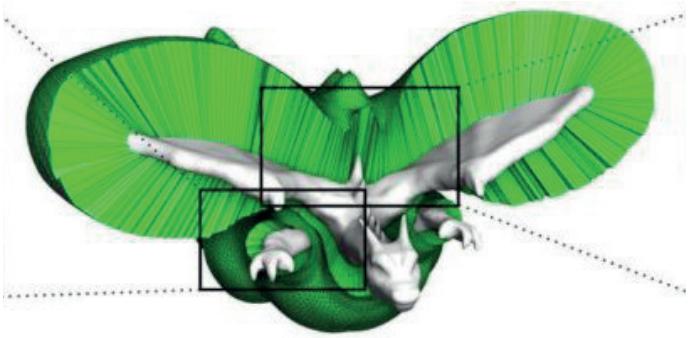
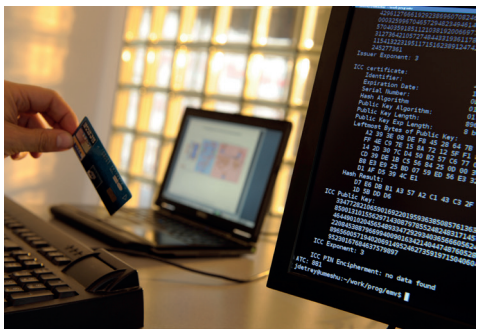
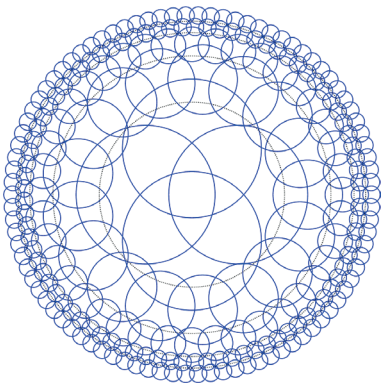
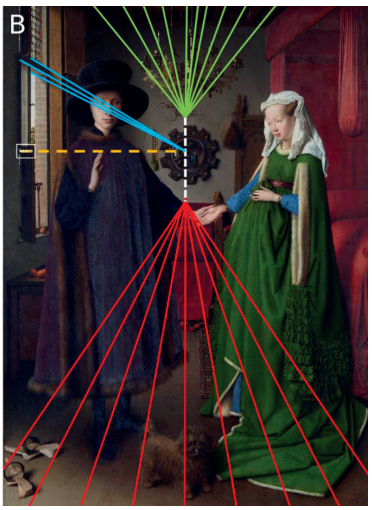
PORTFOLIO
DEPARTMENT 1

Algorithms, Computation, Geometry and Image









Loria cnrs Inria UNIVERSITÉ DE LORRAINE

En partenariat avec :
CentraleSupélec

Portfolio Département 1

Nous présentons dans le portfolio du département 1 “Algorithmique, calcul, image et géométrie” les 7 éléments suivants.

Rapport détaillé. L’Université de Lorraine a demandé aux laboratoires de rédiger pour juin 2021 les bilans des laboratoires en vue de l’évaluation HCERES 2016-2020, ceci sans attendre les recommandations de l’HCERES. Nous avons donc rédigé un rapport complet (en anglais), structuré sur la base des anciennes évaluations de l’HCERES. Ce rapport contient une première partie qui présente une vision générale du département et de ses réalisations, suivi d’un rapport détaillé pour chacune des équipes au sein du département. Nous avons naturellement réutilisé pour le DAE une partie substentielle de la première partie, ce qui explique la présence de parties en anglais et en francais dans le DAE. Nous présentons ce rapport complet dans le portfolio.

Nous présentons les six autres éléments suivants du portfolio dans la suite de ce document.

- **Jan Van Eyck’s Perspectival System Elucidated Through Computer Vision.** Article publié à SIGGRAPH 2021.
- **Invertible maps.** Article publié à SIGGRAPH 2021.
- **Roots approximation of univariate polynomials.** Article publié à FOCS 2021 et sujet d’un transfert avec la société MapleSoft.
- **Logarithme discret, factorisation d’entiers, et logiciel CADO-NFS.** Article publié à Asiacrypt 2021, best paper, prix de Thèse Gilles Kahn, Prix L’Oréal-UNESCO, et logiciel CADO-NFS.
- **Digital filtering for geometric analysis.** Article publié à DGMM 2021, prix du meilleur article étudiant.
- **IceSL software: modeling and slicing for Additive Manufacturing.**

Notons enfin que nous présentons également un zoom sur le **vote electronique et logiciel Belenios**, travail commun aux départements 1 et 2, dans le portfolio du laboratoire.

Jan Van Eyck's Perspectival System Elucidated Through Computer Vision

Équipe Tangram

Figure 1: Jan van Eyck, Les Époux Arnolfini, 1434, huile sur panneau de chêne, 82,2 $\times$ 60 cm, National Gallery, Londres.

Lorsqu'on regarde un tableau du peintre flamand Jan van Eyck (1390-1441) on a presque l'impression de voir une photographie (Fig. 1). La représentation de l'espace est particulièrement convaincante et l'on pourrait penser que le peintre maîtrisait parfaitement les règles de la perspective, découvertes quelques années plus tôt en Italie. Pourtant, si l'on intersecte les traits supposés représenter des lignes droites de la scène perpendiculaires au plan du tableau, nous n'obtenons pas un unique point de fuite comme cela devrait être le cas, mais plusieurs points de convergence en apparence désordonnés. Des historiens de l'art ont essayé de regrouper les traits de différentes manières – les travaux les plus anciens remontent à 1905 [1] – obtenant des configurations particulières de points de fuite, mais aucune configuration suggérée ne se répète d'un tableau à l'autre. Finalement, l'hypothèse la plus acceptable jusqu'à aujourd'hui était que le peintre ne possédait pas de connaissance en matière de perspective et représentait l'espace en essayant de restituer au mieux ce qu'il pouvait observer.

Les études de perspective menées par les historiens de l'art souffrent malheureusement d'un manque d'objectivité et ne tiennent pas compte de l'imprécision inhérente au tracé ou à la délinéation des traits. Les méthodes de détection a contrario reposent sur un critère probabiliste, appelé Nombre de Fausses Alarmes (NFA), qui permet de prouver qu'un événement tel que la rencontre d'un certain nombre de lignes dans un carré d'une certaine taille ne peut pas être le fruit du hasard (NFA < 1). Ce critère a été exploité par l'équipe TANGRAM pour détecter automatiquement des points de fuite dans une photographie [2]. En calculant la valeur du NFA sur des cartes de probabilité de points de fuite (Fig. 2 – gauche), nous obtenons, dans cinq tableaux de Jan van Eyck, que les regroupements dont le NFA est inférieur à 1 définissent des points de fuite parfaitement ordonnés, c'est-à-dire alignés et équidistants le long d'un axe vertical légèrement incliné

