y a en réalité une cohérence, des thèmes récurrents dans mes recherches passées, alors même que je l'aurais nié avec beaucoup d'aplomb si on m'avait posé la question sur le moment. Il y a plusieurs plans de recherche qui me plairaient, à cet instant. Je trouve ça extrêmement difficile, et plutôt inutile, d'essayer de deviner lequel je suivrai.

Tu es donc chercheuse à plein temps, et tu côtoyes des enseignants-chercheurs et des enseignantes-chercheuses. Te sens-tu des responsabilités à leur égard ? Lesquelles ?

C'est quelque chose qui était très présent dans l'équipe à Montpellier, où j'ai préparé ma thèse. C'était un sujet fréquemment mentionné, et il était communément admis que les chercheurs, privilégiés dans le monde de la recherche par rapport aux enseignants chercheurs, devaient veiller à rester inclusifs et moteurs dans l'animation et l'organisation de la recherche. J'essaie maintenant à ma façon de suivre cette ligne directrice.
Concrètement, si un enseignant-chercheur est impliqué dans un projet, ce n'est pas sympa d'être très actif sur le projet pendant qu'il ou elle est pris par ses charges d'enseignement. Ça crée des situations bancales où l'enseignant-chercheur ne peut pas contribuer confortablement, alors qu'il est facile (sauf contrainte externe du type visiteur) de temporiser avec un autre projet pour ensuite avancer ensemble en groupe. Autre exemple concret, ça me semble normal d'organiser le

séminaire d'équipe (ce que je fais depuis bientôt 5 ans maintenant, même s'il y a heureusement chaque année un doctorant pour m'épauler), ou de partager avec les collègues les problèmes que j'ai entendus en conférence et dont je pense qu'ils peuvent leur plaire. J'ai aussi demandé et obtenu plusieurs financements de mobilité pour divers doctorants et autres collègues – ça me semble normal.

Tu es une femme chercheuse. Là encore, te sens-tu des responsabilités vis-à-vis des autres femmes que tu rencontres? Quel rôle as-tu envie de jouer auprès d'elles?

Question difficile. Je ne sais pas si je me sens une responsabilité. En revanche, je suis douloureusement consciente de la difficulté qu'il peut y avoir à trouver sa place en tant que chercheuse. Je mets un point d'honneur à être moi-même, porter des robes (colorées), faire des blagues (nulles), sourire (beaucoup), y compris dans des contextes où ce n'est pas forcément attendu, comme lorsque je suis oratrice invitée dans une conférence. Je me dis que si je contribue à changer même un peu l'image qu'on a d'un chercheur, c'est déjà une satisfaction. J'ai pris conscience avec horreur pendant ma thèse du fait que j'avais moi-même des a priori négatifs envers les femmes en maths, qui plus est les femmes féminines. J'espère avoir mûri sur le sujet. De façon plus tangible, je prête attention aux doctorants du domaine. J'essaye de leur parler aussi des difficultés qu'on peut rencontrer, et, quand j'ai une bonne impression, de leur donner des opportunités. C'est particulièrement le cas avec les doctorantes, même si c'est une démarche plus générale.
Pour résumer, en tant que chercheuse, j'essaye simplement de jouer mon rôle de représentation. En tant que personne faisant de la recherche en graphes, j'essaye que les jeunes s'y sentent inclus et qu'ils puissent exploiter leur potentiel. L'idée d'être un modèle pour quelqu'un est touchante mais effrayante, et j'aurais beaucoup de mal à dire que je veux l'être.

On dit souvent que les femmes se posent plus de questions sur leur réussite dans le métier, la qualité de leur recherche, que leurs collègues hommes. Est-ce vrai pour toi aussi? As-tu déjà ressenti le syndrôme de l'imposteur?

Aha, oui, très souvent. C'est le cas de la plupart des chercheurs que je connais, hommes et femmes. C'est une petite voix désagréable qu'on apprend au fil du temps à ignorer… du moins dans les bons jours. Dans les mauvais jours, je me rassure parfois en pensant au fait que certains collaborateurs (dont Nicolas Bousquet et Louis Esperet, que je mentionnais précédemment !) me côtoient depuis longtemps et continuent visiblement à me tolérer. Je ne crois pas que la petite voix disparaisse vraiment un jour, je crois surtout qu'on lui prête moins attention. J'ai encore l'impression d'être une chercheuse inexpérimentée, et je suis vite mal à l'aise quand je sens qu'on attend autre chose de moi. Mon premier doctorant co-encadre actuellement un stage M2 qui va peut-être déboucher sur une thèse. Ça me fait bien sûr plaisir, mais ça me semble absurde aussi de devenir une grand-mère scientifique. Je suis encore pleine d'incertitudes, je navigue à vue… mais je m'amuse dans mon travail, et je trouve du plaisir dans ce que je fais. C'est sans doute le plus important au quotidien.

Et la médaille de bronze?

Le processus de sélection pour une telle récompense est si fort qu'il me met un peu mal à l'aise…. Mais, c'est vrai que cela fait très plaisir d'avoir été choisie ! Ça a beaucoup de valeur pour ma famille, pour qui mon métier reste énigmatique. Mes parents gardent espoir que j'aie l'an prochain l'or ou au moins l'argent, et risquent d'être un peu déçus de voir que je ne ramènerai même pas le bronze une deuxième fois. Je ne leur ai pas encore avoué…

Les journées nationales 2021 du GDR IM

ont eu lieu en distanciel du 23 au 26 mars. Les transparents des conférenciers peuvent être téléchargés sur le site des journées
`https://jnim2021.sciencesconf.org/program`
et des vidéos seront prochainement accessibles sur le site du GDR :
`http://www.gdr-im.fr`

NOS JOURNÉES NATIONALES 2022 AURONT LIEU À LILLE, DU 29 MARS AU 1ER AVRIL : RÉSERVEZ CES DATES !

Entretien avec

Ludovic Patey

Chargé de recherches CNRS à l'ICJ

Conduit par Youssouf Oualhadj le 12 mars 2020

Bonjour Ludovic, peux tu revenir brièvement sur ton parcours?

Après le lycée, j'ai intégré *SUPINFO*; une école d'ingénieur avec des campus à travers toute la France et à l'internationale, j'y ai passé deux ans dans le campus de Paris et une année à Grenoble. C'est une école d'informatique orientée technologie avec peu de cours théoriques. À partir de la deuxième année, j'ai commencé à suivre en parallèle des cours de mathématiques à distance avec le *CNED* et j'ai pu suivre le cursus de L1 et L2 de Mathématiques. Par la suite en 2009, j'ai passé le concours externe de l'ENS Paris en Informatique et j'ai été admis en L3 d'Informatique. Ensuite, j'ai suivi les cours du Master Parisien de Recherche en Informatique (*MPRI*) entre 2010 et 2012. Entre 2012 et 2013 j'ai suivi les cours de Master de Logique et Fondements de L'informatique (*LMFI*). En 2013, j'ai entamé une thèse intitulée *Mathématiques à rebours des théorèmes ramseyens* encadrée par Laurent Bienvenu, qui été mon enseignant de Calculabilité au MPRI, et Hugo Herbelin. Après avoir soutenu en 2016, j'ai passé une année de Post-doctorat à Berkeley en tant que « Morrey Visiting Assistant Professor ». Enfin depuis 2017, je suis chargé de recherche CNRS à L'Institut Camille Jordan à Lyon.

