Lorraine Laboratory of **Research** in **Computer Science** and its **Applications**

ACTIVITY REPORT 2011 - 2016
PROSPECTIVES FOR 2017 - 2022

A research unit from the **research department AM2I** of **Lorraine University: Automatics, Mathematics, Computer Science and** their **Interactions**

Loria
Laboratoire lorrain de recherche en informatique et ses applications



Volume 2

Loria
cnrs
Inria
INVENTEURS DU MONDE NUMÉRIQUE
UNIVERSITÉ DE LORRAINE

Contents

01

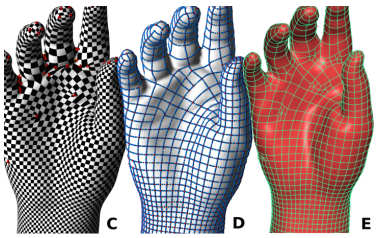
Activity Report

Department 1

Algorithms, Computation, Geometry and Image

Department Head: Sylvain Lazard

Department 1 entitled *Algorithms, Computation, Image and Geometry* regroups six teams that share scientific interests on these topics. Beside *algorithms* which is a common center of interest to all these teams (and of course to some teams of other departments as well), there are various centers of interest common to several teams. *Geometry* plays an important role in most teams, i.e., ADAGIO, ALICE, CARAMBA, MAGRIT, and VEGAS. *Symbolic and algebraic computing* is of common interest of CARAMBA and VEGAS, *image* is of interest to ADAGIO, ALICE and MAGRIT, *combinatorics and complexity* also concerns several groups as ADAGIO, CARAMBA, and VEGAS, *certified computing* (in a sense that sometimes requires computing with arbitrary precision numbers) is also of common interest to CARAMBA, VEGAS, ADAGIO, and ALICE. The main common interest of ABC with the other groups is the algorithmic culture they share.



Overview of Department 1

1 Department Composition

Department leader

Sylvain Lazard (since June, 2014)
Bruno Lévy (before June, 2014)

List of teams

ABC statistical learning theory, bioinformatics

ADAGIO discrete and digital geometry, discrete algorithms, combinatorics, imaging

ALICE numerical geometry & simulation, computer graphics, 3D printing (EPC Inria)

CARAMBA (formerly **CARAMEL**) computer arithmetic, algebraic curves, integer factorization, cryptography, computer algebra (EPC Inria)

MAGRIT motion tracking, multimodal fusion, augmented reality, medical imaging (EPC Inria)

VEGAS computational, non-linear, non-Euclidean and probabilistic geometry (EPC Inria)

	PR	MCF	PRAG	DR	CR	Total
2011	1	11	1	4	9	26
2016	2	8	-	8	6	24

Phd's defended	18	On-going PhD's	17
Postdocs	13	Engineers	12

22 of our 35 PhD students are/were supported by ministry grants (via university or ENS), 5 by INRIA, 2 by CIFRE grants, 2 by the region and 4 by foreign grants.

Departement evolution

None.

2 Life of the department

In terms of governance, we run our department with a council that consists of the head of the department and the heads of the teams. This council handles matters at the level of the department such as the evaluation and ranking of PhD candidates for UL contracts, the department bugdet, the needs for new faculty positions (*profils de postes*). The head of the department also handles

We also handle the restructuration of the teams within the departement, although this has only been theoretical so far because the teams in our departement have been stable.

The departement seminar is distributed in the sense that it is the teams' seminars that we share within the departement. We also organize once a year a day of the departement in which every PhD student presents their work. This is both a way to interact scientifically within the departement and also to help detect possible difficulties that PhD students may have.

3 Research topics

Keywords: algorithms, computing (symbolic, algebraic and numerical), geometry (computational, discrete, probabilistic and non-linear), classification and statistical learning, image processing, computer vision.

Before detailing the research topics of each team, we briefly describe here the main common centers of interest of these teams, in *Algorithms and computation*, *Geometry* and *Image*.

- **Algorithms and computation** is central to the scientific culture of the department and it covers various domains. First, research on *combinatorics and complexity analysis* (worst case or probabilistic) naturally concern several groups, in particular, ADAGIO, CARAMBA, and VEGAS. On an algorithmic level, *optimization* problems, including convex programming, mixed-integer programming and non-convex optimization are central to the teams ABC, ALICE, and MAGRIT, while they also are of some interest to the VEGAS team. *Learning theory* and *classification* are also of concern to several groups; it is central to ABC's research but other groups share some interest on this topic, in particular MAGRIT and ALICE (constrained optimization, spectral analysis). *Arithmetic and certified computing*, in the sense that algorithms are usually designed over the reals although they are implemented with integers or floating-point numbers, plays an important role in CARAMBA, VEGAS, ADAGIO, and ALICE. On an algorithmic level, CARAMBA and VEGAS are also very involved in *symbolic and algebraic computing*.

- **Geometry**: As hinted above, geometry plays an important role in almost all teams. Geometry refers here to a wide spectrum of theories, each of which depending both on the mathematical objects under considerations (e.g. simplicial and cellular complexes, algebraic curves and surfaces) and on the properties that are studied (e.g. intersections, topology, singularities, combinatorial structure). The forms of geometry known as *discrete*, *projective*, *digital*, *algebraic*, and *computational* are each of interest to several groups.

- **Image**: Finally, the department is interested in methods that use images as input data *(image analysis, image processing, registration, modeling from images)* and methods that produce images *(image synthesis, texture generation)*. These two classes of methods share a common background, of interest to half the teams of the department, namely ALICE, MAGRIT and ADAGIO.

The application domains of the department include geometric modeling, imaging, augmented reality, numerical simulation, videogames, bioinformatics, computer algebra systems and cryptography. This spectrum of applications is quite large and it should be mentioned that most teams have fairly disjoint such application domains. This can be explained by fact that departments were created to bring together teams with the same scientific culture rather than with an application-based view. The rest of this section summarizes the research topics of the six teams.

ABC contributes to three different fields: **machine learning, bioinformatics and statistics**. Its scientific goal is to develop the theory and practice of supervised and unsupervised learning. ABC focuses on the theory of multi-class pattern classification, deriving uniform convergence results dedicated to margin discriminant models. Its applications are in the field of biological sequence processing. More precisely, ABC develops theoretical bounds on the risk of classifiers, methods of model selection, multi-class support vector machines, methods of switching and piecewise regression, methods for robust data mining and methods for statistical processing of biological sequences (e.g., protein secondary structure prediction).