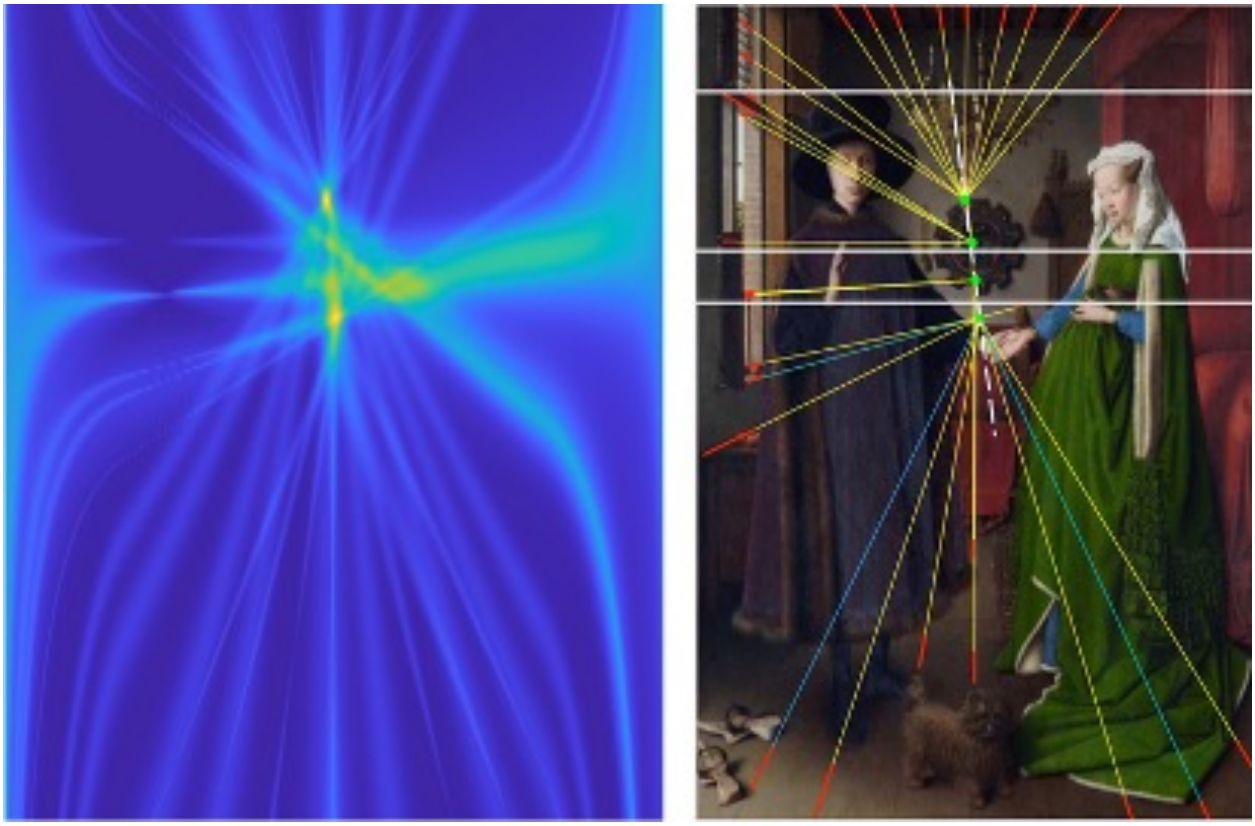


Figure 2: Application de la méthode a contrario au portrait des Arnolfini. À gauche : carte de probabilité des points de fuite tenant compte d'une incertitude sur les extrémités des arêtes extraites (visibles en rouge dans l'image de droite). À droite : application de la méthode a contrario à cette carte de probabilités. Les arêtes extraites sont reliées au point de fuite correspondant, la couleur du lien traduisant sa consistance : du bleu foncé au jaune clair pour une consistance allant respectivement de 0 à 1. Les arêtes se regroupent par bandes horizontales, délimitées ici par des lignes blanches.

(Fig. 2 – droite) [3]. Cet ordre lui-même ne peut être le fruit du hasard, tout comme ne peut l'être l'effet de parallaxe mesurable entre différentes bandes des tableaux examinés.

Cela démontre que le peintre utilisait un dispositif optique polyscopique (également appelé " machine à perspective") pour réaliser ses dessins préparatoires. Il dessinait la réalité bande par bande à travers une vitre, avec une encre carbone qu'il transférait ensuite sur le panneau à peindre. Chaque bande correspond à une hauteur différente de visée, la vitre étant déplacée verticalement en cours d'exécution. L'inclinaison de l'axe de visée introduit un écart horizontal entre le point de vue le plus bas et celui le plus haut égal à l'écart interpupillaire moyen d'un homme adulte. En représentant les objets de face quelle que soit leur hauteur, et en réalisant une sorte de " fondu" entre la vue de l'œil droit et celle de l'œil gauche, le peintre semble avoir voulu représenter l'espace au plus près de la vision humaine.

Cette découverte est importante pour l'histoire de l'art mais également pour l'histoire des sciences, la machine à perspective de Jan van Eyck étant la plus ancienne répertoriée à ce jour – Léonard de Vinci dessinera un dispositif plus simple près d'un demi-siècle plus tard. Elle a fait l'objet d'une publication à SIGGRAPH 2021 [3] (transmis dans les fichiers du portfolio). Des articles de presse lui ont été consacrés dans les magazines papier Pour la Science [4] et Sciences et Avenir [5], ainsi que des reportages télévisés réalisés pour France 3 [6] et la télévision publique allemande SR [7]. Elle fut également mentionnée sur

France Culture par l'historien Ludovic Balavoine, spécialiste de Jan van Eyck, dans le programme radiophonique intitulé "Sans oser le demander" [8]. Une vidéo adressée au grand public est diffusée sur la chaîne YouTube du Loria [9], et un article de vulgarisation a été édité (en français et en anglais) par la revue en ligne The Conversation (40854 lecteurs au 8/3/2022) [10], dont une version augmentée est disponible sur le site de la revue Interstices [11].

References

[1] Karl Doehlemann. Die perspektive der brüder van Eyck. *Zeitschrift für Mathematik und Physik, LII, 419*, 1905.

[2] Gilles Simon, Antoine Fond, and Marie-Odile Berger. A-Contrario Horizon-First Vanishing Point Detection Using Second-Order Grouping Laws. In *ECCV 2018 - European Conference on Computer Vision*, pages 323–338, Munich, Germany, September 2018. https://hal.inria.fr/hal-01865251/file/1988.pdf.

[3] Gilles Simon. Jan Van Eyck's Perspectival System Elucidated Through Computer Vision. *Proceedings of the ACM on Computer Graphics and Interactive Techniques (SIGGRAPH 2021)*, 4(2), July 2021. https://hal.univ-lorraine.fr/hal-03287031.

[4] L. Mangin. La perspective, une invention flamande ? *Pour la Science*, 528, 2021.

[5] A. Devillard. Van Eyck, maître des points de fuite. *Sciences et Avenir*, 896, 2021.

[6] M. Boudiba. Science : la perspective dans les tableaux de Jan Van Eyck, une énigme élucidée. *Reportage. France 3*, 2021. https://youtu.be/Ejl-FuFhSUM.

[7] D. Differdange. Versteckt: Informatiker aus Nancy entschlüsselt Van Eyck-Code. *SR*, 2022. https://www.ardmediathek.de/video/wir-im-saarland-grenzenlos/versteckt-informatiker-aus-nancy-entschluesselt-van-eyck-code/sr/Y3JpZDovL3NyLW9ubGluZS5kZS9HTC1XSU1TXzExMTkxOQ.

[8] R. de Becdelièvre. Que nous révèle l'Agneau mystique de Van Eyck ? *Sans oser le demander (min. 45:25-50:00), France Culture*, 2021. https://www.franceculture.fr/emissions/sans-oser-le-demander/que-nous-revele-l-agneau-mystique-de-van-eyck.

[9] M. Diaz Ramirez and M. Baron. La perspective chez Jan van Eyck au carrefour entre informatique et histoire de l'art. *LORIA*, 2021. https://www.youtube.com/watch?v=L0SBR3lcHc4.

[10] G. Simon. La véritable invention de Jan van Eyck : une machine à représenter l'espace tel que nous le percevons. *The Conversation*, 2021. https://theconversation.com/la-veritable-invention-de-jan-van-eyck-une-machine-a-representer-lespace-tel-que-nous-le-percevons-165685.

[11] G. Simon. La machine à perspective de Jan van Eyck. *Interstices*. https://interstices.info/la-machine-a-perspective-de-jan-van-eyck/.