Directement après le lycée tu as rejoins une école d'informatique, cela s'explique-t-il par le fait que tu as toujours voulu faire de l'informatique?

Oui tout-à-fait, j'ai toujours été fasciné par la puissance de la programmation avec un simple ordinateur, par rapport à d'autres domaines demandant du matériel beaucoup plus onéreux. Mais au bout de deux ans j'ai eu l'impression d'en avoir fait le tour, j'étais à la recherche de nouveaux challenges intellectuels, ce qui a motivé les cours du CNED, puis j'ai décidé de tenter le concours à l'ENS.

Qu'est-ce qui a motivé ton choix pour l'ENS?

A vrai dire je ne connaissais pas plus que cela! Mais le fait d'avoir suivi en parallèle des cours d'informatique orientés technologies et des cours de mathématiques pures m'a donné envie de mélanger les deux. Un jour un ami m'a dit : « Il y a cette école avec un parcours qui conviendrait à ton profil » Je me suis renseigné et j'ai décidé de passer le concours.

Qu'est ce qui t'a attiré le plus dans la Calculabilité?

Au MPRI, j'ai suivi le cours de calculabilité de Laurent Bienvenu et Olivier Bournez et cela m'a, immédiatement, énormément plu! J'ai réalisé que le genre de raisonnement utilisés en calculabilité correspond à ma manière de me représenter les choses. Personnellement, je crois que l'on peut vraiment être très bon dans un domaine et très mauvais dans un autre, donc autant choisir un domaine qui nous convient et dans lequel on peut aller loin!

Tu as commencé par faire beaucoup de programmation, maintenant tu t'intéresses à des questions plus théorique, y-t-il des similarités?

Me concernant je ne fais aucune différence entre les deux disciplines, je suis un fervent croyant de la correspondance de *Curry-Howard* et pas que d'un point de vue formel. Quand on programme, on essaye de respecter des bonnes pratiques, on accorde beaucoup de temps à concevoir des solutions logiciels élégantes, claires et faciles à manipuler. Me concernant j'essaye d'adopter la même discipline quand il s'agit de faire des preuves ou manipuler des notions abstraites. J'essaye de decomposer les preuves, de trouver les bons concepts pour rendre le raisonnement le plus simple possible, et aussi à le rendre le plus compréhensible possible pour les autres.

Peux tu nous parler un peu des Mathématiques à rebours et de leur succès?

Avant tout, il faut savoir que tel que je les conçois, les Mathématiques à rebours sont un formalisme pour faire de la calculabilité et que quand on prouve un résultat de Mathématiques à rebours, on prouve un résultat de calculabilité qui nous permet d'obtenir des résultat en théorie de la preuve. Cet aspect théorie de la preuve m'intéresse moins et une partie de la communauté des Mathématiques à rebours n'est pas si intéressée que ça par cet aspect-la non plus. Mais je dirais que les mathématiques à rebours ont soulevé des points intéressants concernant la structure des mathématiques. Par exemple des phénomènes tels que : la majorité des théorèmes classiques en mathématiques vont demander une

puissance axiomatique faible et être equivalent à cinq grands systèmes de l'arithmétique ce qui montre que les mathématiques sont très structurées, et c'est un phénomène dont on avait pas conscience ! D'autant plus qu'il a des conséquences importantes, notament du point de vue du programme de Hilbert. Bien sûr, le programme de Hilbert n'est pas réalisable en général tout simplement parce que on a découvert les théorèmes d'incomplétudes de Gödel entre autres. Typiquement, la notion de cohérence de l'arithmétique de Peano est un énoncé finitaire pour lequel il existe des preuves à l'aide des méthodes infinitaires, par exemple ZFC permet de prouver l'arithmétique de Peano mais ce n'est pas prouvable par l'arithmétique de Peano. Par conséquent le programme de Hilbert a été remis en question, et ce que montrent les mathématiques à rebours, c'est que la plupart des énoncés mathématiques sont prouvables dans un système axiomatique faible qui s'appelle le lemme faible de Köning et qui, lui, est conservatif dans un système finitaire. Cela implique que la majorité des énoncés mathématiques peuvent se prouver dans un système finitaire. D'une certaine manière, à l'aide des mathématiques à rebours on arrive montrer que la majorité des énoncés mathématiques échappent aux paradoxes engendrés par l'infini. Je pense vraiment que le grand succès des mathématiques à rebours vient du fait que c'est une réalisation partielle du programme de Hilbert.

Quelles directions penses-tu donner à tes thématiques de recherche pour les années qui viennent ?

En fait, le visage des Mathématiques à rebours a pas mal changé ces dernières années. Historiquement ce formalisme été étudié pour des questions de l'ordre de la théorie de la preuve, ensuite il a été utilisé pour résoudre des problèmes de calculabilité, maintenant on s'oriente vers utilisation de ce formalisme comme un outil pour comparer la puissance calculatoire entre les théorèmes et cela a permis de définir d'autres outils plus fin notament la réduction calculatoire qui s'inspire de la théorie de la calculabilité et de la complexité. Bien sûr avec ces nouveaux outils d'autres problématiques excitantes se posent.

As tu été confronté à des difficultés dans ton parcours

J'ai eu beaucoup de mal à obtenir une bourse de thèse, après le MPRI et j'ai refait un M2 au LMFI, ce qui était une bonne chose car cela m'a permis d'obtenir des bases solides en logique mathématique. À présent, je vois cela comme une opportunité qui s'est offerte à moi plus tôt qu'une difficulté.

Tu as passé une année à Berkeley, entre le statut de chercheur au CNRS et chercheur à Berkeley, y a-t-il des différences ?

Mon expérience été assez courte, mais je pense que c'est assez incomparable. à Berkeley j'ai eu du étudiants qui ont déboursé des fortunes ou ont eu des bourses prestigieuses. C'était très intimidant et j'ai apprécié l'expérience, mais le statut de chercheur au CNRS est unique. J'ai une vocation à faire de la recherche plus que de l'enseignement, et le CNRS me permet de m'épanouir dans cette voie.

Le saviez-vous ?

Il existe des ensembles de dés *non-transitifs*, c'est-à-dire que : si A joue contre B, A gagne en moyenne ; si B joue contre C, B gagne en moyenne ; et si C joue contre A, C gagne en moyenne !
Voici trois dés équilibrés à six faces ayant cette propriété : $A = 6, 3, 3, 3, 3, 3$; $B = 5, 5, 5, 2, 2, 2$; et $C = 4, 4, 4, 4, 4, 1$.
Décidément, les probabilités ne cessent de nous surprendre...
Pour en savoir plus :
`https://fr.wikipedia.org/wiki/Dés_non_transitifs`

Vous aimez cette rubrique ? Nous lançons un appel à contributions !!!