The general goal of **ADAGIO** is to develop efficient algorithms on **discrete and digital structures.** In order to develop efficient algorithms, the properties of the underlying structures need to be understood thoroughly. The main objective of ADAGIO is to study these properties, which can be *geometrical*,

arithmetical or *combinatorial* depending on the situation. More specifically, ADAGIO is interested in the fundamental aspects of *discrete and digital geometry*, which characterizes discrete objects that have a geometric (planar or spatial) interpretation. The general goal is to define a theoretical framework to translate to $\mathbb{Z}^n$ basic notions of the Euclidean geometry (such as distance, length and convexity) as faithfully as possible. The algorithms developed by ADAGIO are naturally used in imagery applications.

ALICE is a team that does research in **geometry processing** and in **computer-aided fabrication**. In geometry processing, ALICE develops algorithms to transform and optimize the geometric representations of 3D objects. The targeted applications are meshing for numerical simulation and 3D rendering. In computer-aided fabrication, ALICE develops algorithms for making 3D fabrication easy to use for a widest possible audience. In particular, they focus on easy generation of 3D content for casual users, and integrating physical constraints of fabrication into geometry processing tools.

CARAMBA studies the algorithmic aspects of **cryptography and cryptanalysis** from the top-level mathematical background down to the optimized high-performance software implementations. CARAMBA strives in particular to develop and provide fast software dealing with various mathematical objects. These mathematical objects are of utmost importance for cryptology, as they are the background of the most widely developed cryptographic primitives, such as the RSA cryptosystem or the Diffie-Hellman key exchange. One central challenge is the assessment of the security of proposed cryptographic primitives through the study of two cornerstone problems: the integer factorization and discrete logarithm problems. Another key challenge is to produce cryptographic implementations that are both efficient and secure.

MAGRIT does research in **computer vision** with a focus on **augmented reality** (AR) applications. The basic concept of AR is to place information correctly registered with the environment into the user's perception. Realistic integration of virtual objects also requires to manage interactions between the added objects and the real scene (e.g. occlusions, shadowing, contact). Pose computation and model acquisition are thus key issues of AR. Despite significant progress of tracking technologies over the years, there are still technological barriers that prevent applications from reaching the robustness and the accuracy required by cutting-edge applications, for instance in medical imaging or urbanism. The aim of MAGRIT is thus to develop reliable and effective vision-based methods for pose computation and model acquisition.

The main scientific objective of **VEGAS** is to contribute to the development of an effective geometric computing dedicated to non-trivial geometric objects. Our main axes of research focus on various aspects of **computational geometry**, in particular, on problems that deal with **non-linear objects** and with **combinatorial and probabilistic properties** of data structures and algorithms.

4 Main results

We shortly present some main results we obtained in our three axes of research, namely *Algorithms and Computation*, *Geometry* and *Image*.

Algorithms and Computation

Discrete logarithms in finite fields (Caramba). We published in 2013 an algorithm with quasi-polynomial complexity $n^{O(\log n)}$ for computing discrete logarithms in finite fields $\mathbb{F}_{p^n}$, where the characteristic p is fixed to a small value [251] (best paper award) This is an enormous breakthrough, as this problem was previously among the purportedly hardest problems which underpin modern cryptography. As a result, some of the mathematical objects proposed for use in cryptography (small characteristic finite fields, or pairings on elliptic curves defined over such fields) were permanently removed from the cryptographer's portfolio. This work also received the "Prix de thèse

Le Monde" [208].

We also worked on the discrete logarithm problem in more general finite fields (not only small characteristic case). We improved algorithms for specific cases [250, 208, 278, 256, 217, 275, 263, 264], illustrated by record computations [248, 250] relevant to pairing-based cryptography in particular. On the practical side, we published the LogJam attack [244] (best paper award), which mixes findings on protocol design flaws in SSL/TLS, as well as algorithmic adaptations of the Number Field Sieve method to mount a convincing proof of concept for the attack. This work also received the Pwnie award in the category "Most innovative research" during the BlackHat 2015 conference.

Certified drawing of plane algebraic curves (Vegas). We obtained many results on this fundamental problem [377, 382, 403, 404, 405, 431, 444]. In a nutshell, we decreased the worst-case bit complexity of solving bivariate algebraic systems via rational parameterizations from $\widetilde{O}_B(d^{12} + d^{10}\tau^2)$ in 2009 to $\widetilde{O}_B(d^6 + d^5\tau)$, where d and τ bound the input degrees and coefficient bitsizes, and we also presented more efficient $\widetilde{O}_B(d^5 + d^4\tau)$ Las Vegas algorithms. These bounds are "morally" optimal in the sense of that improving them would essentially require to improve bounds on several other fundamental problems (on resultants and roots isolation of univariate polynomials) that have hold for decades. The efficiency of our algorithm Isotop is based on these algorithms.

Optimal Transport (Alice). We developed the first practical algorithm for computing L_2 Optimal Transport in 3D [138]. This opens the path for new solvers for a whole familly of Partial Differential Equations (with the Monge-Ampere operator) that are involved in fluid dynamics and astrophysics (early-universe reconstruction). Our algorithm scales up to multi-million variables, thus gaining more than three orders of magnitude compared to the state of the art which is limited to a few thousand variables.

Theory of multi-category pattern classification (ABC). We proved a breakthrough bound on the complexity of pattern classification in terms of the number C of categories and the size m of the sample. Under minimal hypotheses, the best previous bound was linear in $C/\sqrt{m}$ and we proved a bound in $\sqrt{C/m}$ [12]. Roughly speaking, this means that, for any classifier, if a sample of size m is enough to learn a C-category problem, then a sample of size km (instead of k^2m) is enough to learn a kC-category problem.

Switching and piecewise regression (ABC) are difficult learning problems that suffer long-standing limitations on the number of data that can be handled. We proved their NP-hardness and that they admit polynomial-time algorithms for fixed dimensions [17, 18]. We also developed new heuristics that increase by two the order of magnitude of data that can be handled efficiently [13, 16, 24, 19, 39].

Geometry

The worst visibility walk in a random Delaunay triangulation is $O(\sqrt{n})$ (Vegas). Using percolation theory and stochastic geometry, we showed that the memoryless routing algorithms Greedy Walk, Compass Walk, and all variants of visibility walk based on orientation predicates are asymptotically optimal in the average case on the Delaunay triangulation [437]. This settle a long-standing conjecture in point location using walking algorithms. Along that line, we also presented several other substential results and methods on the probabilistic analysis of geometric structures [412, 411, 389, 439].

Multinerves and Helly numbers of acyclic families (Vegas). We unified several Helly-type theorems in and outside geometric transversal theory, and we generalized the nerve theorem, a result that is fundamental in topological data analysis. As a consequence, it was well received in both mathematic and computer science communities, and published at SoCG 2012 (best paper award) [410] and in Advances in mathematics [388].