Invertible maps

Pixel Team

Mapping a 3D surface to 2D space (or a solid domain to 3D space) is one of the most important problems in geometry processing, because it is much easier for many applications to work in the map than to directly manipulate the object itself. Historically, maps were introduced to represent the surface of the Earth. Mathematically speaking, to compute a map of the Earth, we need to cut a sphere to obtain topological disc(s), and then deform it to make a flattening (Figure 3–top). At the end, the most fundamental property we have to ensure is the invertibility of the map, and the importance of this property cannot be overstated. The very idea of computing a map is being able to go back and forth between the object itself and its image without any ambiguity.

The most versatile way to represent geometric objects inside a computer is to discretize them. An object can be approximated by a number of primitives such as polygons in 2D and polyhedra in 3D. Figure 3–bottom shows a discrete map of the Earth made with office supplies (rubber bands and push pins). First of all, we approximate a sphere by a polygonal surface (here by a dodecahedron), then we cut it into two topological discs. Finally, we represent each edge by an elastic band; we pin the boundary of the surface to flatten, and the stable position of the mesh inside provides a discrete map.

In fact, this procedure corresponds exactly to a method proposed by Tutte in 1963 in his famous paper "How to draw a graph" [1]. For several decades, Tutte embedding remained the only way with theoretical guarantees of success: if we pin the boundary vertices to lie on a convex polygon, we are guaranteed to obtain an invertible map (free of folds). Unfortunately, there are severe limitations for Tutte embeddings. First of all, if the boundary is constrained to a non-convex polygon, folds may be present (Jacobian determinant of the map is not everywhere positive). Figure 4–left provides an illustration. This map contains foldovers, and thus is not invertible, there are points in the map with two distinct pre-images. In addition to that, Tutte

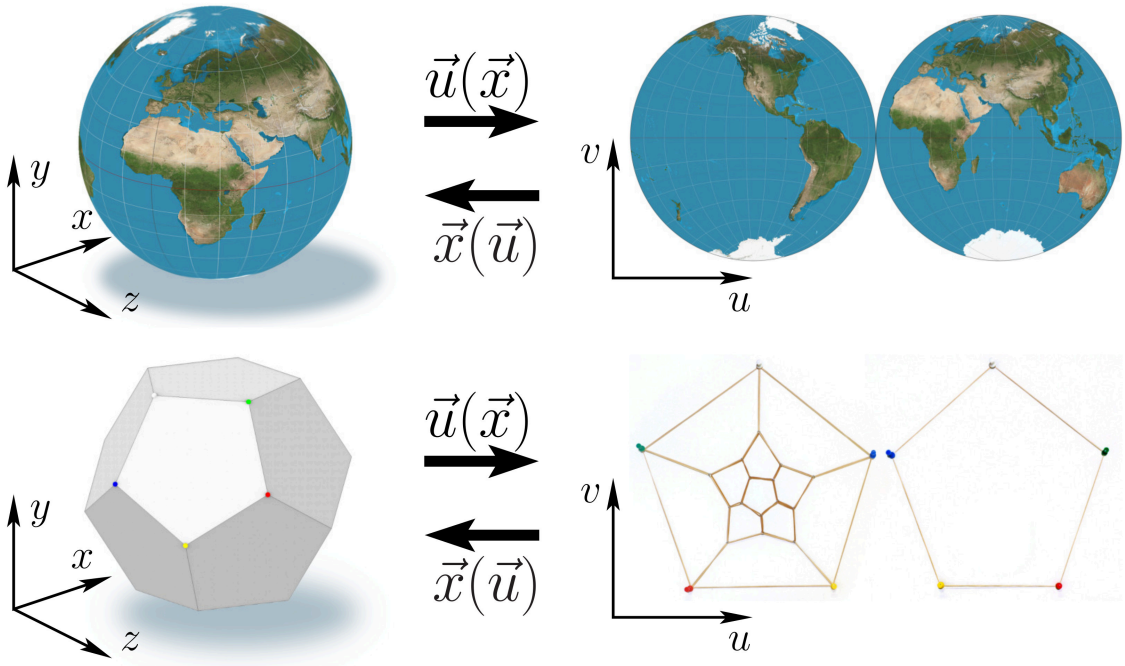


Figure 3: Top row: a map of the Earth by Nicolosi globular projection. Bottom row: a discrete map of the Earth via Tutte embedding made with office supplies (rubber bands and push pins).

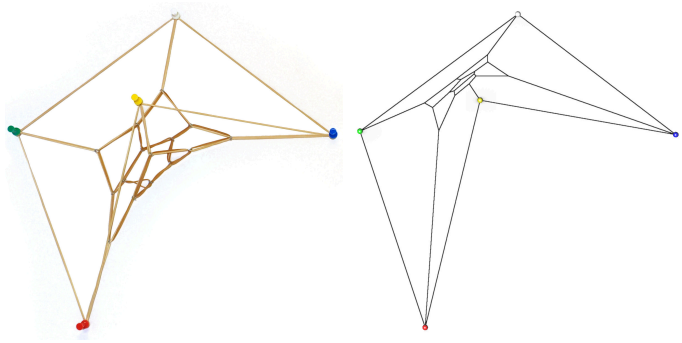


Figure 4: Tutte embedding may produce foldovers if the boundary is constrained to a non-convex polygon (left), while our untangling procedure is guaranteed to produce valid results (right).

(a) (b)

Figure 5: Tetrahedral mesh deformation, locked vertices are shown in red. (a): Shape, (b): our untangling result.

embedding does not apply to free boundary deformations nor to 3D deformations, it only works for planar meshes with boundary constrained to a convex polygon.

Almost 60 years later, we made a breakthrough [2]. We proposed the first mapping method free of the limitations of Tutte embeddings, but still with theoretical guarantees of success. Our method supports both constrained as well as free boundary mapping, and is also suitable to solid domains. The idea behind is very simple: first deform the mesh subject to necessary constraints (planarity, position of vertices etc.), ignoring eventual folds in the map. In this way we obtain a *tangled* mesh, a mesh with inverted elements. We have already seen an example of a tangled mesh in left image of Figure 4. Then, we *untangle* the mesh by solving a series of numerical optimization problems, penalizing the folds more and more until no inverted elements are present in the domain. Figure 4–right shows the resulting untangled mesh. As we have already said, the method also works in 3D, refer to Figure 5 for an illustration. We took a tetrahedral mesh of a combination wrench, and we imposed positional constraints on the vertices located on both ends of the wrench. In under a second, a valid deformation was found. In addition to being valid, our method produces deformations that minimize average distortion.

Our results were presented at the SIGGRAPH 2021 conference and published in the ACM Transactions on Graphics (TOG) journal [2]. Cherry on top of the cake: our method is so simple that a complete implementation fits in one page, and even has been published directly in the main text of our paper. We also made a short educational video (3:30mn) presenting these results and available at youtu.be/UQ4mbvKHKZk. We provide the SIGGRAPH/TOG article [2] in the portfolio. The video of our SIGGRAPH presentation is also available on the ACM website dl.acm.org/doi/abs/10.1145/3450626.3459847.

References

[1] W. T. Tutte. How to Draw a Graph. *Proceedings of the London Mathematical Society*, s3-13(1):743–767, 01 1963. https://doi.org/10.1112/plms/s3-13.1.743.

[2] Vladimir Garanzha, Igor Kaporin, Liudmila Kudryavtseva, François Protais, Nicolas Ray, and Dmitry Sokolov. Foldover-free maps in 50 lines of code. *ACM Transactions on Graphics*, 40(4), 2021. https://doi.org/10.1145/3450626.3459847.

Roots approximation of univariate polynomials

Gamble Team

Two fundamental problems in computer algebra are the evaluation of polynomials and the extraction of their roots. In a recent work published at FOCS 2021 [1], we present a new data structure that allows us to solve those problems with a complexity quasi-linear in the degree for well-conditioned polynomials.