Multiplier des entiers en temps $O(n \log n)$

Joris van der Hoeven
CNRS, LIX (UMR 7161)

Résumé. Il a été démontré récemment que deux entiers de n chiffres peuvent être multipliés en temps $O(n \log n)$ [12]. L'existence d'un tel algorithme fut conjecturé en 1971 par Schönhage et Strassen [23]. Ils émettaient également leurs doutes sur l'existence d'une méthode encore plus rapide, ce que l'on ignore toujours.

Dans cet article, je présenterai brièvement une longue histoire et je poursuivrai avec un aperçu du nouvel algorithme.

Cet article est une traduction libre de [15].

Introduction. Quelle est la meilleure façon de multiplier deux entiers ? Cette question, simple en apparence, est peut-être le plus ancien problème mathématique non résolu. Ainsi, ce problème est au moins dix fois plus ancien que la conjecture de Fermat, alias « théorème de Wiles ».

Il faut bien sûr préciser ce que nous entendons par « meilleur ». Pour cela, il a fallu attendre l'invention de la machine de Turing : équipée d'un modèle de calcul précis, on peut définit le nombre $\mathsf{M}(n)$ d'étapes nécessaires pour multiplier deux nombres de n chiffres. La meilleure méthode est alors celle pour laquelle $\mathsf{M}(n)$ augmente aussi lentement en fonction de n.

Prenons par exemple la méthode de l'école primaire, qui consiste à multiplier chaque chiffre du premier nombre par chaque chiffre du deuxième nombre, en ajoutant les résultats de manière appropriée. Cela donne $\mathsf{M}(n) = O(n^2)$: il existe une constante $C > 0$ avec $\mathsf{M}(n) \leqslant Cn^2$ pour tout n.

Afin de rendre notre question principale indépendante de la machine de Turing en cher et en os sur laquelle nous faisons notre calcul, nous nous intéressons uniquement au temps de calcul à un facteur constant près. Une méthode 100 fois plus rapide n'est donc pas une amélioration significative, mais un algorithme $\log\log\log n$ fois plus rapide est un énorme pas en avant.

C'est probablement Kolmogorov qui a été le premier à formuler notre problème ainsi, dans un séminaire célèbre à Moscou. Emporté par son enthousiasme, il avait également conjecturé que $n^2 = O(\mathsf{M}(n))$. Car, raissona-t-il, s'il y avait une meilleure méthode que celle de l'école, on l'aurait bien trouvé depuis six mille ans.

La formulation précise d'un problème facilite la recherche de solutions. Mais l'absence d'une telle formulation n'exclut pas d'éventuels progrès. Les Babyloniens ont déjà calculé $\sqrt{2}$ jusqu'à seize chiffres derrière la virgule. Un jour, on trouvera peut-être une tablette d'argile avec des méthodes inédites de multiplication à grande vitesse. Les amateurs du nombre π, comme mon compatriote Ludolph van Ceulen, auraient pu en tirer profit (voir la figure 3a).

Karatsuba. La conjecture de Kolmogorov ne fit pas long feu. Après trois semaines, il a été surpris par un jeune élève avec une méthode de multiplication en $O(n^{\log 3/\log 2})$ étapes. Kolmogorov rédigea immédiatement cette nouvelle trouvaille, la publia sous le nom de son créateur, Karatsuba, et la regroupa avec un autre article qui n'avait rien à voir [18, 17].

Expliquons l'idée de Karatsuba avec un exemple :

$$\begin{aligned} u &= 220629012020 \\ v &= 314159265358. \end{aligned}$$

Nous commençons par couper les deux nombres en deux :

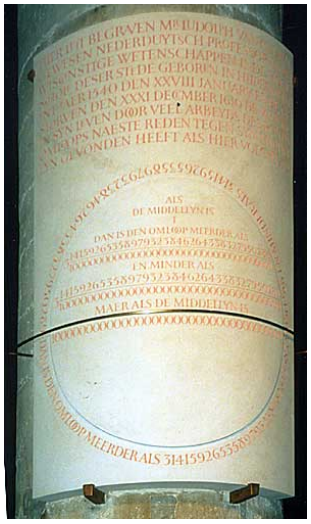
$$\begin{aligned} u &= \overbrace{220629}^{a} \times \overbrace{1000000}^{x} + \overbrace{012020}^{b} \\ v &= \underbrace{314159}_{c} \times 1000000 + \underbrace{265358}_{d} \end{aligned}$$

Ensuite, nous faisons deux additions et trois multiplications :

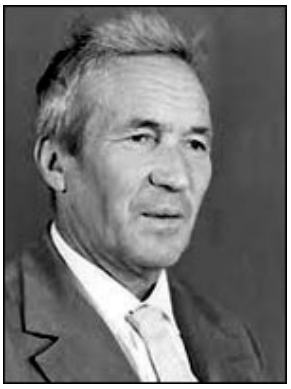
$$\begin{aligned} a+b &= 232649 \\ c+d &= 579517 \\ ac &= 069312586011 \\ bd &= 003189603160 \\ (a+b)(c+d) &= 134824050533 \end{aligned}$$

Maintenant, nous remarquons qu'il suffit de deux soustractions pour trouver

$$\begin{aligned} ad+bc &= (a+b)(c+d) - ac - bd \\ &= 62321861362. \end{aligned}$$



(a) ◀ Pierre commémorative dans le Pieterskerk à Leyde, avec une reconstruction du texte original de la pierre tombale de Ludolph van Ceulen (1540–1610), qui a passé vingt-cinq ans de sa vie à calculer 35 décimales de π.



(b) Andrej Kolmogorov.

(c) Anatoly Karatsuba.

(d) Volker Strassen (à gauche) et Arnold Schönhage (à droite).

(e) John Pollard.

Figure 3 – Quelques portraits.

Enfin, on a

$$\begin{aligned} uv &= (ax+b)(cx+d) \\ &= acx^2 + (ad+bc)x + bd, \end{aligned}$$

et on termine avec une dernière addition :

$$\begin{array}{rrr} 069312586011000000000000 & ac & x^2 \\ 62321861362000000 & (ad+bc) & x \\ 003189603160 & bd & \\ \hline 06931264833284551603160 & uv & \end{array}$$

Au final, nous avons réduit une multiplication à 12 chiffres à trois multiplications à 6 chiffres et quelques additions et soustractions.

En général, multiplier des nombres deux fois plus longs prend environ trois fois plus de temps. Plus précisément, on a l'« inégalité récurrente » suivante :

$$\mathsf{M}(2n) \leqslant 3\mathsf{M}(n) + O(n).$$

Pour une certaine constante C et pour $n = 2^r$, nous avons donc

$$\begin{aligned} \mathsf{M}(n) &\leqslant 3\mathsf{M}(n/2) + Cn \\ &\leqslant 9\mathsf{M}(n/4) + \left(1+\tfrac{3}{2}\right)Cn \\ &\leqslant 27\mathsf{M}(n/8) + \left(1+\tfrac{3}{2}+\tfrac{9}{4}\right)Cn \\ &\vdots \\ &\leqslant 3^r\mathsf{M}(1) + O\left(\left(\tfrac{3}{2}\right)^r n\right) = O(3^r). \end{aligned}$$

Or nous pouvons toujours rajouter des zéros à gauche d'un nombre afin que son nombre de chiffres devienne une puissance de deux. En fin de

compte, ceci prouve

$$\mathsf{M}(n) \quad = \quad O(n^{\log 3/\log 2}).$$

Des nombres aux polynômes. L'un des ingrédients de la méthode de Karatsuba est de couper les nombres en deux morceaux. Cela permet de voir u et v comme des polynômes $ax+b$ et $cx+d$ de degré < 2. En fait, cela revient simplement à travailler en base $x = 1\,000\,000$ au lieu de 10.

