Université Paris 8 Année 2023–2024

Master Mathématiques et applications

Algorithmes arithmétiques II — Présentations d'algorithmes

4 novembre 2023

Choix du sujet. Envoyer par email, jusqu'au lundi 13 novembre 2023, à l'adresse suivante :

`julien.lavauzelle@univ-paris8.fr`

une liste ordonnée des 5 numéros de sujets que vous préférez traiter. L'un de ces sujets vous sera ensuite attribué. Sans réponse de votre part, un sujet aléatoire sera attribué.

Si vous souhaitez traiter un autre sujet en lien avec l'algorithmique et l'arithmétique, veuillez m'envoyer un **autre** email avec une description du sujet en quelques lignes et des références, pour que je le valide (ou non).

Format de l'évaluation. L'évaluation consiste en un oral de présentation d'un algorithme avancé. L'**objectif** est de présenter cet algorithme à vos camarades étudiants ; vous devez donc le rendre accessible à un niveau M2. La présentation durera 15 minutes maximum, et vous aurez à répondre à une ou deux questions supplémentaires. Vous aurez le droit d'utiliser un support visuel (slides), impérativement au format `.pdf`, à m'envoyer par email au plus tard **la veille** de votre évaluation.

Consignes pour tous les sujets. Vous devez articuler votre présentation selon trois axes :

1. **Définition du problème** à résoudre et de ses enjeux (grandeurs d'intérêt, hypothèses sur les entrées et les sorties, etc.)
2. **Présentation du/des algorithme/s**, la plus accessible possible. Donner un exemple si nécessaire.
3. **Analyse et mise en perspective** de l'algorithme. Par exemple : quelle est sa complexité ? Comment se compare t-il avec ce qui existe ? Quelles sont ses spécificités ?

Barème.

- 4 points pour chaque axe
- 4 points pour la clarté/qualité des supports
- 4 points pour la réponse à la question finale et la clarté de la présentation à l'oral

Indications/autonomie. Dans la liste de sujets ci-dessous, vous trouverez :

(i) Un **titre** décrivant le sujet exact à traiter. Il est **obligatoire** de traiter précisément ce sujet.
(ii) Quelques **questions** spécifiques que vous **pouvez** traiter, ou des **conseils** pour vous aider à comprendre/présenter l'algorithme.
(iii) Des **références**, en anglais ou en français, vers lequelles vous tourner pour appréhender le sujet. **Vous pouvez en choisir d'autres** (c'est même conseillé). Dans tous les cas, **donnez en fin de présentation les références** que vous avez utilisées.

Table des matières

1 Algorithme de décodage en liste de codes de Reed–Solomon

Conseils / questions spécifiques.

— Traiter l'algorithme de Sudan qui permet de décoder au-delà du rayon de décodage unique.
— Lien avec l'algorithme de Berlekamp–Welch.
— Limites théoriques (borne de Johnson, ...).

Références.

— Notes de cours de V. Guruswami, disponibles `[ici]` et `[là]`
— La section 4.3 du rapport *Les codes algébriques principaux et leur décodage*, D. Augot, `https://hal.inria.fr/inria-00543322/document`

2 Algorithme d'évaluation multi-points par arbre de restes et de produits

Conseils / questions spécifiques.

— Il est important de bien définir la complexité de la multiplication entre coefficients.
— Traiter le cas de polynômes univariés, puis éventuellement celui des polynômes multivariés.

Références.

— *Algorithmes Efficaces en Calcul Formel*, `https://hal.archives-ouvertes.fr/AECF`, section 5.4.
— Chapitre 10 de *Modern computer algebra, 3rd ed.*, J. von zur Gathen et J. Gerhard (demandez-moi si besoin).
— Ellis Horowitz, 1972. *A fast method for interpolation using preconditioning.*, Inf. Proc. Letters 1 (4), 157–163. `https://www.sciencedirect.com/science/article/abs/pii/0020019072900506`
— Borodin, A., Moenck, R. T., 1974. *Fast modular transforms.* J. Comput. Syst. Sci. 8 (3), 366–386. `https://www.sciencedirect.com/science/article/pii/S0022000074800292`

3 Interpolation de Hermite

Conseils / questions spécifiques.

— Bien expliquer la différence entre interpolations de Lagrange et de Hermite.
— Donner l'algorithme d'interpolation "directe", puis éventuellement par "changement de base".
— Traiter le cas des polynômes bivariés, voire multivariés.

Références.