Additive manufacturing (Alice). We proposed for the first time algorithms for generating 3D objects with moving parts, such as mechanisms, and for creating inner cavities and inconspicuously deforming shapes to ensure that they are well balanced after fabrication. We also made a leap forward regarding the example-based synthesis of structures and micro-structures by optimizing the topology, rigidity and appearance of surface and inner structures of objects. Considering fabrication processes, we presented solutions for the problems of oozing filaments and features that are overhanging during the fabrication by generating automatically protecting shields and scaffoldings. All these results were presented at SIGGRAPH [169, 141, 158, 128], SIGGRAPH Asia [144] and Eurographics [132, 131] (with one best paper honorable mention).

Unstructured meshes (Alice). We developed efficient algorithms for sampling surfaces and volumes embedded in arbitrary dimensions, which resulted in an anisotropic meshing algorithm, which is resistant to defects in the input data (e.g., skinny triangles, overlaps, holes) [168, 148]. We applied it in the context of oil exploration, results we published in *Computers and Geosciences Journal* and which obtained the 2014 journal best paper award [155].

Connectivity of discrete hyperplanes (ADAGIo). For any normal vector, there exists a critical thickness, called connecting thickness, under which the discrete hyperplane is disconnected and above which it is connected. We have solved a problem that has been opened for about fifteen years by showing that, in any dimension, the hyperplane at the connecting thickness is almost always disconnected, except when the normal vector belongs to some fractal set with zero Lebesgue measure [82].

Analysis of noisy discrete curves (ADAGIo). We proposed an unsupervised algorithm for the problem of estimating the noise of digital contours, problem that has been opened for two decades [68, 69, 88]. Based on this estimation, we showed how it was possible to obtain a parameter-free generalization of the tangential cover, a classical tool for the study noisy digital contours [96]. This opened new research perspectives, which led so far to results on dominant point detection [74, 97] and curve decomposition into arcs [99].

Image

CT scans of wood trunks (ADAGIo). We work with INRA on the detection of wood knots in 3D CT images of trunks in order to optimize their cuts. For this original problem, no off-the-shelf solution works well. We proposed new methods based on the accumulation of local intensity changes [90, 91, 70] and on the generation of tangent slices [75, 95, 92], which were succesfully validated through the development of our TKDetection software [71] (best demonstration award). This work also received the “Prix de thèse de la Région Lorraine” [60].

Localization and 3D tracking (Magrit). Computing pose estimates from monocular images without any guess on the localization is still a deadlock depending on the complexity of the scene and on the viewpoint variations between the current image and the model. We proposed various methods that dramatically improve the reliability of the localization: (i) we designed a new a contrario

model for matching to cope with repetitive patterns [288, 310] and (ii) we proved the effectiveness of models enriched with simulated viewpoints to perform image/model matching when large viewpoints variations occur [335, 357]. We have also done significant work on tracking deformable objects in collaboration with the MIMESIS Inria team (Strasbourg) with promising applications to laparoscopy [298]; this work also received the best paper honourable mention at ISMAR [328].

Acquisition of structured models for Augmented Reality (Magrit). Making AR application effective requires the availability of structured models of the scene capable of supporting real-time object interactions such as occlusions, lighting or contacts. In this context, we proposed (i) original methods based on the camera-mouse principle for in-situ modeling of man-made environments and (ii) a new model of vasculature consisting of a tree of local implicit blobby models [347, 348]. These contributions meet, in particular, the computational requirements of interactive simulation in interventional radiology.

Scientific production and quality

5 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis	4	3	7	5	6	1	26
H.D.R	1	1		1			3
Journal	36	25	31	27	28	15	162
Conference proceedings	38	34	37	33	25	5	172
Book chapter	3	2	5	3	1	1	15
Book (written)	1		1				2
Book or special issue (edited)	1	2	2	2	3		10
Patent	1		3	1	1		6
General audience papers	1		2		1		4

List of top journals in which we have published

Mathematics of Computation (5) [215, 217, 226, 216, 238]
DCG – Discrete and Computational Geometry (4) [381, 393, 395, 383]
JSC – Journal of Symbolic Computation (5) [233, 240, 231, 397, 382]
Advances in Mathematics (1) [388]
TVCG – IEEE Trans. on Visualization and Computer Graphics (4) [297, 298, 161, 136]
SIAM journal on imaging sciences (2) [310, 307]
JMLR – Journal of Machine Learning Research (1) [14]
Automatica (3) [13, 17, 18]
TCS – Theoretical Computer Science (2) [65, 67]
TPAMI – IEEE Transactions on Pattern Analysis and Machine Intelligence (1) [68]
PR – Pattern Recognition (2) [74, 70]
TOG – ACM Transactions on Graphics (11) [130, 122, 143, 151, 158, 168, 159, 128, 141, 144, 129]
(including 6 SIGGRAPH and 2 SIGGRAPH ASIA)
Computer Graphics Forum (8) [169, 142, 149, 150, 137, 132, 131, 121]
(6 EUROGRAPHICS and 2 ACM Symposium on Geometry Processing)

List of top conferences in which we have published

In Computer Graphics, all the proceedings of the top conferences are published as a special issue of a journal (SIGGRAPH and SIGGRAPH ASIA → ACM Transactions on Graphics, EUROGRAPHICS and ACM Symposium on Geometry Processing → Computer Graphics Forum).

SoCG – Symposium on Computational Geometry (5) [410, 412, 411, 402, 413]
ISSAC –International Symposium on Symbolic and Algebraic Computation (5) [403, 405, 404, 259, 258]
ISMAR – Int. Symp. on Mixed and Augmented Reality (4) [339, 320, 328, 326]
MICCAI Int. Conf. on Medical Image Computing and Computer-Assisted Intervention (1) [348]
Eurocrypt (2) [251, 250]
Asiacrypt (3) [261, 243, 252]
ANTS – Algorithmic Number Theory Symposium (1) [247]
DGCI – International Conf. on Discrete Geometry for Computer Imagery (5) [82, 91, 84, 86, 102]
SODA – Symposium on Discrete Algorithms (1) [419]

These represent only 31% and 24% of our journal and conferences publications, which is small because our 6 groups publish in different venues (with the exception of JSC, TVCG and ISSAC) and we tried to keep these lists reasonably short.

6 Software

We highlight here some of our principal software and refer to the team's sections for details.

Machine Learning. (ABC) Our main software products, for which updates are regularly released, are MSVMpack [14] for multi-class discrimination (with more than 5000 downloads over the last 5 years, url), MSVMpred for biological sequence segmentation and MLweb (url) for machine learning on the web (with more than 600 downloads in 5 months).

DGtal library (ADAGIo). We are part of the main development team of this open source library for Digital Geometry programming. We participate to the main library framework (structure, organisation, pull request review, diffusion, tutorials, tools with the associated DGtalTools project) and actively contribute to the Topology, Geometry and IO packages (url).