L'idée de remplacer l'arithmétique entière par l'arithmétique polynomiale a déjà été suggérée par Kronecker au 19ème siècle. Par exemple, nous pouvons couper un nombre de n chiffres en l morceaux de $p := \lceil n/l \rceil$ chiffres et réinterpréter le résultat comme un polynôme.

Dans les années 1960, on a développé une série d'améliorations de la méthode de Karatsuba, en prenant le nombre de morceaux l supérieur à deux [24, 22, 19] ; voir le tableau 1 pour un aperçu historique.

Sans entrer dans les détails, chacune de ces améliorations est basée sur une généralisation de l'astuce de Karatsuba. La multiplication de deux polynômes de degré $< l$ se réduit alors à $2l-1$ multiplications de coefficients, après quoi $\mathsf{M}(n) = O(n^{\log(2l-1)/\log(l-1)})$.

Des polynômes aux cyclonômes. Désormais, nous nous focaliserons principalement sur la multiplication de polynômes et il est utile de travailler avec des coefficients dans un anneau général R. Nous laissons de côté le choix précis de R, pour l'instant.

Pour la suite, il est également utile de travailler avec des « cyclonômes » au lieu de polynômes. Un *cyclonôme* de degré l est un élément de $R[x]/(x^l-1)$.

La relation $x^l = 1$ n'entre en action que lorsque le degré d'un polynôme excède l. Le produit de deux polynômes de degré $< l/2$ dans $R[x]$ peut ainsi tout tout aussi bien se calculer dans $R[x]/(x^l-1)$.

L'avantage des cyclonômes est que nous avons de nouvelles astuces de calcul à notre disposition. Par exemple, supposons que $l = 2$ et que 2 soit inversible dans R. Alors il devient possible d'optimiser la méthode de Karatsuba : modulo x^2-1 on a

$$(a_1x+a_0)(b_1x+b_0) = \frac{\hat{a}_0\hat{b}_0 - \hat{a}_1\hat{b}_1}{2}x + \frac{\hat{a}_0\hat{b}_0 + \hat{a}_1\hat{b}_1}{2},$$

où

$$\begin{array}{rclcrcl} \hat{a}_0 & = & a_0 + a_1 & \qquad & \hat{b}_0 & = & b_0 + b_1 \\ \hat{a}_1 & = & a_0 - a_1 & & \hat{b}_1 & = & b_0 - b_1. \end{array}$$

Dans $R[x]/(x^2-1)$, le calcul d'un produit ne nécessite donc que deux multiplications dans R. Il y a aussi un certain nombre d'additions, de soustractions et de divisions par deux.

Les relations ci-dessus viennent de la factorisation

$$(x^2-1) = (x-1)(x+1) \qquad (1)$$

et de l'application du théorème des restes chinois à celle-ci :

$$\begin{array}{rcl} R[x]/(x^2-1) & \cong & R[x]/(x-1) \times R[x]/(x+1) \\ \overline{a_1x+a_0} & \mapsto & (\overline{a_0+a_1}, \overline{a_0-a_1}) \end{array}$$

Cela permet de remplacer les calculs arbitraires dans $R[x]/(x^2-1)$ par des calculs dans $R[x]/(x-1) \times R[x]/(x+1) \cong R^2$.

La multiplication FFT. La factorisation (1) est valable pour chaque anneau R. Dans certains anneaux, le polynôme x^l-1 se scinde de la même manière en facteurs linéaires pour certains $l > 2$. Cela arrive dès que R admet un élément ω avec $\sum_{k=0}^{l-1}(\omega^j)^k = 0$ pour $j = 1, \ldots, l-1$. Un tel élément ω est appelé racine principale d'unité d'ordre l et conduit à la factorisation

$$x^l - 1 \quad = \quad \prod_{0 \leqslant k < l} (x - \omega^k).$$

Si l est également inversible dans R, le théorème des restes chinois donne alors :

$$R[x]/(x^l-1) \quad \cong \quad \prod_{0 \leqslant k < l} R[x]/(x-\omega^k).$$

De gauche à droite, cet isomorphisme est appelé *transformée de Fourier discrète* ou DFT. Pour tout $A \in R[x]$ et $0 \leqslant k < l$ on a $x = \omega^k$ et $P(x) = P(\omega^k)$ modulo $x - \omega^k$, donc

$$\mathrm{DFT}(\bar{A}) \quad = \quad (\overline{A(1)}, \overline{A(\omega)}, \ldots, \overline{A(\omega^{l-1})}).$$

L'algèbre $R[x]/(x-\omega^k)$ est à son tour isomorphe à R pour tout k, d'où

$$R[x]/(x^l-1) \quad \cong \quad R^l.$$

−4000	Onbekend	$O(n^2)$
1962	Karatsuba	$O(n^{\log 3/\log 2})$
1963	Toom	$O\left(n2^{5\sqrt{\frac{\log n}{\log 2}}}\right)$
1966	Schönhage	$O\left(n2^{\sqrt{\frac{2\log n}{\log 2}}(\log n)^{\frac{3}{2}}}\right)$
1969	Knuth	$O\left(n2^{\sqrt{\frac{2\log n}{\log 2}}\log n}\right)$
1971	Pollard	$O(n\log n\log\log n\cdots)$
1971	Schönhage-Strassen	$O(n\log n\log\log n)$
2007	Fürer	$O(n\log n2^{O(\log^* n)})$
2014	Harvey-vdH-Lecerf	$O(n\log n8^{\log^* n})$
2017	Harvey	$O(n\log n6^{\log^* n})$
2017	Harvey-vdH	$O\left(n\log n\left(4\sqrt{2}\right)^{\log^* n}\right)$
2018	Harvey-vdH	$O(n\log n4^{\log^* n})$
2019	Harvey-vdH	$O(n\log n)$

Table 1 – De meilleures limites supérieures pour $\mathsf{M}(n)$ au fil des ans. Dans le tableau, la fonction $\log^*$ est définie par $\log^* x = \min\left\{n\in\mathbb{N} : \left(\log\circ^{n}\times\circ\log\right)(x)\leqslant 1\right\}$.

Or des calculs dans l'anneau R^l se font à moindre frais : une multiplication dans R^l équivaut par exemple à l multiplications dans R. Si nous disposions d'algorithmes efficaces à la fois pour la DFT et son inverse DFT^{-1}, alors cela donnerait une bonne méthode pour multiplier des cyclonômes $A, B \in R[x]/(x^l-1)$:

$$AB \quad = \quad \mathrm{DFT}^{-1}(\mathrm{DFT}(A)\,\mathrm{DFT}(B)).$$

Cela s'appelle la *multiplication FFT*.