Since 1972, it is known that evaluating a univariate polynomial of degree d on d points can be done in a quasi-linear number of arithmetic operations [2]. Unfortunately, this bound does not hold if we consider the bit complexity, where the arithmetic operations performed with a precision of m bits costs $\widetilde{O}(m)$ bit operations (log terms are omitted in the $\widetilde{O}(\cdot)$ notation). If we want to evaluate approximatively a polynomial on d points up to a constant absolute error, a direct application of Fiduccia algorithm leads to a bit-complexity bound in $\widetilde{O}(d^2)$ bit operations, and a more sophisticated algorithm provides a bound in $\widetilde{O}(d^{3/2})$ [3]. For almost 50 years, the following problem has remained open.

> Given a polynomial f of degree d with coefficients of constant size, and d complex points x_k in the unit disk, is it possible to compute all the $f(x_k)$ up to a constant absolute error with a number of bit operations quasi-linear in d ?

Nevertheless, the evaluation of polynomials on multiple points is used in many areas of computer science, such as polynomial system solving with the Newton method, homotopy continuation or subdivision algorithms, visualization of algebraic surfaces through raytracing or mesh computation, among others. Speeding up the numerical evaluation of polynomials may lead to an effortless practical improvement for many existing algorithms.

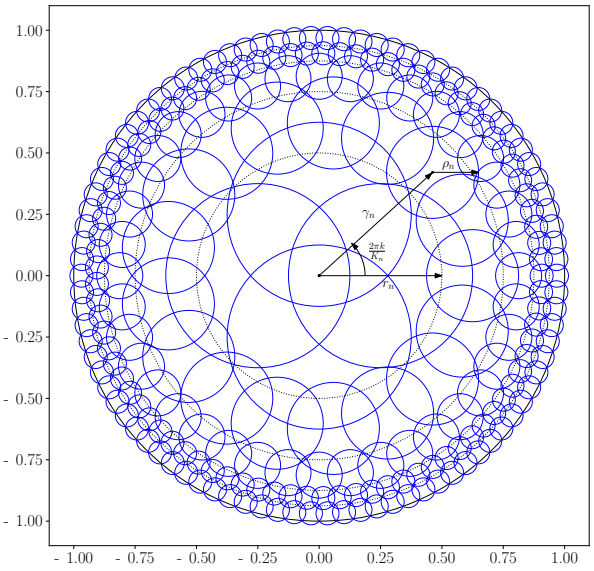


Figure 6: 5-hyperbolic covering

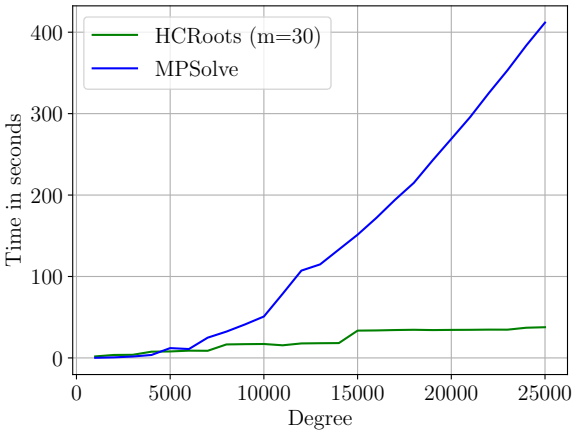


Figure 7: Time to approximate the roots of polynomials where the coefficients are random variable, centered Gaussian of variance 1

The data structure

Given a polynomial f of degree d and an integer m, the so-called *m-hyperbolic approximation* of f is roughly a piecewise approximation of f by polynomials of degree m. The key that allows us to improve the

state-of-the-art complexity bounds of several classical problems related to univariate complex polynomials is the hyperbolic layout of this piecewise approximation. This layout is a set of disks of radius exponentially smaller near the unit circle, and such that their union contains the unit disk, as illustrated in Figure 6. Although this layout is simple, it allowed us for the first time to derive algorithms quasi-linear in d for the two problems of numerical multipoint evaluation and polynomial root finding.

For the computation of the piecewise polynomials associated with each disk, we use evaluation and interpolation techniques on a carefully chosen set of points (Figure 8), that allows us to use the Fast Fourier Transform algorithm.

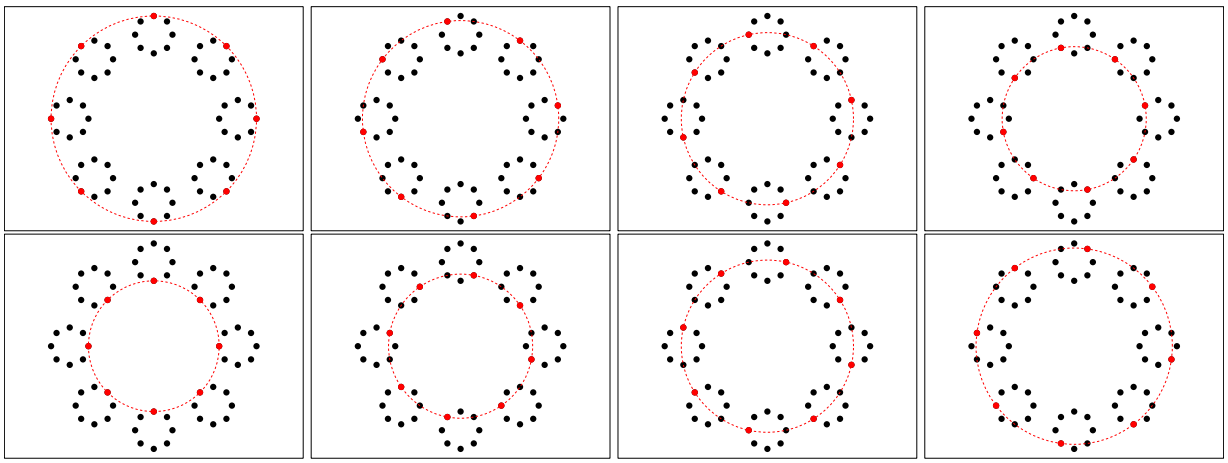


Figure 8: A polynomial f can be evaluated on a set of red points with a Fast Fourier Transform. With 8 calls to FFT, it is possible to retrieve the approximate polynomials of degree 8 for a 8-hyperbolic approximation.

Experimental proof of concept

For approximating the complex roots of a polynomial, we implemented `HCRoots` a small prototype in `Python`, using the standard numerical library `Numpy` for the routines based on Fast Fourier Transform.

The current state-of-the-art implementation of a root solver for complex polynomials is the software `MPSolve` [4, 5], implemented in the `C` programming language, and based notably on the Aberth-Ehrlich method [6] . Its development started more than 20 years ago and it has received several improvements over time, making it the fastest current implementation to find all the complex roots of a polynomial. This software also uses multi-precision arithmetic when necessary. By contrast, our solver `HCRoots` is an early prototype written in `Python`, working in machine precision only, and depending solely on the `NumPy` library. Nevertheless, as we can see in Figure 7, our solver `HCRoots` called with a precision parameter $m = 30$ is an order of magnitude faster than `MPSolve` for random polynomials.

Transfer

The practical efficiency of our new method attracted the software company Maplesoft, developer of the Maple Computer Algebra System Maple. We signed a contract in 2021 to enhance a prototype developed in `C`, and to integrate it in a future release of Maple. We also plan to make our software available with an open-source license, and to develop an open-source interface for the Sage Computer Algebra System.

References

[1] Guillaume Moroz. New data structure for univariate polynomial approximation and applications to root isolation, numerical multipoint evaluation, and other problems. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1090–1099, 2021. https://hal.archives-ouvertes.fr/hal-03249123v2.

[2] Charles M. Fiduccia. Polynomial evaluation via the division algorithm the fast fourier transform revisited. In *Proceedings of the Fourth Annual ACM Symposium on Theory of Computing*, STOC '72, page 88–93, New York, NY, USA, 1972. Association for Computing Machinery. https://doi.org/10.1145/800152.804900.