IceSL (Alice) is a 3D modeler for additive manufacturing, which directly drives 3D printers (url). It avoids the requirement of most other software to produce large intermediate triangular meshes, which are prone to numerical issues. Our very compact memory representation in IceSL enables the fabrication of complicated 3D models with internal structures and details of micro-metric size. We recently received an ERC Proof of Concept grant (named IceXL) to further develop the software and study its industrial potential via a number of existing partnerships in the medical, automotive and design industries.

Geogram-Vorpaline-Graphite (Alice). Geogram is an open-source library (url) of data structures and geometric algorithms for reconstruction, remeshing, 3D Delaunay triangulations, Lloyd relaxation in nD, restricted Voronoi diagram in nD, numerical solvers and generation of predicates (from their formulas). Vorpaline is a proprietary extension of Geogram and Graphite is a graphical user interface built on top of them. Since 2011, our main result is the first fully automatic hexahedral-dominant mesher, which is well suited to solve a certain class of Partial Differential Equations (e.g., elasticity). Through our ERC 'Proof of Concept' grant Vorpaline, we then transformed this prototype into a technology preview, which is in the process of being acquired by two of the GOCAD-consortium oil compagnies.

CADO-NFS (Caramba) is a state-of-the-art implementation for factoring integers and computing discrete logarithms in finite fields (url). The C/C++ code source is about 200 000 lines long and most of the main developers are members of Caramba. Over the evaluation period, efforts have been put on efficiency, code quality, scalability, and improving of the discrete logarithm support. The factorization part is now mature and stable, so that the number of external users (number theorists, cryptographers, or factoring enthusiasts) is constantly increasing.

Arithmetic libraries. (Caramba) We develop and maintain libraries for various arithmetic building blocks. The GNU MPFR (url) and GNU MPC (url) are mature projects that provide multiprecision floating point arithmetic with correct rounding up to the last bit. Due to the fact that they are both required to compile GCC, these libraries enjoy a very high visibility.

Belenios (Caramba) is an open-source private and verifiable electronic-voting protocol (url), that we develop in collaboration with the PESTO team (Dpt. 2). Our system is an evolution of an existing system, Helios, developed by Ben Adida, and used e.g., by UCL and the IACR association in real elections. The main differences with Helios are that the list of voters is not publicly exposed and the server hosting the ballot box cannot add ballots (so the server does not have to be trusted). Belenios has been eperimented in real-life "local" elections (e.g., "Comité de Centre" of Inria Rennes; head of the "groupes de travail C2 et calcul formel" of the GDR-IM.)

Isotop (Vegas) plots plane algebraic curves in a certified way, that is without missing connected components, self-intersections, etc. (url). Isotop 2 (2013) is faster than its contenders although timing ratios depend substantially on instances. Isotop 3, which is still in development, is drastically faster than Isotop 2.

Academic reputation and appeal

7 Prizes and Distinctions

Best papers

- Best paper award at Eurocrypt 2014 for our *heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic* [251]. This result was also much commented in the blogosphere.
- Best Paper Award at the ACM CCS 2015 for our work on the Logjam attack [244] and Pwnie award in the category "Most innovative research" during the BlackHat 2015 conference. This also received a large media coverage (especially in the USA).
- Best Paper Award at Asiacrypt 2011 for *Counting Points on Genus 2 Curves* [261].
- J. Computers and Geosciences best 2014 article award for *Automatic surface remeshing of 3D structural models at specified resolution: A method based on Voronoi diagrams* [155].
- Best paper honourable mention at ISMAR 2013 for *Image-guided Simulation of Heterogeneous Tissue Deformation For Augmented Reality during Hepatic Surgery* [328].
- Lasting Impact Award at ISMAR 2013 for *Markerless Tracking using Planar Structures in the Scene*.[SFZ00]
- Best paper award at SoCG 2012 for *Multinerves and Helly Numbers of Acyclic Families* [410] and also published in Advances in mathematics [388].
- Best paper honorable mention at Computer Graphics Forum 2015 for *3D Fabrication of 2D Mechanisms* [132].
- Best demonstration award at DGCI'13 for the TKDetection software [71] (url).

Distinctions

- R. Barbulescu received the "Prix de thèse Le Monde" in 2013 [208].
- A. Krähenbühl received the "Prix de thèse de la Région Lorraine" in 2014 [60].
- B. Levy reveiced the Inria young researcher award in 2011.
- B. Levy and S. Lefebvre received 4 ERC grants (2 starting grants and 2 Proofs of Concept).
- E. Thomé receieved the "prix régional du chercheur" by Région Lorraine.
- P. Gaudry, A. Kruppa, E. Thomé, and P. Zimmermann were awarded the "Prix La Recherche" in 2012 for a factorisation of a 768-bit RSA modulus.

[SFZ00] Gilles Simon, Andrew W. Fitzgibbon, and Andrew Zisserman. Markerless Tracking using Planar Structures in the Scene. In *Proc. International Symposium on Augmented Reality*, pages 120 – 128, 2000.

Invited talks Department members were invited speakers at 16 international and 8 national events. We were also invited to about 10 invitation-only workshops such as Dagstuhl, Bellairs, Banff and Oberwolfach workshops.

8 Editorial and organizational activities

Program and Paper Committees. Department members participated to the PCs of most major conferences in our fields and in particular, SIGGRAPH, SIGGRAPH ASIA, SGP and Eurographics in computer graphics, Eurocrypt and Asiacrypt in Cryptology, ISSAC in computer algebra, SoCG in computational geometry, DGCI and IWCIA in discrete geometry, ISMAR, ICPR, ICRA and MICCAI in vision and Medical Imaging and NIPS and IJCAI in machine learning. Noticably, we also (co-)chaired Eurographics 2014, Pacific Graphics 2013, CAD Graphics 2013, Geometric Modelling and Processing 2016, RFIA 2014 and DGCI 2011.

Editorial responsibilities. Department members are editors of many of the main journals in our fields. In particular, JoCG, CGTA, IJCGA in computational geometry, IPOL in image processing, and, in computer graphics, ACM Transactions on Graphics, IEEE Transactions on Visualization and Computer Graphics, Graphical Models and Computer and Graphics.

Steering committees. We are member of the steering committees of several conferences: ESA in algorithmic, Elliptic Curve Cryptography and ANTS in cryptography and number theory, and DGCI in discrete geometry. We are also in the steering committee for the colocation of STOC and SoCG in 2016.

Workshop organizations. Our department regularly organizes various workshops with, in particular, 11 international workshops and 4 French ones during the evaluation period.

9 Services as expert or evaluator

Thesis and habilitation committees, Hiring committees. We participated to 99 PhD and Habilitation committees including 53 as external examiners (but excluding those as advisor). We also served in 18 hiring committees outside Nancy and 14 in Nancy (4 of which as president).