La transformation de Fourier rapide. Mais comment calculer rapidement une telle DFT ? Nous avons déjà étudié le cas $l = 2$. Plus généralement, la factorisation

$$x^{2l}-1 \quad = \quad (x^l-1)(x^l+1)$$

pour des degrés pairs $2l$ induit l'isomorphisme

$$R[x]/(x^{2l}-1) \quad \cong \quad R[x]/(x^l-1)\times R[x]/(x^l+1).$$

Si $A, B \in R[x]$ sont des polynômes de degré $< l$, alors cet isomorphisme envoie $A + Bx^l$ vers $(A+B, A-B)$; pour la lisibilité, nous omettons désormais les barres des modulos. Calculer $A \pm B$ revient à additionner et soustraire l fois dans R. Pour l'isomorphisme dans l'autre sens, il faut rajouter $2l$ divisions par deux.

Si ω est une racine principale d'unité d'ordre $2l$, on a en outre l'isomorphisme suivant :

$$\begin{array}{rcl} R[x]/(x^l+1) & \cong & R[x]/(y^l-1) \\ \displaystyle\sum_{0\leqslant k<l} a_k x^k & \mapsto & \displaystyle\sum_{0\leqslant k<l} (a_k\omega^k)y^k. \end{array}$$

Le calcul de cet isomorphisme se réduit à l multiplications par des puissances de ω. Ici, il est important de noter qu'une multiplication par une puissance de ω est parfois moins chère qu'une multiplication arbitraire dans R (voir plus bas).

En résumé, cela montre comment une DFT de longueur $2l$ peut être réduite à deux DFTs de longueur l. Si on écrit $\mathsf{F}(l)$ pour le temps qu'il faut pour calculer une DFT de longueur l, puis $\mathsf{T}_\pm$ pour le temps d'une addition ou d'une soustraction dans R, et T_ω pour le temps d'une multiplication par une puissance de ω, alors nous avons

$$\mathsf{F}(2l) \quad \leqslant \quad 2\mathsf{F}(l) + 2l\mathsf{T}_\pm + l\mathsf{T}_\omega.$$

En appliquant cette formule récursivement dans le cas où $l = 2^{\lg l}$ est une puissance de deux, nous obtenons

$$\begin{array}{rcll} \mathsf{F}(l) & \leqslant & 2\mathsf{F}(l/2) + l\left(\mathsf{T}_\pm + \frac{1}{2}\mathsf{T}_\omega\right) & \\ & \leqslant & 4\mathsf{F}(l/4) + 2l\left(\mathsf{T}_\pm + \frac{1}{2}\mathsf{T}_\omega\right) & \\ & \vdots & & \\ & \leqslant & (l/2)\mathsf{F}(2) + (\lg l - 1)l\left(\mathsf{T}_\pm + \frac{1}{2}\mathsf{T}_\omega\right) & \\ & \leqslant & l\lg l\left(\mathsf{T}_\pm + \frac{1}{2}\mathsf{T}_\omega\right). & (2) \end{array}$$

Pour la transformation inverse, il faut rajouter l divisions par l.

Intermezzo. Avant de continuer, c'est un bon moment pour quelques commentaires. La FFT a percé en 1965, après la publication de l'article de Cooley et Tukey [3]. Mais une méthode similaire avait déjà été décrite dans des travaux non publiés de Gauss [6, 14].

Par ailleurs, nous avons vu qu'une multiplication de cyclonômes peut être réduite à deux DFT directes plus une DFT inverse. En 1970, Bluestein a noté qu'une DFT de longueur l peut également être réduite à un produit de cyclonômes de même degré l [2].

Pour expliquer cela, supposons pour simplifier que l est pair et que η est une racine principale d'unité d'ordre $2l$ avec $\eta^2 = \omega$. Pour des entiers j, k, on a alors

$$\eta^{(j+l)^2} = \eta^{j^2}\eta^{2l(j+l/2)} = \eta^{j^2}$$

et

$$\omega^{jk} = \eta^{j^2}\eta^{k^2}\eta^{-(j-k)^2}.$$

Le coefficient j-ième de la DFT d'un cyclonôme $u_0 + \cdots + u_{l-1}x^{l-1}$ vaut donc

$$\sum_{0\leqslant k<l} u_k\omega^{jk} \;=\; \eta^{j^2}\sum_{0\leqslant k<l}(u_k\eta^{k^2})\eta^{-(j-k)^2}.$$

Dans la somme à droite nous reconnaissons maintenant le produit de deux cyclonômes :

$$\begin{aligned} V &= \sum_{0\leqslant k<l}(u_k\eta^{k^2})x^k \\ W &= \sum_{0\leqslant k<l}\eta^{-k^2}x^k. \end{aligned}$$

Retour aux nombres entiers. En 1971, pas moins de trois méthodes apparurent pour appliquer la FFT à la multiplication des nombres entiers [21, 23]. Chacune de ces méthodes reposait sur un choix distinct de R. Le choix le plus naturel est de prendre $R = \mathbb{C}$ et $\omega = \mathrm{e}^{2\pi\mathrm{i}/l}$. Bien sûr, nous ne pouvons travailler qu'avec des approximations de nombres complexes dans notre cas. Pour multiplier des nombres de n chiffres, on peut prouver qu'il suffit de travailler avec une précision de $C\log n$ chiffres derrière la virgule pour une certaine constante $C > 0$. Cela signifie que nous pouvons travailler avec $l = O(n/\log n)$ blocs de $O(\log n)$ chiffres. En combinaison avec (2), ceci donne

$$\mathsf{M}(n) = O\left(l\log l\mathsf{M}(\log n)\right) = O\left(n\mathsf{M}(\log n)\right).$$

En appliquant cette formule de manière récursive, nous obtenons

$$\mathsf{M}(n) = O(n\log n\log\log n\log\log\log n\cdots).$$

Ceci donnait le «premier algorithme» de l'article de Schönhage–Strassen [23].

Cependant, l'algorithme zéro fut découvert légèrement plus tôt par Pollard [21]. Il proposa de prendre $R = \mathbb{F}_p$, où p est un nombre premier de la forme $p = s2^r + 1$ (plus que s soit petit, mieux que ça vaut). Pour de tels nombres premiers p, nous savons qu'il existe des racines primitives d'unité d'ordre 2^r. Cette fois-ci encore, cela permet de choisir $\log p = O(\log p)$ et $l = O(n/\log n)$, ce qui conduit à la même borne de complexité pour $\mathsf{M}(n)$ que ci-dessus. Pour être tout à fait correct, il faut noter que cette borne de complexité ne figurait pas dans l'article de Pollard. Il était plus intéressé par un algorithme pratique et son article décrit plusieurs optimisations en ce sens. Pour de très grands nombres, son algorithme est toujours le meilleur sur les ordinateurs d'aujourd'hui [8].