[3] Joris van der Hoeven. Fast composition of numeric power series. Technical Report 2008-09, Université Paris-Sud, Orsay, France, 2008.

[4] Dario A. Bini and Giuseppe Fiorentino. Design, analysis, and implementation of a multiprecision polynomial rootfinder. *Numerical Algorithms*, 23(2):127–173, Jun 2000. https://doi.org/10.1023/A:1019199917103.

[5] Dario A. Bini and Leonardo Robol. Solving secular and polynomial equations: A multiprecision algorithm. *Journal of Computational and Applied Mathematics*, 272:276–292, 2014. https://www.sciencedirect.com/science/article/pii/S037704271300232X.

[6] Louis W. Ehrlich. A modified newton method for polynomials. *Commun. ACM*, 10(2):107–108, February 1967. https://doi.org/10.1145/363067.363115.

Logarithme discret, factorisation d'entiers, et logiciel CADO-NFS

Équipe Caramba

En cryptographie à clé publique, l'immense majorité des systèmes actuellement déployés proviennent de la théorie des nombres. La sécurité repose sur la difficulté présumée de factoriser des entiers ou sur le problème du logarithme discret dans un groupe qui est soit le groupe multiplicatif d'un corps fini, soit le groupe des points rationnels d'une courbe elliptique.

Avec la menace de l'arrivée potentielle de l'ordinateur quantique, de nombreuses recherches sont menées pour préparer le remplacement de ces systèmes dont la sécurité s'écroulerait si ceci se produisait. Il n'en reste pas moins que les algorithmes cryptographiques classiques sont toujours omniprésents et le resteront encore probablement longtemps. Dans ce contexte, il est important de continuer à étudier la sécurité et la performance des systèmes d'aujourd'hui et de demain, sans se contenter de préparer ceux d'après-demain.

Logiciel CADO-NFS

https://gitlab.inria.fr/cado-nfs/cado-nfs

- L'équipe CARAMBA comprend les principaux contributeurs, depuis le début du projet en 2007.
- Licence libre GNU LGPL.
- Plus de 250,000 lignes de C/C++.
- Seule implémentation libre et complète de l'algorithme du crible algébrique (NFS) pour la factorisation et le logarithme discret.
- Implémente les algorithmes état de l'art, et parfois des améliorations pas encore publiées.
- Utilisé pour de nombreux records passés et présents, ainsi que pour des expériences de type preuve de concept.

Les travaux de l'équipe CARAMBA sur la période mêlent des études théoriques à des considérations très pratiques. En particulier, l'équipe développe depuis une quinzaine d'années le **logiciel libre CADO-NFS**, qui s'est désormais imposé comme la référence pour les calculs de factorisation ou de logarithme discret dans les corps finis, à la limite de ce qui est envisageable d'effectuer actuellement. L'algorithme utilisé est le crible algébrique (*Number Field Sieve*, NFS, en anglais), qui doit plutôt se voir comme un cadre algorithmique général se déclinant en de multiples variantes. Grâce à ce logiciel et aux améliorations apportées sur la période, des **calculs records** ont été effectués (voir encadré), dont le but est de calibrer de manière fiable les tailles de clés recommandées pour avoir un niveau de sécurité souhaité. Par exemple, dans [1], le calcul de factorisation d'une clé RSA de 829 bits, effectué en environ 2700 core-années, permet de mieux estimer la sécurité offerte par une clé RSA de 2048 bits.

Calculs records effectués par CARAMBA sur la période

- Factorisation des entiers RSA-240 (795 bits) et RSA-250 (829 bits) du Challenge RSA.
- Logarithme discret dans un corps premier de 795 bits.
- Logarithme discret dans un corps premier "truqué" de 1024 bits.
- Logarithme discret dans un corps de 521 bits de la forme $\mathbb{F}_{p^6}$.

(Voir aussi les pages Wikipedia recensant les records en factorisation et en logarithme discret.)

En ce qui concerne le problème du logarithme discret, les records effectués sont de type variés, car la question posée est multi-forme. Le problème le plus typique est obtenu lorsque l'on considère un corps premier (un $\mathbb{Z}/pZ$, avec p un nombre premier). La question principale qui se posait était la difficulté relative par rapport à un calcul de factorisation sur une entrée de taille similaire. Pour la première fois dans l'histoire, deux calculs records de taille égale (795 bits) ont été effectués dans un contexte complètement identique (même base logicielle, mêmes ma-

chines), ce qui a permis de constater que de subtiles améliorations algorithmiques en logarithme discret ramènent le ratio de difficulté à uniquement un facteur 3 en défaveur du logarithme discret, là où l'estimation classique se résumait auparavant à "c'est bien plus difficile". Ce double record a eu un écho au-delà de la sphère académique, et a été mentioné dans la presse (Le Monde, Ars Technica)[1].

Depuis la conception de l'algorithme NFS, il est bien connu que si le nombre premier p qui définit le corps fini est d'une forme très particulière, par exemple, tout proche d'une puissance de 2, alors le calcul de logarithme discret peut être accéléré (sans toutefois se faire en temps polynomial). Dans l'article [2], les connaissances sur ce sujet ont été remises au goût du jour: il est en fait possible d'avoir le même type d'accélération pour des nombres premiers d'apparence anodine. En guise de démonstration, un calcul de logarithme discret a été effectué dans un corps fini de 1024 bits, avec un nombre premier p truqué, au sens où il n'est pas aléatoire et est sujet à cette vulnérabilité. De fait, en l'état actuel des connaissances, il est même impossible de détecter cette particularité du nombre premier choisi. Ceci a mis en évidence la nécessité que tout nombre premier qui va être utilisé dans ce contexte vienne avec un "certificat de naissance", expliquant comment il a été obtenu, et prouvant ainsi son innocence. Certains nombres premiers ont ainsi été retirés des standards.

D'autres types de corps finis sont utilisés dans le contexte de la cryptographie à base de couplages, puisque l'on a alors des corps finis dont le cardinal est une puissance d'un nombre premier. Typiquement, il va s'agir de corps finis de la forme $\mathbb{F}_{p^k}$, où p est grand premier et k est un petit entier (disons entre 4 et 12). L'algorithme NFS fournit de nouveau la meilleure approche connue pour y résoudre le problème du logarithme discret, mais dans des versions assez éloignées de la variante principale utilisée en factorisation.

Le travail de thèse de Gabrielle De Micheli [3] a consisté à étudier plus précisément la portée théorique et pratique des attaques sur le logarithme discret dans ce contexte. Il faut mentionner que la demande est devenue forte, suite à une utilisation intense de la cryptographie à base de couplages dans bon nombre de blockchains. En effet, le besoin d'anonymat se traduit par l'omniprésence de preuves zero-knowledge d'un certain type, dont l'avatar à base de couplages est de loin le plus efficace.

Durant cette thèse, de premières analyses asymptotiques fines [4] ont révélé la difficulté intrinsèque d'une approche purement théorique à la question du niveau de sécurité offert par des corps finis de la forme $\mathbb{F}_{p^k}$. Puis, le résultat le plus marquant a été le développement et l'adaptation de la machinerie CADO-NFS à ce nouveau contexte. Le point crucial a été l'utilisation d'algorithmes issus de la théorie des réseaux euclidiens, dans un contexte bien différent de ceux pour lesquels ils avaient été développés. Ceci a permis d'effectuer un nouveau calcul record dans un corps de la forme $\mathbb{F}_{p^6}$, qui a eu un fort écho. L'article correspondant [5] a obtenu un Best Paper Award à la conférence ASIACRYPT 2021.

Gabrielle De Micheli a été récompensée pour ses travaux par le Prix L'Oréal – UNESCO en 2021, ainsi que le **Prix de thèse Gilles Kahn** en 2022. Elle est actuellement en postdoc à l'UCSD (San Diego).