Non-local scientific responsibilities. We served in the following commitees and panel: HCERES visiting commitee for LABRI (Bordeaux), LITIS (Rouen) and LTSI (Rennes). Coordination of one of the INRIA scientific evaluations. *Conseil scientifique* of the INS2I CNRS institute. Chairwoman of the *Association Française pour la reconnaissance et l'interprétation des formes.* Inria evaluation committee. *Commission Pédagogique Nationale* Infocom/SRC. Chairman of the INRIA COST- GTRI committee. Scientific Board of the *Société Informatique de France* (SIF). Chairwoman of the steering committee of the flagship international conference in computational geometry (SoCG).

Local scientific responsibilities. We serve in many local committes. The main responsibilities we had/have are: LORIA deputy head (2 years). Inria deputy head (6 years). Head of the Inria hiring committee for PhD and postdoc positions (6 years). Director of the Department *Services et réseaux de communication* of IUT Charlemagne (1 year).

10 Collaborations

We have a large set of collaborators with 136 co-authors within France and 130 abroad over the evaluation period. Among our formal collaborations, we have an Inria Associate Team with Hong-Kong University (url) and, through our 9 ANR and others PEPS and Inria Exploratory Project, we have formal collaborations with many groups in France (Sophia-Antipolis, Poitiers, Paris, Nantes, Montpellier, Bordeaux, Rennes, Lyon). Of course, we also have many collaborations that are not formalized but that are nevertheless fruitfull.

Through our various collaborations, we co-supervised 7 PhDs students with other labs in Nancy-Metz (in CRAN, IECL, Supélec, Geology School), 5 others in France (in Paris 6, Nantes, Lille) and 5 abroad in Calgary (Canada), Eindhoven (The Netherlands), Oran (Algérie) and Zinguinchor (Sénégal).

Finally, we mention two interesting inter-disciplinary collaborations. We built strong collaborations around **Augmented Reality applications in the medical field** with **Nancy University Hospital** (CHU), **GE Healthcare** [365, 316, 317] and with the MIMESIS Inria team which is part of part of **Strasbourg University Hospital** (IHU) [347, 348, 336, 329, 326, 298]. These collaborations are critical to have clinically validated algorithms and solutions.

We also built a collaboration with **INRA** (near Nancy) on **image processing applications** for the detection of wood knots in 3D CT images of wood trunks [60, 70, 90, 94, 72, 95, 75] and produced a sofware (url) which we validated in collaboration with them.

11 External support and funding

The main extenal funding of the department comes from 4 ERC grants (2 starting grants and 2 Proofs of Concept), 9 ANR projects (2 of which as coordinator, 2 projects within the CPER, 1 with the region Lorraine, and 2 contracts with compagnies (HTCS and Numalliance).

Involvement with social, economic and cultural environment

GOCAD is a consortium that regroups all the major companies in oil and gas industry. We have a long-term cooperation with the leader of this consortium, the School of Geology of Nancy. The consortium funded 5 of our Ph.D. theses during the evaluation period and 2 of these companies are in the process of acquiring a license for our sofware resulting from our Vorpaline ERC Proof of Concept. During the evaluation period, 3 of our co-advised Ph.D. student were hired by these companies right after their defense.

Cryptanalysis. Our work on integer factorization and discrete logarithm is of interest for governmental agencies and standardization bodies for tuning accurately their key size recommendations. Our work on the Logjam attack (see Section 7) had a direct real life impact: it was complemented by a *Common Vulnerabilities and Exposures* entry (CVE-2015-4000) and many software updates followed. Since 2012, we have a yearly-renewed contract with the **High Tech Communications Services (HTCS)** company on which we cannot say much due to confidentiality clauses.

E-voting. In connection with our work on the Belenios software and in collaboration with **Departement 2**, we have participated to two contracts (Voxaly in 2013 and Docapost in 2015), where we evaluated the e-voting solutions of the companies and proposed them directions for improvements.

Augmented reality. Through closed collaborations with the **Nancy University Hospital** (CHU), **Strasbourg University Hospital** (IHU) and **GE Healthcare**, we have promoted the use of AR and simulation in the clinical routine and the training of junior physicians to complex interventional clinical gestures in **neuroradiology and hepatic surgery**.

Popularization. We designed an inquiry-based **Augmented Reality** learning environment (AIBLE, url) for teaching and learning **astronomy in primary school** [319]. Department members are also *Chargé de Mission* for scientific popularization at Inria Nancy and member of committee for the *Olympiades de mathématiques.*

Involvement in training through research

Our department is involved in training of qualified personnel at different levels. First, we are naturally involved in the Master specialities of computer sciences at UL and also in several Engineering Schools (Mines Nancy, SUPELEC Metz, Geology School). Of course, our 13 faculty staff play a critical role there but several researchers also give courses.

As an example, we wish to emphasize the activity of M. Videau as the head of the engineering master's degree in "Services, security of systems and network" within the Master 2 in computer science in 2013–2014. She created then a bi-monthly joint seminar between LORIA and the Master which still is very successful in terms of attendance and that fosters the relations between the teaching at the master level and the research activities in the laboratory. The speakers are mostly from the industry or from governmental agencies with an emphasis on strong research and development profiles.

We also wish to emphasize that we submitted in 2016 an H2020 ITN project (with U. Louvain and the SIMULA compagny)

At a different level 3 department members are part of the board for computer science in the Doctoral school of Lorraine University, 3 are part of the hiring committee for PhD and postdoc positions at INRIA Nancy Grand Est (including the head of the committee) and 1 is the representative for Nancy of the Inria *Young researcher council* (url).

Apprentissage et Biologie Computationnelle (Machine Learning and Computational Biology)

Synopsis

1 Team Composition

Permanents

Yann Guermeur (DR CNRS), Fabien Lauer (MCF UL), Martine Cadot (PRAG UL, left 31/12/13), Fabienne Thomarat (MCF UL, left 31/10/13), Hoai An Le Thi (PR, "accueil en délégation CNRS" from 01/09/12 to 31/08/13).

	PR	MCF	PRAG	DR	CR	Total
2011		2	1		1	4
2016		1		1		2

Post-docs, and engineers

Emmanuel Didiot (engineer 09/2013–08/2015), Khadija Musayeva (engineer 10/2014–12/2014), Pedro Ernesto Garcia-Rodriguez (engineer 10/2015–01/2016).

Doctoral students

Hafida Bouziane-Chouarfia (Ass. Prof. USTO, Oran, 2008-11/2014), Rémi Bonidal (Région-FCH, 10/2009-06/2013), Le Van Luong (UL, 10/2010-09/2013), Mounia Hendel (Ass. Prof. USTO, Oran, 2010-...), Edouard Klein (Supélec, 03/2011-11/2013), Khadija Musayeva (UL, 11/2015-...), Aya El Dakdouki (funding from Lebanon, 12/2015-...).