Pour le «deuxième algorithme» de Schönhage–Strassen, nous passons au système binaire et prenons $R = \mathbb{Z}/\ (2^m+1)\mathbb{Z}$, où m est une puissance de deux. Dans cet anneau, nous avons par définition $2^m = -1$, de sorte que $\omega := 2$ est une racine principale d'unité d'ordre $2m$. Un autre avantage est que ω est une racine « rapide » de l'unité. Nous entendons par là que nous pouvons rapidement multiplier par des puissances de ω : il suffit de décaler les bits du nombre en prenant soin d'utiliser la relation 2^m-1 lorsque l'on dépasse 2^m. Pour $l \in \{m, 2m\}$ Schönhage et Strassen montrent ensuite comment une multiplication dans $\mathbb{Z}/(2^{lm/2}+1)\mathbb{Z}$ se réduit à l multiplications dans R. En écrivant $\mathsf{M}'(m)$ pour le coût d'une multiplication dans R, cela donne

$$\mathsf{M}'(lm/2) \;\leqslant\; l\mathsf{M}'(m) + O(ml\log l). \quad (3)$$

Le terme $O(ml\log l)$ vient des DFTs, où on utilise le fait que $\mathsf{T}_\omega = O(l)$ dans R. Le terme $l\mathsf{M}'(m)$ vient de la multiplication « interne » dans $\prod_{k=0}^{l-1} R[x]/(x-\omega^k) \cong R^l$.

Réexprimé en fonction de n, l'inégalité (3) conduit *grosso modo* à la relation

$$\mathsf{M}'(n) \;\leqslant\; 2n^{1/2}\mathsf{M}'(n^{1/2}) + Cn\log n, \quad (4)$$

pour une certaine constante C. On peut ensuite « dérouler » cette formule :

$$\begin{aligned}\mathsf{M}'(n) &\leqslant 2n^{1/2}\mathsf{M}'(n^{1/2}) + Cn\log n\\ &\leqslant 4n^{3/4}\mathsf{M}'(n^{1/4}) + 2Cn\log n\\ &\leqslant 8n^{7/8}\mathsf{M}'(n^{1/8}) + 3Cn\log n\\ &\vdots\\ &\leqslant n\log n\mathsf{M}'(O(1)) + Cn\log n\log\log n.\end{aligned}$$

Cela prouve que $\mathsf{M}(n) = O(n\log n\log\log n)$, et cette borne a tenu pendant quarante-cinq ans.

Et ensuite ? Parmi les trois méthodes de 1971 que l'on vient de rappeler, la dernière présente un inconvénient majeur : puisque $l \leqslant 2m$, une multiplication de longueur n est « seulement » réduite à des multiplications de longueur $O(\sqrt{n})$ au lieu de $O(\log n)$. En revanche, contrairement aux deux autres méthodes, les DFTs ne coûtent presque rien. Cela fournit deux pistes d'amélioration.

Une première option est de réduire les coûts des DFTs à coefficients dans $\mathbb{C}$ ou $\mathbb{F}_p$. En 2007, Fürer fut le premier a appliquer cette stratégie avec succès [5]. Sa méthode conduit à une inégalité de la forme

$$\begin{aligned}\frac{\mathsf{M}(n)}{n\log n} &\leqslant K\frac{\mathsf{M}(n')}{n'\log n'} + O(1),\\ \text{avec}\quad n' &= O((\log n)^2)\end{aligned}$$

et la borne suivante pour $\mathsf{M}(n)$:

$$\begin{aligned}\mathsf{M}(n) &= O(n\log nK^{\log^* n})\\ \log^* x &= \min\left\{k\in\mathbb{N} : \left(\log\circ\overset{k\times}{\dots}\circ\log\right)(x)\leqslant 1\right\}.\end{aligned}$$

Fürer ne s'attarda pas sur le « facteur d'expansion » $K > 1$ précis. Depuis 2014, David Harvey, Grégoire Lecerf, et moi-même avons pu faire baisser ce facteur de plus en plus [13, 9, 10, 11] ; voir le tableau 1.

Notre deuxième option consiste à réexaminer l'inégalité (4). Or le facteur 2 dans $\underline{2}n^{1/2}\mathsf{M}'(n^{1/2})$ est très exactement compensé par le fait que $\log\sqrt{n} = 1/2\log n$: en déroulant l'inégalité, chaque itération nécessite exactement $Cn\log n$ opérations supplémentaires. Si nous pouvions améliorer ne serait-ce que très légèrement ce facteur 2, le déroulement se ferait ainsi :

$$\begin{aligned}&\mathsf{M}(n)\\ &\leqslant 1.98n^{1/2}\mathsf{M}(n^{1/2}) + Cn\log n\\ &\leqslant 1.98^2n^{3/4}\mathsf{M}(n^{1/4}) + (1+0.99)Cn\log n\\ &\leqslant 1.98^3n^{7/8}\mathsf{M}(n^{1/8}) + (1+0.99+0.99^2)Cn\log n\\ &\vdots\\ &\leqslant o(n\log n) + 100Cn\log n.\end{aligned}$$

Halte ! Nous avons bien lu ?

$$\mathsf{M}(n) = O(n\log n).$$

Avec cette nouvelle ligne de mire, nous allons pouvoir broder. Il suffit par exemple de prouver que

$$\mathsf{M}(n) \leqslant \alpha n^{(d-1)/d}\mathsf{M}(n^{1/d}) + O(n\log n), \quad (5)$$

où $n \geqslant 2$ et $\alpha < 1/d$.

En route vers les dimensions supérieures. De fait, la méthode de Schönhage et Strassen présente un aspect frustrant : la racine de l'unité $\omega = 2$ dans R, que nous avons créé artificiellement et à grand frais, est en réalité terriblement « sous-utilisée ». Pour cette raison, notre réduction de longueur $m \rightsquigarrow \sqrt{n}$ n'était que très modeste.

Or il existe aussi des DFTs qui fonctionnent dans plusieurs directions. Supposons à nouveau que R est un anneau arbitraire avec une racine d'unité ω d'ordre l. Une DFT d-dimensionnelle effectue l'isomorphisme

$$\begin{aligned}&R[x_1,\dots,x_d]/(x_1^l-1,\dots,x_d^l-1)\\ &\cong\\ &\prod_{0\leqslant k_1,\dots,k_d<l} R[x_1,\dots,x_d]/(x_1-\omega_1^{k_1},\dots,x_d-\omega_d^{k_d})\end{aligned}$$

Si nous remplaçons maintenant les DFTs en $x_2,\dots,x_d$ par des DFTs à coefficients dans l'anneau $R[x_1]/(x_1^l-1)$, ils coûteront beaucoup moins cher, puisque x_1 est une racine rapide de l'unité dans cet anneau. L'utilisation systématique de ce type de DFTs a d'abord été proposée par Nussbaumer et Quandalle [20].

Cette idée nous permet de faire un grand pas en direction de (5). Si $n = l^d$, alors une multiplication dans $R[x_1,\dots,x_d]/(x_1^l-1,\dots,x_d^l-1)$ nécessite $O(n\log n)$ additions et soustractions dans R plus $n^{(d-1)/d}$ multiplications dans $R[x_1]/(x_1^l-1)$.