References

[1] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *CRYPTO 2020*, volume 12171 of *LNCS*, pages 62–91. Springer, 2020. https://hal.inria.fr/hal-02863525.

[2] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. A kilobit hidden SNFS discrete logarithm computation. In *EUROCRYPT 2017*, volume 10210 of *LNCS*, pages 202–231. Springer, 2017. https://hal.inria.fr/hal-01376934.

[1] Article du Monde https://www.lemonde.fr/sciences/article/2019/12/03/deux-...1650684.html ; article de Ars Technica https://arstechnica.com/information-technology/2019/12/new-crypto-...-law/.

[3] Gabrielle De Micheli. *Discrete Logarithm Cryptanalyses : Number Field Sieve and Lattice Tools for Side-Channel Attacks*. Phd thesis, Université de Lorraine, May 2021. https://hal.univ-lorraine.fr/tel-03335360.

[4] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields. In *CRYPTO 2020*, volume 12171 of *LNCS*, pages 32–61. Springer, 2020. https://hal.archives-ouvertes.fr/hal-02871839.

[5] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. Lattice enumeration for tower NFS: a 521-bit discrete logarithm computation. In *ASIACRYPT 2021*, volume 13090 of *LNCS*, pages 67–96. Springer, 2021. https://hal.inria.fr/hal-03242324.

Digital filtering for geometric analysis

Équipe Adagio

Depuis plusieurs années, l'équipe ADAGIo mène une collaboration soutenue avec des chercheurs de l'INRAE de Champenoux dans le cadre d'applications en analyse d'images. Dès 2011, dans le cadre d'une thèse, des travaux ont été entrepris sur des images issues de scanner médical à rayons X afin d'étudier la morphologie des nœuds présents dans des images scannées de billons de bois. Ces travaux [1] ont été récompensés par un prix de thèse de la région en 2015. Deux projets ANR, pilotés par nos collaborateurs de l'INRAE, ont succédé à ce premier travail commun. Le projet ANR TreeTrace, débuté en 2018, s'intéresse au suivi des grumes de la forêt jusqu'à la scierie en exploitant des informations biométriques issues des images RVB des sections des grumes. Le projet ANR WoodSeer, initié en 2019, a pour objectif de détecter les défauts apparaissant sur les troncs d'arbre à partir de données LIDAR mais aussi de faire le lien avec la structure interne de l'arbre avec des données issues de scanner à rayons X.

Dans le cadre du projet TreeTrace, une thèse a été engagée sur l'estimation de la qualité du bois à partir des images de sections transversales de grumes, celles-ci pouvant être obtenues aussi bien en forêt que dans une scierie, ceci impliquant une grande variabilité de couleurs ainsi que du bruit du aux conditions de coupes. Dans ce cadre, nous avons publié nos travaux sur la segmentation des grumes et la détection de la moelle [2–4]. Notre étude de la détection et de l'analyse des cernes nous a conduit à élaborer un nouveau filtre morphologique directionnel qui utilise les propriétés arithmétiques des droites discrètes et qui peut être appliqué sur des images variées. Ce travail a été présenté en 2021 à la dernière conférence DGMM (Discrete Geometry and Mathematical Morphology) [5], première édition de la fusion entre les conférences internationales DGCI (Discrete Geometry for Computer Imagery) et ISMM (International Symposium on Mathematical Morphology). Rémi Decelle a remporté pour cet article le prix du meilleur article étudiant.

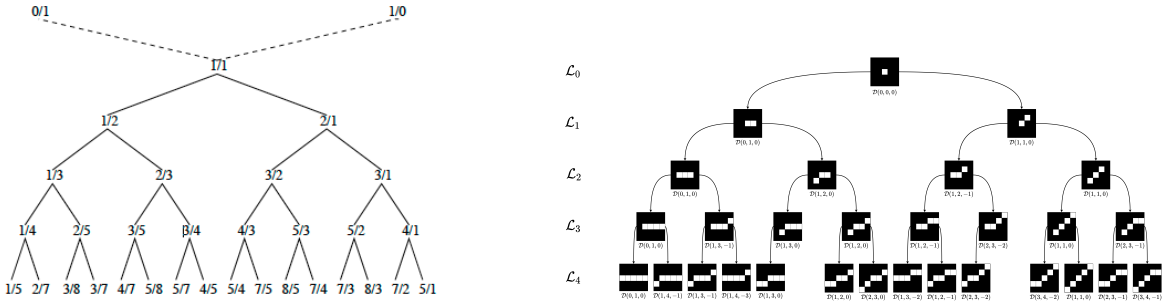


Figure 9: A gauche, début de la construction de l'arbre de Stern-Brocot. A droite, sous-arbre des segments de droite discrètes de pentes les noeuds d'une partie du sous-arbre gauche de l'arbre de Stern-Brocot.

Cet article s'intéresse à l'analyse et aux caractérisations locales d'une image, c'est à dire aux différentes propriétés en chaque pixel ou groupe de pixels de l'image en fonction de son voisinage. Ces informations permettent de caractériser différents éléments dans l'image et elles sont très souvent utilisées dans les tâches de traitement et d'analyse d'images, de reconnaissance de formes, de détection d'objets, etc. Parmi ces caractéristiques, l'orientation locale est une des plus importantes pour extraire des structures de haut niveau dans l'image : des contours, des textures et des formes présentes dans l'image.

L'objectif de notre article est de calculer en chaque pixel d'une image une caractéristique locale correspondant à la direction du plus long segment de droite discrète arithmétique passant par ce point, direction privilégiée avec de plus des informations de longueur et d'épaisseur associées à ce segment.

Notre méthode repose sur la définition arithmétique des droites discrètes [6] permettant d'avoir une épaisseur variable. De plus, les structures géométriques engendrées pour une longueur $2n+1$ fixée sont en

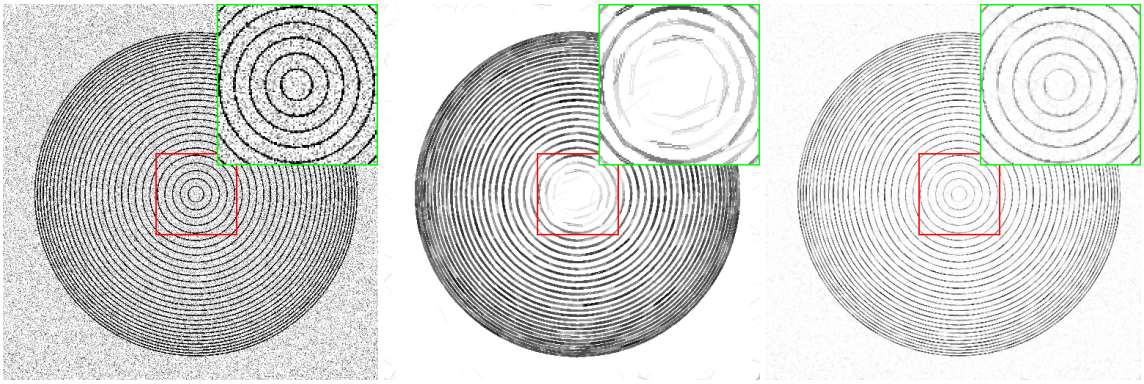


Figure 10: (a) Image bruitée, (b) Image filtrée avec [8], (c) Image filtrée avec notre méthode. En haut à droite sur chaque image, zoom sur la partie centrale.