— Francis Y. Chin, *A generalized asymptotic upper bound on fast polynomial evaluation and interpolation*, SIAM J. Comput. 5 (1976), no. 4, 682–690.
— Chapitre 5 de *Modern computer algebra, 3rd ed.*, J. von zur Gathen et J. Gerhard (demandez-moi si besoin).

4 Construction explicite d'extensions de corps finis

Conseils / questions spécifiques.

— Étant donné un corps fini $\mathbb{F}_q$ et un entier $m \geq 2$, décrire ce dont on a besoin pour construire $\mathbb{F}_q^m$ explicitement.
— Vous aurez besoin de test d'irréductibilité et de construire des polynômes irréductibles : donnez les algorithmes (ex : algorithme de Ben'Or)).
— Mentionnez rapidement la complexité des opérations élémentaires ($+$, $\times$, inverse) dans $\mathbb{F}_q^m$, en fonction de celle dans $\mathbb{F}_q$.

Références.

— Shuhong Gao et Daniel Panario, *Tests and Constructions of Irreducible Polynomials over Finite Fields*, Foundations of Computational Mathematics, `[ici]`
— Chapitre 14.9 de *Modern computer algebra, 3rd ed.*, J. von zur Gathen et J. Gerhard (demandez-moi si besoin).

5 Algorithme de Strassen pour la multiplication de matrices

Conseils / questions spécifiques.

— Faire le lien avec l'algorithme de Karatsuba.
— Faire une analyse de complexité précise.

Références.

— *Algorithmes Efficaces en Calcul Formel*, `https://hal.archives-ouvertes.fr/AECF`, section 8.2.
— Section 4.2, *Introduction to Algorithms, 3rd ed.*, T. Cormen, C. Leiserson, R. Rivest, C. Stein, disponible en ligne `[ici]`

6 Algorithme de Cornacchia

Conseils / questions spécifiques.

— Bien définir le problème.
— Applications ?

Références.

— *L'algorithme de Cornacchia*, A. Nitaj, `https://nitaj.users.lmno.cnrs.fr/cornacchia.ps`
— *On Cornacchia's algorithm for solving the diophantine equation* $u^2 + dv^2 = m$, F. Morain, J.-L. Nicolas, `http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/cornac.pdf`

7 Algèbre linéaire rapide pour des matrices structurées

Conseils / questions spécifiques.

- On pourra traiter le cas des matrices de Toeplitz, des matrices circulantes, des matrices de Vandermonde, etc. (au choix)
- But : algorithmes plus rapides que le cas de matrices génériques pour :
  - La création / le stockage de matrices
  - La multiplication matrice/vecteur matrice/matrice
  - L'inverse matriciel
  - La résolution de systèmes linéaires
- Chercher et donner des applications.

Références.

- *Matric computations, 4th ed.*, Chapitre 4, G.H. Golub, C.F. Van Loan
- *Matrix structures and applications*, D.A. Bini, note de cours pour les JNCF, `[ici]`

8 Multiplication rapide par l'algorithme de Schönhage–Strassen

Conseils / questions spécifiques.

- Faire le lien entre polynômes et entiers.
- FFT classique : quelle(s) contrainte(s) arithmétique(s) ?
- Préciser l'apport de Schönhage–Strassen.

Références.

- *Algorithmes Efficaces en Calcul Formel*, `https://hal.archives-ouvertes.fr/AECF`, section 2.4 et 2.5.
- Notes de cours [ici]

9 La méthode ECM de Lenstra pour la factorisation d'entiers

Conseils / questions spécifiques.

- Faire l'analogie avec la méthode $p - 1$.
- Donner une version simple avant de discuter d'optimisations.

Références.

- H. Lenstra, *Factoring integers with Elliptic Curves*, `https://wstein.org/edu/Fall2001/124/lenstra/lenstra.pdf`
- Notes de cours `[ici]` + introduction du manuscrit de thèse [lien] de C. Bouvier (par exemple)

10 Factorisation d'entiers par fractions continues

Conseils / questions spécifiques.

— Bien rappeler les résultats théoriques sur les fractions continues.
— Lien avec les équations de Pell.

Références.

— *On factoring large numbers*, D. Lehmer, R. Powers, `https://www.ams.org/journals/bull/1931-37-10/S0002-9904-1931-05271-X/`
— *A method of factoring and the factorization of F_7*, M. Morrison, J. Brillhart, `https://www.ams.org/journals/mcom/1975-29-129/S0025-5718-1975-0371800-5`

11 Test de primalité de Lucas–Lehmer pour les nombres de Mersenne

Conseils / questions spécifiques.