Il reste cependant un problème de taille : la multiplication rapide dans $R[x_1,\dots,x_d]/(x_1^l-1,\dots,x_d^l-1)$ n'est pas la même chose que la mul-

tiplication rapide dans $R[x]/(x^{l^d}-1)$. Nous avons donc besoin d'un moyen de transformer des cyclonômes en une variable x en cyclonômes en plusieurs variables $x_1, \ldots, x_d$.

Avec l'aide de la Chine ancienne. Dans certains cas, il est en effet possible de changer de dimension. Supposons que $l_1, \ldots, l_d$ soient premiers entres eux. Selon le théorème des restes chinois, nous avons

$$\mathbb{Z}/(l_1 \cdots l_d)\mathbb{Z} \quad \cong \quad \mathbb{Z}/l_1\mathbb{Z} + \cdots + \mathbb{Z}/l_d\mathbb{Z}.$$

Formellement, ceci donne également

$$x^{\mathbb{Z}/(l_1\cdots l_d)\mathbb{Z}} \quad \cong \quad x_1^{\mathbb{Z}/l_1\mathbb{Z}} \times \cdots \times x_d^{\mathbb{Z}/l_d\mathbb{Z}}.$$

Considérant ensuite des combinaisons linéaires, ceci nous amène enfin à

$$\begin{aligned} &R[x]/(x^{l_1\cdots l_d}-1) \\ &\qquad \cong R[x_1,\ldots,x_d]/(x_1^{l_1}-1,\ldots,x_d^{l_d}-1). \end{aligned}$$

En relation avec les DFTs, cela a été remarqué pour la première fois par Good [7]. Agarwal et Cooley ont ensuite utilisé cet isomorphisme pour calculer des convolutions [1].

Cependant, nous avons maintenant un nouveau problème : dans la section précédente nous avions besoin d'un isomorphisme pour lequel tous les l_i étaient égaux. Mais notre isomorphisme ne marche que dans le cas où $l_1, \ldots, l_d$ sont au contraire premiers entre eux...

Le dernier ingrédient qui nous manque est un moyen de modifier légèrement la longueur d'une DFT. Cela permettrait de réduire une DFT d-dimensionnelle de longueur $(l_1, \ldots, l_d)$ en une autre de longueur $(l, \ldots, l)$. En utilisant une version d-dimensionnelle de l'algorithme de Bluestein, une telle DFT se réduit ensuite à une multiplication dans $R[x_1, \ldots, x_d]/(x_1^l - 1, \ldots, x_d^l - 1)$. Et cela peut être fait efficacement à l'aide des racines rapides de l'unité.

Rééchantillonnage gaussien. Comment remplacer une DFT de longueur s par une DFT de longueur t légèrement supérieure ? Pour y parvenir, nous supposons à partir de maintenant que $R = \mathbb{C}$.

Considérons une DFT de longueur s. Dans la théorie du signal, l'entrée est vue comme une série d'échantillons d'un signal. La fréquence d'échantillonnage est proportionnelle à s. Est-il possible de reconstruire le signal original à partir de notre ensemble d'échantillons ? Cela permettrait de prendre un nouvel ensemble d'échantillons, avec une fréquence différente.

La manière la plus évidente de rendre un signal numérique analogique est par convolution avec une gaussienne $G_\alpha(x) = \mathrm{e}^{-\alpha x^2}$. Plus α est petit, plus le signal analogique est lisse (mais moins net). Une propriété utile est que la transformée de Fourier de G_α est à nouveau une gaussienne.

Traduisons ces idées en formules. Au lieu de cyclonômes de degré s, nous considérons maintenant leurs vecteurs associés $u \in \mathbb{C}^s$ de coefficients. Nous convenons que $u_{k+js} \equiv u_k$ pour tout $j \in \mathbb{Z}$. Étant donné $u \in \mathbb{C}^s$, on définit $\mathcal{F}_s(u) \in \mathbb{C}^s$ par

$$(\mathcal{F}_s u)_k \quad := \quad \sum_{0 \leqslant k < s} u_k \mathrm{e}^{-2\pi \mathrm{i} \frac{jk}{s}}.$$

Ceci est une variante de notre définition précédente d'une DFT (ici $\omega = \mathrm{e}^{-2\pi\mathrm{i}/s}$). Puis on définit deux applications linéaires $\mathcal{S}, \mathcal{T} : \mathbb{C}^s \to \mathbb{C}^t$ par

$$\begin{aligned} (\mathcal{S}u)_k &:= \alpha^{-1} \sum_{j\in\mathbb{Z}} \mathrm{e}^{-\pi\alpha^{-2}s^2(\frac{k}{t}-\frac{j}{s})^2} u_j \\ (\mathcal{T}u)_k &:= \sum_{j\in\mathbb{Z}} \mathrm{e}^{-\pi\alpha^2 t^2(\frac{k}{t}-\frac{j}{s})^2} u_j. \end{aligned}$$

Enfin, nous introduisons deux permutations $\mathcal{P}_s : \mathbb{C}^s \to \mathbb{C}^s$ et $\mathcal{P}_t : \mathbb{C}^t \to \mathbb{C}^t$ par

$$\begin{aligned} (\mathcal{P}_s u)_j &:= u_{tj} \\ (\mathcal{P}_t u)_k &:= u_{-sk}. \end{aligned}$$

Dans [12, Theorem 4.2] nous montrons que le diagramme suivant commute :

$$\begin{array}{ccccc} \mathbb{C}^s & \xrightarrow{\mathcal{F}_s} & \mathbb{C}^s & \xrightarrow{\mathcal{P}_s} & \mathbb{C}^s \\ \mathcal{S}\downarrow & & & & \downarrow\mathcal{T} \\ \mathbb{C}^t & \xrightarrow{\mathcal{F}_t} & \mathbb{C}^t & \xrightarrow{\mathcal{P}_t} & \mathbb{C}^t \end{array}$$

C'est ce que nous utilisons pour réduire le calcul de $\mathcal{F}_s$ au calcul de $\mathcal{F}_t$.

Puisque $t > s$, les matrices de $\mathcal{S}$ et $\mathcal{T}$ ne sont pas carrées. Par construction, les éléments qui ne sont pas sur la diagonale diminuent rapidement. En effet, les gaussiennent déclinent à la vitesse de l'éclair loin du centre. En supprimant $t-s$ des lignes bien choisies de $\mathcal{T}$, il reste une matrice presque diagonale. Ceci peut être utilisé pour calculer rapidement $\mathcal{T}^{-1}\mathcal{P}_t\mathcal{F}_t\mathcal{S}$.

Si l'on choisit α et la précision de calcul avec

précaution, on montre que $\mathcal{F}_s$ peut être calculé ainsi avec presque autant de précision que $\mathcal{F}_t$ et que le temps de calcul de $\mathcal{S}$ et de $\mathcal{T}^{-1}$ est négligeable par rapport à celui de $\mathcal{F}_t$.

Ceci parachève notre méthode et la démonstration que $\mathsf{M}(n) = O(n \log n)$. La figure 4 récapitule toutes les réductions que nous avons utilisées.