Phd's defended	4	On-going PhD's	3

Team evolution

- In the period of interest, two permanent members left the team: Fabienne Thomarat now focuses on teaching and Martine Cadot moved to the Multispeech team.
- The team benefited from the presence of Hoai An Le Thi for one year in the framework of a ”délégation CNRS”.
- The switch from one CR to one DR corresponds to the change of status of Yann Guermeur, in October 2011.

2 Life of the team

Each year, the ABC research team organizes a scientific day. The talks are given both by invited speakers and by team members.

3 Research topics

Keywords

Statistical learning theory, computational biology, pattern recognition, regression, kernel methods

Research area and main goals

The aim of the ABC (”Apprentissage et Biologie Computationnelle”, i.e., Machine Learning and Computational Biology) team is to develop the theory and practice of supervised and unsupervised learning. We focus on the theory of multi-class pattern recognition, deriving uniform convergence results which primarily deal with margin classifiers such as multi-class support vector machines (M-SVMs) [14, 11]. Our applications are in the field of biological sequence processing. A specificity of the team is its interdisciplinarity. Basically, our contributions belong to three fields: machine learning, bioinformatics and statistics.

4 Main Achievements

Our main achievements correspond to contributions in machine learning bridging the gap between theory and practice. The best example is provided by Rémi Bonidal’s thesis [1, 6]. This work, dealing with model selection for bi-class and multi-class SVMs, introduced efficient methods whose objective functions are upper bounds on the cross-validation error.

5 Research activities

Theory of multi-class discrimination

Description In the framework of agnostic learning, one of the main open problems of the theory of multi-category pattern classification is the characterization of the way the complexity varies with the number C of categories. More precisely, if the classifier is characterized only through minimal learnability/measurability hypotheses, then the optimal dependency on C that an upper bound on the probability of error should exhibit is unknown. This question is to be studied in connection with that of the convergence rate, i.e., the way the control term of the guaranteed risk decreases with the sample size m.

Main results For classifiers whose classes of component functions are uniform Glivenko-Cantelli classes [DGZ91], we have established a guaranteed risk whose control term grows as the square root of C, for a convergence rate optimal up to a logarithmic factor [12]. This result is based on the uniform convergence norm. We then derived a guaranteed risk based on the L_2-norm. The main contribution of this work is an upper bound on the Rademacher complexity of interest growing sublinearly with C. This result holds for all behavior of the fat-shattering dimensions of the classes of component functions.

Switching and piecewise regression

Description Regarding regression, we focus on switching and piecewise regression problems, where the aim is to learn a collection of models without the a priori knowledge of the assignment of the data to each model. These problems are in particular encountered in the subfield of automatic control known as hybrid system identification.

Main results Our main results on switching and piecewise regression concern on the one hand efficient heuristic methods that can deal with larger problems than the previous ones [13, 16, 24, 19, 39] and on the other hand, the analysis of the complexity of these problems [17, 18].

Sparse and nonconvex optimization

Description Optimization is with statistics one of the applied maths subfields most relevant to machine learning. In particular, we focus on sparse optimization problems related to compressive sensing, in which the number of nonzero variables is minimized, and the difference of convex functions (DC) programming approach to nonconvex optimization.

Main results In [20] we proposed and analyzed a new reweighting scheme to recover the sparsest solution of a linear system, with better performance than the state of the art [CWB08]. In [15], we considered the nonlinear setting of recovering the sparsest solution of a system of polynomial equations and proposed and analyzed a set of group-sparsity based methods.

Nonconvex optimization based on DC programming was investigated for classication purposes in [22] and [8].

Nonconvex optimization algorithms were also developed with computational efficicency in mind for specific clustering problems: in [23], for Minimum Sum-of-Squares Clustering, in [21] for block clustering.

Robust data mining

Description Data mining consists in applying algorithms for producing models over the data. Robust Data Mining consists in not doing any hypothesis about the data, such as normality, etc.; on the contrary, we use the principles of inferential statistics (randomization tests, cross-validation…) so as to guarantee the generalization capabilities of the discovered models.

[DGZ91] R.M. Dudley, E. Giné, and J. Zinn. Uniform and universal Glivenko-Cantelli classes. *Journal of Theoretical Probability*, 4(3):485–510, 1991.

[CWB08] E. J. Candès, M. B. Wakin, and S. P. Boyd. Enhancing sparsity by reweighted ℓ_1 minimization. *Journal of Fourier Analysis and Applications*, 14(5):877–905, 2008.

Main results A line of thought on extracting models from data was initiated in [55], by analyzing how the ASI (Analyse Statistique Implicative) produces a set of rules for causal reasoning. We used a 3-way data factorization method for cineradiographic data [46], which highlighted the importance of taking into account the relationships of level higher than 2 between variables.

Biological sequence segmentation

Description We are interested in problems of bioinformatics which can be stated as follows: given a biological sequence and a finite set of categories, split the sequence into consecutive segments each assigned to a category different from those of the previous and next segments. Many problems of central importance in biology fit in this framework, such as protein secondary structure prediction, solvent accessibility prediction, splice site / alternative splicing prediction or the search for the genes of non-coding RNAs, to name just a few. Our aim is to devise a global solution for the whole class of these problems. On the one hand, it should be generic enough to allow a fast implementation on any instance. On the other hand, it should be flexible enough to make it possible to incorporate efficiently the knowledge available for a specific problem, so as to obtain state-of-the-art performance.

Main results The solution advocated by the ABC team is based on a hybrid architecture that combines discriminative and generative models in the framework of a modular and hierarchical approach. It was first assessed for protein secondary structure prediction [33, 43]. This gave birth to the MSVMpred2 prediction server, maintained by Fabienne Thomarat. In [56], we introduce the latest version of the application. It is evaluated on one specific task: protein secondary structure prediction. For this task, the use of input data derived from two types of position-specific scoring matrices (PSSMs) is investigated in [59]. The fusion of knowledge sources induces a gain in prediction accuracy which is statistically significant.

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis			3	1			4
Journal	5	3	5	4	2	1	20
Conference proceedings	7	6	12	1	1		27
Book chapter		1	2			1	4

List of top journals in which we have published
Journal of Machine Learning Research (1) [14]
Automatica (3) [13, 17, 18]
IEEE Transactions on Automatic Control (2) [20, 24]
Journal of Global Optimization (2) [15, 22]
Pattern Recognition (1) [23]
Neural Computation (1) [21]

List of top conferences in which we have published

Pattern Recognition in Bioinformatics (2) [33, 43]
IEEE Conference on Decision and Control (1) [37]
American Control Conference (2) [40, 27]
ACM/IEEE International Conference on Hybrid systems: computation and control (1) [39]

7 Software

Our main software products are: MSVMpack [14] for multi-class discrimination (with more than 5000 downloads over the last 5 years), MSVMpred2 for biological sequence segmentation and MLweb for machine learning on the web (with more than 600 downloads in 5 months).