— Préciser les hypothèses sur les entiers dont on teste la primalité.
— Donner une analyse théorique.

Références.

— Notes de cours 1, section 6 : `[ici]`
— Notes de cours 2 : `[là]`

12 Certificats de primalité grâce aux courbes elliptiques

Conseils / questions spécifiques.

— Expliquer ce qu'est un certificat de primalité, avec par exemple le ceryificat de Pratt.
— Traiter l'algorithme de Goldwasser–Kilian (en supposant que l'on ait à disposition une méthode pour le comptage de points d'une courbe elliptique).
— Mentionner les améliorations evéntuelles (Atkin–Morain par exemple).

Références.

— Pratt, *Every prime has a succinct certificate*, SIAM Journal on Computing, vol. 4, pp. 214–220, 1975. `http://boole.stanford.edu/pub/SucCert.pdf`
— Goldwasser, Kilian, *Almost All Primes Can Be Quickly Certified*, Proc. 18th STOC. pp. 316–329, 1986 `http://groups.csail.mit.edu/cis/pubs/shafi/1986-stoc-gk.pdf`
— Atkin, Morain,, *Elliptic Curves and Primality Proving*, Mathematics of Computation. 61 (203) : 29–68, 1993. `https://www.ams.org/journals/mcom/1993-61-203/S0025-5718-1993-1199989-X`

13 Crible d'Atkin

Conseils / questions spécifiques.

— Comparer au crible d'Eratosthene.
— Discuter des techniques d'optimisation/implantation.

Références.

— *Prime sieves using binary quadratic forms*, A. Atkin, D. Bernstein, `https://www.ams.org/journals/mcom/2004-73-246/S0025-5718-03-01501-1`

14 Algorithmes rapides pour le calcul de PGCD et de demi-PGCD

Conseils / questions spécifiques.

— Ne pas s'arrêter au « pgcd binaire » : voir par exemples les algorithmes de Knuth ou de Schönhage.
— Bien définir la notion de demi-pgcd.
— Travailler sur les entiers et/ou les polynômes (à préciser).

Références.

— *Euclid's Algorithm for Large Numbers*, D. Lehmer
— *On Schönhage algorithm and subquadratic integer gcd computation*, N. Möller, `https://www.ams.org/journals/mcom/2008-77-261/S0025-5718-07-02017-0/S0025-5718-07-02017-0.pdf`
— *Algorithmes Efficaces en Calcul Formel*, `https://hal.archives-ouvertes.fr/AECF`, section 6.3.

15 Algorithme de Schoof pour le calcul de l'ordre d'une courbe elliptique

Conseils / questions spécifiques.

— Attention à ne pas faire que de la théorie
— Applications ?

Références.

— *Elliptic curves over finite fields and the computation of square roots mod p*, R. Schoof.
— *Counting points on elliptic curves over finite fields*, R. Schoof, `https://jtnb.centre-mersenne.org/item/10.5802/jtnb.142.pdf`
— Notes de cours : `[ici]`

16 Calcul de racines cubiques dans $\mathbb{F}_q$: algorithme de Pocklington–Padró–Sáez

Conseils / questions spécifiques.

— Lien avec les algorithmes d'extraction de racines carrées vus en cours.
— Généralisation à $\sqrt[m]{\cdot}$?

Références.

— C. Padró, G. Sáez, *Taking cube roots in $\mathbb{Z}_m$*, `https://www.sciencedirect.com/science/article/pii/S0893965902000319`

17 Multiplication modulaire par l'algorithme de Montgomery

Conseils / questions spécifiques.

— Dans quel contexte applicatif cet algorithme est-il utile ?
— Analyse précise de complexité et de validité.

Références.

— P. Montgomery, *Modular Multiplication Without Trial Division*, `https://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777282-X/`
— Section 14.3.2 de *Handbook of Applied Cryptography*, A. Menezes, P. van Oorschot, and S. Vanstone, `https://cacr.uwaterloo.ca/hac/about/chap14.pdf`

18 Algorithme de Buchberger pour la réduction de bases de Gröbner

Conseils / questions spécifiques.

— Prendre garde à bien définir le problème.
— Terminaison de l'algorithme ?

Références.

— *An Algorithmic Criterion for the Solvability of a System of Algebraic Equations*, B. Buchberger.
— *Algorithmes Efficaces en Calcul Formel*, `https://hal.archives-ouvertes.fr/AECF`, section 24 (particulièrement 24.2).
— Chapitre 1 (particulièrement section 1.7) de *An Introduction to Gröbner bases*, W. Adams, Ph. Loustaunau.