Une variante de notre méthode de rééchantillonnage fut publiée pour la première fois par Dutt et Rokhlin [4]. Cette variante est plus générale et permet de calculer des DFT quand échantillons des signaux sont irréguliers. En revanche, leur méthode ne fonctionne que pour $\log s = O(\alpha)$; de ce fait, elle est juste un peu trop lente pour notre application.

Et les applications ? D'un point de vue pratique, nous verrons… Mais la fonction $\mathsf{M}(n)$ est importante pour la théorie, afin de décrire avec précision les coûts de toutes sortes d'opérations arithmétiques. Ainsi la division de deux entiers de $\leqslant n$ chiffres prend $O\left(\mathsf{M}(n)\right) = O(n \log n)$ opérations et le calcul d'un pgcd en prend $O\left(\mathsf{M}(n) \log n\right) = O(n \log^2 n)$. Désormais, on sait calculer n chiffres de π en temps $O\left(\mathsf{M}(n) \log n\right) = O(n \log^2 n)$. Une DFT complexe de longueur l nécessite $O\left(\mathsf{M}(lp)\right)$ opérations, si on calcule avec $p \geqslant \log l$ chiffres derrière la virgule [13]. Cela détermine également les émissions minimales de CO_2 pour des gros calculs sur le rechauffement climatique. D'une certaine manière, la fonction $\mathsf{M}(n)$ comme « vitesse de l'arithmétique élémentaire » joue donc un rôle similaire à la vitesse de la lumière c en physique.

Existe-t-il des algorithmes plus rapides ? Nous l'ignorons !

Références

[1] R. Agarwal et J. Cooley. New algorithms for digital convolution. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 25(5) :392–410, 1977.

[2] Leo I. Bluestein. A linear filtering approach to the computation of discrete Fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 18(4) :451–455, 1970.

[3] J. W. Cooley et J. W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Math. Computat.*, 19 :297–301, 1965.

[4] A. Dutt et V. Rokhlin. Fast Fourier transforms for nonequispaced data. *SIAM J. Sci. Comput.*, 14(6) :1368–1393, 1993.

[5] M. Fürer. Faster integer multiplication. Dans *Proceedings of the Thirty-Ninth ACM Symposium on Theory of Computing (STOC 2007)*, pages 57–66. San Diego, California, 2007.

[6] C. F. Gauss. Nachlass : theoria interpolationis methodo nova tractata. Dans *Werke*, volume 3, pages 265–330. Königliche Gesellschaft der Wissenschaften, Göttingen, 1866.

[7] I. J. Good. The interaction algorithm and practical Fourier analysis. *Journal of the Royal Statistical Society*, Series B. 20(2) :361–372, 1958.

[8] D. Harvey. Faster arithmetic for number-theoretic transforms. *J. Symbolic Comput.*, 60 :113–119, 2014.

[9] D. Harvey. Faster truncated integer multiplication. `https://arxiv.org/abs/1703.00640`, 2017.

[10] D. Harvey et J. van der Hoeven. Faster integer and polynomial multiplication using cyclotomic coefficient rings. Technical Report, ArXiv, 2017. `http://arxiv.org/abs/1712.03693`.

[11] D. Harvey et J. van der Hoeven. Faster integer multiplication using short lattice vectors. Dans R. Scheidler et J. Sorenson, éditeurs, *Proc. of the 13-th Algorithmic Number Theory Symposium*, Open Book Series 2, pages 293–310. Mathematical Sciences Publishes, Berkeley, 2019.

[12] D. Harvey et J. van der Hoeven. Integer multiplication in time $O(n \log n)$. Technical Report, HAL, 2019. `http://hal.archives-ouvertes.fr/hal-02070778`, accepted for publication in Annals of Math.

[13] D. Harvey, J. van der Hoeven, et G. Lecerf. Even faster integer multiplication. *Journal of Complexity*, 36 :1–30, 2016.

[14] M. T. Heideman, D. H. Johnson, et C. S. Burrus. Gauss and the history of the FFT. *IEEE Acoustics, Speech and Signal Processing Magazine*, 1 :14–21, oct 1984.

[15] J. van der Hoeven. Getallen vermenigvuldigen in $O(n \log n)$ stappen. *Nieuw Archief voor Wiskunde*, 21(1) :55–60, 2020. Vijfde serie.

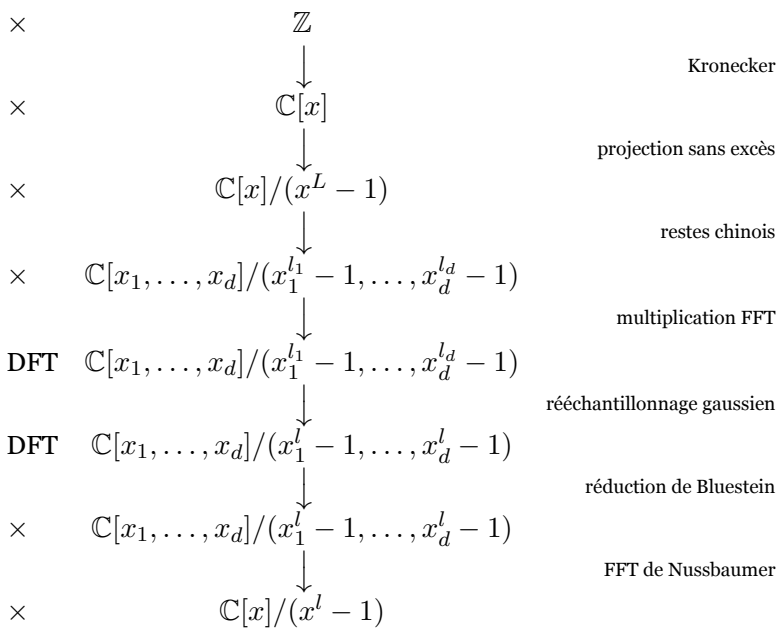


Figure 4 – Représentation schématique des différentes réductions dans le nouvel algorithme. Nous avons triché un peu ici et là pour faire simple.

[17] A. A. Karatsuba. The complexity of computations. *Proc. of the Steklov Inst. of Math.*, 211 :169–183, 1995. English translation ; Russian original at pages 186–202.

[18] A. Karatsuba et J. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Doklady*, 7 :595–596, 1963.

[19] D. E. Knuth. *The Art of Computer Programming*, volume 2 : Seminumerical Algorithms. Addison-Wesley, 1969.

[20] H. J. Nussbaumer et P. Quandalle. Computation of convolutions and discrete Fourier transforms by polynomial transforms. *IBM J. Res. Develop.*, 22(2) :134–144, 1978.

[21] J. M. Pollard. The fast Fourier transform in a finite field. *Mathematics of Computation*, 25(114) :365–374, 1971.

[22] A. Schönhage. Multiplikation großer Zahlen. *Computing*, 1(3) :182–196, 1966.

[23] A. Schönhage et V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7 :281–292, 1971.

[24] A. L. Toom. The complexity of a scheme of functional elements realizing the multiplication of integers. *Soviet Mathematics*, 4(2) :714–716, 1963.