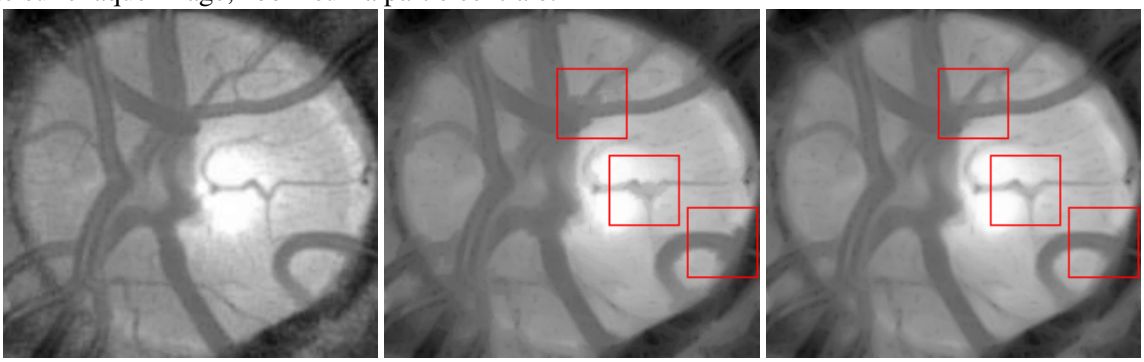


Figure 11: (a) Image originale de rétine, (b) filtrage avec [8], (c) filtrage avec notre méthode.

lien avec les suites de Farey d'ordre n (*i.e.*, les suites de fractions irréductibles entre 0 et 1 pour lesquelles le dénominateur est inférieur ou égal à n). La croissance d'un segment à partir d'un point correspond à un cheminement dans l'arbre de Stern-Brocot [7] dans lequel chaque fraction $\frac{m+m'}{n+n'}$ est telle que $\frac{m}{n}$ est son plus proche ancêtre droit et $\frac{m'}{n'}$ son plus proche ancêtre gauche. La suite de Farey d'ordre n définit un sous-arbre dans l'arbre de Stern-Brocot (cf. Fig. 9).

Nos algorithmes utilisent ces propriétés et, dans les images en niveau de gris, le filtre est complété par des opérations morphologiques inspirées des travaux de Soille et al [8]. Nos méthodes et les résultats obtenus, plus performants que les techniques antérieures (cf. Fig. 10 et Fig. 11), ont suscité l'intérêt de la communauté de géométrie discrète et de morphologie mathématique lors de la conférence DGMM de 2021 avec l'obtention du prix du meilleur article étudiant.

References

[1] Adrien Krähenbühl, Bertrand Kerautret, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. Knot segmentation in 3d CT images of wet wood. *Pattern Recognit.*, 47(12):3852–3869, 2014. https://hal.archives-ouvertes.fr/hal-00780731.

[2] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. Pith estimation on tree log end images. In *Reproducible Research in Pattern Recognition - Third International Workshop, RRPR 2021, Virtual Event, January 11, 2021, Revised Selected Papers*, volume 12636 of *Lecture Notes in Computer Science*, pages 101–120. Springer, 2021. https://hal.archives-ouvertes.fr/hal-03006060.

[3] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frederic Mothe, and Fleur Longuetaud. A new algorithm to automatically detect the pith on rough log-end images. In *21st International Nondestructive Testing and Evaluation (NDTE) of Wood Symposium*, Freiburg, Germany, September 2019. https://hal.inria.fr/hal-02275651.

[4] Rémi Decelle and Ehsaneddin Jalilian. Neural Networks for Cross-Section Segmentation in Raw Images of Log Ends. In *IPAS 2020 - Fourth IEEE International Conference on Image Processing, Applications and Systems*, Gênes / Virtual, Italy, December 2020. https://hal.archives-ouvertes.fr/hal-03058259.

[5] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. Digital straight segment filter for geometric description. In *Discrete Geometry and Mathematical Morphology - First International Joint Conference, DGMM 2021, Uppsala, Sweden, May 2021*, volume 12708 of *Lecture Notes in Computer Science*, pages 255–268. Springer, 2021. https://hal.archives-ouvertes.fr/hal-03144152.

[6] Jean-Pierre Reveillés. *Géométrie discréte, calcul en nombres entiers et algorithmique*. PhD thesis, Université Louis Pasteur, 1991.

[7] M. Stern. Uber eine verallgemeinerung der kreistheilung. *Journal fur die reine und angewandte Mathematik*, 55:193–220, 1858.

[8] P. Soille and H. Talbot. Directional morphological filtering. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 23(11):1313–29, 2001.

IceSL: modeling and slicing for Additive Manufacturing

MFX Team

The IceSL software https://icesl.loria.fr emerged as a result from the ERC ShapeForge project (StG-2012-307877). It has become a corner stone of the MFX team, serving simultaneously as an internal and external research platform, a vector of diffusion for our results, a vector of collaboration, and a standalone free software for makers, hobbyist, schools and companies alike.

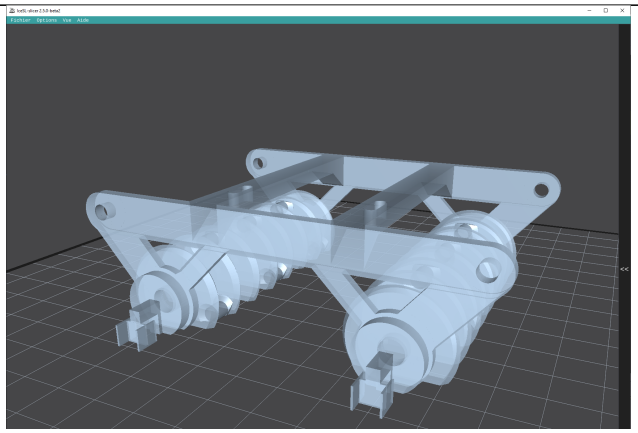
IceSL key originality is to tightly couple a 3D modeler and a *slicer* – the process that prepares trajectories and instructions for additive manufacturing machines. It takes as input a geometry specification and directly produces machine instructions for 3D printing, allowing algorithms to produce trajectories directly from the specifications, without any intermediate remeshing. Modeling is performed by combining primitives (meshes, implicit volumes, voxel data, signed distance fields) through a powerful scripting language.

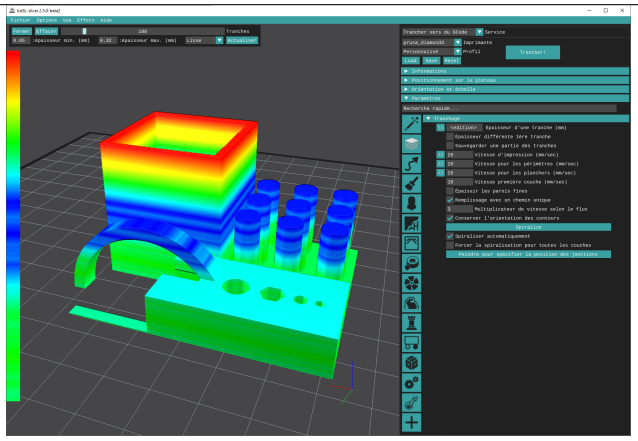
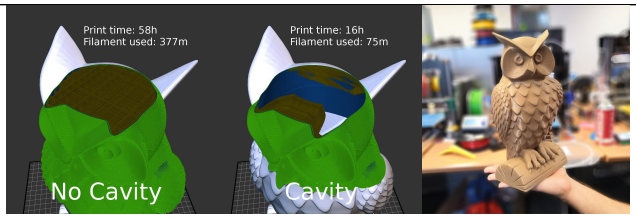
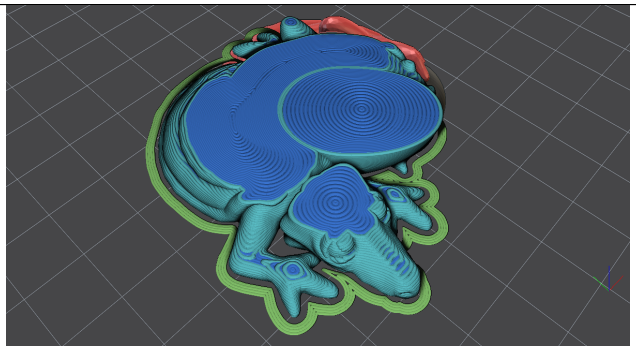
Within the evaluation period, we have developed highly efficient algorithms for visualization and slicing [1], rooted in our rendering expertise. These allow interactive feedback while performing complex combinations of shapes (construction operators such as union, intersection and difference but also erosion and dilation). We revisited slicing and trajectory optimization, to produce more accurate parts [2], synthesize internal cavities to save time and material [3], generate varying width trajectories [4] and enable (for the first time) color printing using fused filament technologies [5]. IceSL goes beyond the description of shapes and allows the specification of gradients of internal properties. These are then used during slicing to generate complex internal patterns, controlling physical properties of the final parts such as its density, flexibility, porosity [6–9]. These features are illustrated in the table below.