Academic reputation and appeal

The ABC research team belonged to the ”Pattern Analysis, Statistical Modelling and Computational Learning” (PASCAL 2) network of excellence until its end in February 2013.

8 Prizes and Distinctions

Le Thi Hoai An was an invited speaker at EURO-INFORMS Joint International Meeting on Operational Research, Rome July 1-4, 2013. She gave a talk entitled ”Difference of convex functions optimization”. She was also an invited speaker of the International Scientific School on Knowledge Management 2012, Quang Binh University (Viet nam), 25-26 Nov. 2012.

9 Editorial and organizational activities

Yann Guermeur has been a member of the program committee of the following conferences: Thirtieth Annual Conference on Neural Information Processing Systems (NIPS 30) in 2016, BIOKDD in 2016, the ”conférence conjointe francophone AAFD & SFC” in 2016, International Joint Conference on Artificial Intelligence (IJCAI) in 2015, ”Modelling, Computation and Optimization in Information Systems and Management Sciences” (MCO) in 2015, ”European Conference on Artificial Intelligence” (ECAI) in 2014, ”IAPR International Conference on Pattern Recognition in Bioinformatics” (PRIB) in 2014, the ”6èmes Journées de la sociéte française de chémoinformatique” (SFCi) in 2013, the ”Stochastic Modeling Techniques and Data Analysis International Conference” (SMTDA) in 2012, and the ”Conférence Francophone sur l’Apprentissage Automatique” (CAp) from 2012 to 2014 and in 2016.

Hoai An Le Thi is a member of Editorial Board of 5 journals: Transactions on Computational Collective Intelligence (Springer), Journal of Optimization: Theory, Methods and Applications (GIP), Journal of Advanced Research in Computer Science (IASR), International Journal of Economics and Management Engineering, Vietnam Journal of Computer Science (a new journal in Springer). She is the editor of the special issue ”Optimization and Learning”, International Journal of Intelligent Information and Database Systems (IJIIDS), 2012.

10 Services as expert or evaluator

Yann Guermeur is an expert for the ANR and was, over the period of interest, a member of 8 PhD committees (6 of which as a referee) and one HDR committee. In 2015, he was the member of two ”comités de sélection”, one at the Université de technologie de Compiègne (UTC), the other one at the

INSA of Rouen. He also served as an outside reviewer for a promotion to Associate Professor with tenure at the University of Central Florida (UCF).

11 Collaborations

Yann Guermeur worked with F. Abdat and W. Blondel (CRAN, UL) on multi-class classification of skin pre-cancerous stages based on bimodal spectroscopic features [5, 25].

A collaboration with M. Geist (Supélec Metz) and O. Pietquin (Lille University) dealing with the connections between reinforcement learning and multi-category classification was established during the PhD of E. Klein [51].

Fabien Lauer worked with Henrik Ohlsson (University of Berkeley) on sparse optimization and non-linear compressive sensing [15, 58].

Fabien Lauer also pursued a collaboration with G. Bloch (CRAN, UL) on switching regression [13], including the co-supervision of the thesis of L. Van Luong [20, 19, 39, 27]. Some of these works were also conducted in collaboration with L. Bako (Ecole Centrale de Lyon) [39, 27] and René Vidal (Johns Hopkins University) [13].

12 External support and funding

The APPAT project (Machine learning for everyone everywhere) led by F. Lauer was supported by the ”valorisation non économique” (non-economical transfer) program of the University of Lorraine.

The A3SB project (Statistical learning for biological sequence segmentation) was funded by the CNRS for 30 months.

The operation ”Apprentissage statistique pour le traitement des problèmes de Discrimination sur les Séquences Biologiques” (ADiSBio) was funded until the end of 2013 by the thema ”Modélisation des Biomolécules et de leurs Interactions” (MBI) of the CPER ”Modélisations, Informations et Systèmes Numériques” (MISN).

Involvement with social, economic and cultural environment

The APPAT project intends to disseminate machine learning knowledge and tools towards a general audience.

Involvement in training through research

Martine Cadot is PRAG in the Department of Computer Science at the UL where she teaches statistics and data mining to master (M2P) students. She has been the advisor of many internships.

Fabien Lauer is Associate Professor in the Department of Computer Science at the UL where he teaches machine learning to master (M1) students.

Fabienne Thomarat is Associate Professor at the Ecole Nationale Supérieure des Mines de Nancy / UL (engineering school, master of engineering school). She is in charge of the option bioinformatics at the Department of Computer Science.

Applying Discrete Algorithms to Genomics and Imagery

Synopsis

1 Team Composition

Permanents

Isabelle Debled-Rennesson (PR UL), Eric Domenjoud (CR CNRS), Philippe Even (PR UL), Damien Jamet (MCF UL, left 1/3/2012), Bertrand Kerautret (MCF UL), Phuc Ngo (MCF UL, arrived 1/9/2014).

	PR	MCF	DR	CR	Total
2011	1	3		1	5
2016	2	2		1	5

Post-docs, and engineers

Adrien Krähenbühl (Post-doc, ATER UL, 09/2014 to 09/2015), Hervé Locteau (engineer 11/2012 to 2/2013).

Doctoral students

Adrien Krähenbühl (Doctoral contract, sept 2011- dec 2014), Nicolas Aubry (CIFRE contract with Numalliance, oct 2013-...), Hayat Nasser (Erasmus doctoral contract, dec 2013-...).

Phd's defended	1	On-going PhD's	2

Team evolution

In 2011, M. Margenstern (LITA, Metz) was in CNRS delegation and he spent time in our team. In 2014, P. Ngo was recruited at the Lorraine University and she has joined our team.

2 Life of the team

Since 2011, the application area of our team has been focused on Imagery and we haven't any application in genomics. Therefore, we wish to change the name of our team : **ADAGIo - Applying Discrete Algorithms to Geometry and Imagery**.
Members have regularly meetings to discuss about the life of the team (projects, arrivals of new persons, missions, publications, equipment purchase) and to present their research work.

3 Research topics

Keywords

Discrete Geometry, Algorithms, Discrete Structures, Word Combinatorics, Image Analysis.

Research area and main goals

The general research area of our team is *discrete algorithms*. Constructing a discrete model of a real-world phenomenon means, in mathematical terms, representing it through a *discrete structure*, such as graphs, words, trees, sets of points in a space, etc.