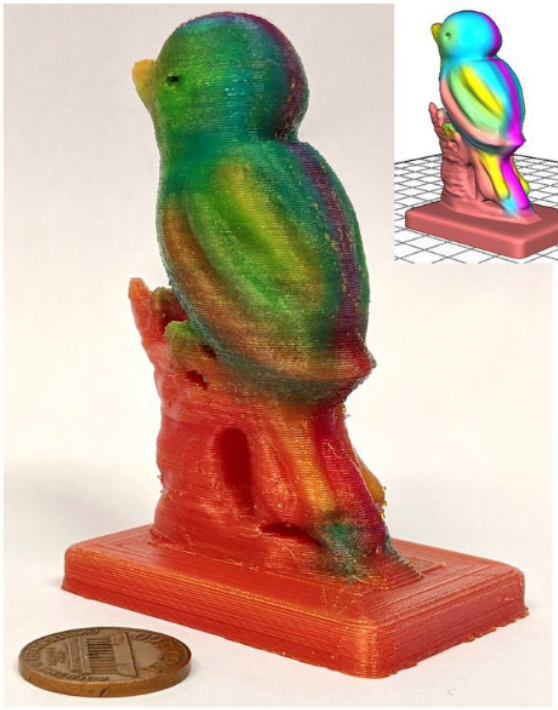
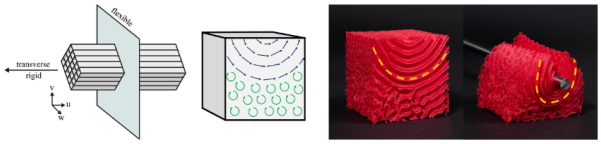
Remarkably, results from our publications cited in the previous paragraphs are all available and interoperate within IceSL. Most of our research either use IceSL or represent future extensions, such as our curved slicing work [10].

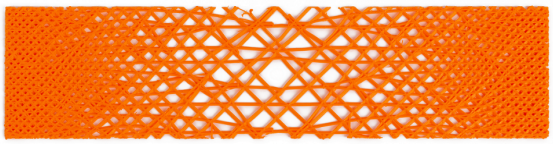
Currently, IceSL is available to the public as a downloadable program for multiple platforms (Windows and Linux) and an online version (through a web browser) through its website https://icesl.loria.fr. It has an active online community in Google, Twitter and Github where people gather news, ask/post on topics related to its use and contribute to its pool of usable 3D printers, modeling effects, printing strategies (through infills), customize its interface and more.

IceSL has a regular release calendar where each version includes new features both on modeling and slicing. Cumulative downloads of the program are around 145K with 55K in 2021 alone. The online version was used 22K times in 2021 with an average of 100 uses per day (a *use* meaning actually processing a model through the software). The community has more than 250 users in the discussion group and more than 500 followers on twitter. IceSL supports more than sixty different 3D printers.

Efficient CSG geometry [1]		Real time construction, visualization and slicing of 3D shapes with CSG operations

Optimal adaptive slicing [2]		Automatic calculation of optimal printing thickness through geometry's height
Maximal self-supporting cavities [3]		Self supporting structure for inner volume to minimize printing material use and printing time
Variable width contouring [4]		Countouring of 3D shapes of variale width to maximize fill of volume

Color mixing [5]		Mixed of fused filament for producing prints with custom color painting
Deformable shapes [6]		Freely orientable microstructures that allow the printing of deformable 3D printed shapes
Space filling printing strategy [7]		Printing curved trajectories with controlable orientation for 3D printing

Elastic properties in 3D printing [8]		Microstructures for 3D printing that allow different elastic behaviours on the final shape
Progressive infills [9]	 **Figure 7: 3D printed part revealing an infill pattern obtained from our technique. Note the very progressive change in density and the curve network extracted at each layer.**	Procedural generation of inner volume for variable density

References

[1] Cédric Zanni, Frédéric Claux, and Sylvain Lefebvre. HCSG: Hashing for real-time CSG modeling. In *Proceedings of the ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games*, Montreal, Canada, May 2018. https://hal.inria.fr/hal-01792866.

[2] Marc Alexa, Kristian Hildebrand, and Sylvain Lefebvre. Optimal discrete slicing. *ACM Transactions on Graphics*, 36(1):1 – 16, February 2017. https://hal.inria.fr/hal-01660773.

[3] Samuel Hornus and Sylvain Lefebvre. Iterative carving for self-supporting 3D printed cavities. In *Eurographics 2018 - Short Papers*, Delft, Netherlands, April 2018. https://hal.inria.fr/hal-01764291.

[4] Samuel Hornus, Tim Kuipers, Olivier Devillers, Monique Teillaud, Jonàs Martínez, Marc Glisse, Sylvain Lazard, and Sylvain Lefebvre. Variable-width contouring for additive manufacturing. *ACM Transactions on Graphics*, 39(4 (Proc. SIGGRAPH)), July 2020. https://hal.inria.fr/hal-02568677.

[5] Haichuan Song, Jonàs Martínez, Pierre Bedell, Noemie Vennin, and Sylvain Lefebvre. Colored fused filament fabrication. *ACM Transactions on Graphics*, 38(5):1–11, June 2019. https://hal.inria.fr/hal-01660621.

[6] Thibault Tricard, Vincent Tavernier, Cédric Zanni, Jonàs Martínez, Pierre-Alexandre Hugron, Fabrice Neyret, and Sylvain Lefebvre. Freely orientable microstructures for designing deformable 3D prints. *ACM Transactions on Graphics*, 39(6):1–16, December 2020. https://hal.inria.fr/hal-02524371.

[7] Adrien Bedel, Yoann Coudert-Osmont, Jonàs Martínez, Rahnuma Islam Nishat, Sue Whitesides, and Sylvain Lefebvre. Closed space-filling curves with controlled orientation for 3D printing. https://hal.inria.fr/hal-03185200, March 2021.

[8] Jonàs Martínez, Samuel Hornus, Haichuan Song, and Sylvain Lefebvre. Polyhedral Voronoi diagrams for additive manufacturing. *ACM Transactions on Graphics*, 37(4):15, August 2018. https://hal.inria.fr/hal-01697103.

[9] Jimmy Etienne and Sylvain Lefebvre. Procedural band patterns. In *Symposium on Interactive 3D Graphics and Games*, Symposium on Interactive 3D Graphics and Games, pages 1 – 7, San Francisco, United States, September 2020. Association for Computing Machinery. https://hal.archives-ouvertes.fr/hal-02457161.

[10] Jimmy Etienne, Nicolas Ray, Daniele Panozzo, Samuel Hornus, Charlie C.L. Wang, Jonàs Martínez, Sara Mcmains, Marc Alexa, Brian Wyvill, and Sylvain Lefebvre. CurviSlicer: Slightly curved slicing for 3-axis printers. *ACM Transactions on Graphics*, 38(4):1–11, August 2019. https://hal.archives-ouvertes.fr/hal-02120033.