In order to develop efficient algorithms on discrete structures and to analyze and optimize those algorithms, we have to understand thoroughly the properties of the underlying structures. These properties can be *geometrical*, *arithmetical* or *combinatorial* depending on the situation. The study of these properties is the main objective of our team.

To be more specific, we are mainly interested in the fundamental study within the area of *Discrete Geometry* of discrete objects having a geometric (planar or spatial) interpretation. The general goal of *Discrete Geometry* is to define a theoretical framework to translate to $\mathbb{Z}^n$ basic notions of the Euclidean geometry (such as distance, length, convexity, ...) as "faithfully" as possible. Several approaches exist to pursue this goal [CM91]. In our studies, we follow an arithmetical approach, where discrete objects, such as straight lines or planes, are defined with arithmetical definitions. These analytical definitions allow us to represent in a compact way any elementary digital object, to study some objects that are intrinsically discrete (and are not only approximations of continuous objects), and to define infinite discrete objects.

The study of the properties of discrete objects such as straight lines, circles, planes, curves and discrete surfaces always remains a topical subject in the last leading conferences of the domain (DGCI and IWCIA). These topics are studied by our team and more particularly the study of noisy discrete curves and surfaces. Our aim is to determine, in the framework of discrete geometry, a paradigm adapted to these objects, taking into account the noise associated with acquisition tools and methods.

Other points of interest of our team are the areas of *Text Algorithm and Words Combinatorics* which have been very actively developed for the last years, as witnessed by the publication of several monographs [Gus97,CHL01]. On the one hand, Sturmian words are well known to code the digitization of lines with irrational slopes. One of our main subject of interest is the study of *natural* extensions of such sequences in any dimension in order to code arithmetical discrete hyperplanes of any dimension. On the other hand, we focus on the introduction of relevant tools for such objects, such as multidimensional substitutions which have links with many other theories, such as number theory, topology or formal language theory.

Our algorithms are naturally used in the application area of Imagery.

[CM91] J-M. Chassery and A. Montanvert. *Géométrie discrète en imagerie*. Hermès, Paris, 1991.

[Gus97] D. Gusfield. *Algorithms on Strings, Trees, and Sequences*. Cambridge University Press, 1997.

[CHL01] M. Crochemore, C. Hancart, and T. Lecroq. *Algorithmique du texte*. Vuibert Informatique, 2001.

4 Main Achievements

Since 2011, four important facts have oriented the research activities of ADAGIo team:
1. In the area of discrete object study, we obtained a complete caracterisation of the facet connectedness of discrete hyperplanes with zero intercept as well as a general procedure for computing the connecting thickness. This problem had been under investigation for several years.
2. The work about detection of noise level in contours of discrete objects opens new research perspectives and permits to solve problems in Image Analysis area.
3. The collaboration with INRA, through a PhD thesis, was very interesting and fruitful (numerous publications in computer science and biology, a software, a prize). We continue to collaborate on several subjects in relation with Image Analysis.
4. An industrial company was interested by our approaches and methods. The collaboration started through a CIFRE PhD thesis.

5 Research activities

Discrete primitives and word combinatorics

Description

Among the basic primitives available in geometry, we can find digital straight line segments. We focus on the arithmetical viewpoint, introduced by Jean-Pierre Reveillès [Rev91]. In this framework, a **digital straight line** is the set of points with coordinates (x, y) of $\mathbb{Z}^2$ verifying the double diophantine inequality $\mu \leqslant ax - by < \mu + \omega$, with a, b, μ, ω integer. The notion of ***arithmetic discrete hyperplanes*** is a generalization in $\mathbb{Z}^d$ of this notion.

Words combinatorics provides many powerful tools for the study of discrete objects such as lines or planes. Such objects have natural encodings as finite or infinite words on finite alphabets. For instance, a discrete line is encoded as a balanced word over the alphabet $\{0, 1\}$ and a discrete plane may be encoded as a 2-dimensional word over the alphabet $\{0, 1\}$. We use tools from words combinatorics to count some patterns in these objects or to study some global properties such as the connectivity.

Main results

Connectivity of arithmetic discrete hyperplanes

A discrete hyperplane in $\mathbb{Z}^d$ is defined as the set of integral points between two parallel hyperplanes in $\mathbb{R}^d$. More formally, given a non-zero *normal vector* v, a thickness $\omega \in \mathbb{R}$ and a *shift* $\mu \in \mathbb{R}$, the hyperplane $\mathbb{P}(v, \omega, \mu)$ is the set of points x in $\mathbb{Z}^d$ satisfying the double inequality $0 \leqslant \langle v, x\rangle + \mu < \omega$ where $\langle ., .\rangle$ denotes the usual scalar product in $\mathbb{R}^d$. We are interested in the $(d-1)$-connectedness (also called facet-connectedness) of this hyperplane. Two integral points x and y are $(d-1)$-neighbours if and only if $x - y = \pm e_i$ where $(e_1, \ldots, e_d)$ is the canonical basis of $\mathbb{R}^d$. A subset S of $\mathbb{Z}^d$ is $(d-1)$-connected if and only if for any two distinct points x and y in S, there exists in S a $(d-1)$-path from x to y.

There exists a critical thickness $\Omega(v, \mu)$, called the *connecting thickness of v with shift μ*, such that $\mathbb{P}(v, \omega, \mu)$ is disconnected for all $\omega < \Omega(v, \mu)$ and connected for all $\omega > \Omega(v, \mu)$[DJT09]. We have described a general procedure for computing $\Omega(v, \mu)$, which almost always terminates, unless v belongs to some fractal set K_d. Kraaikamp & Meester[KM95] have shown that the Lebesgue measure of this set is

[Rev91] J-P. Reveillès. *Géométrie discrète, calculs en nombre entiers et algorithmique*. Thèse d'état, Université Louis Pasteur, Strasbourg, 1991.

[DJT09] E. Domenjoud, D. Jamet, and J-L. Toutant. On the connecting thickness of arithmetical discrete planes. In *proc. of 15th DGCI*, volume 5810 of *LNCS*, Montréal, Canada, October 2009.

[KM95] C. Kraaikamp and R. Meester. Ergodic properties of a dynamical system arising from percolation theory. *Ergodic Theory and Dynamical Systems*, 15(04):653–661, 1995.

zero. When the procedure does not terminate, we know however that $\Omega(v,\mu) = \|v\|/(d-1)$.

We have studied the connectedness of $\mathbb{P}(v,\omega,\mu)$ at this critical thickness, which means the connectedness of $\mathbb{P}(v,\Omega(v,\mu),\mu)$. We have first proven [61] that $\mathbb{P}(v,\Omega(v,0),0)$ is connected if $v = (1, 1+\alpha, 1+\alpha+\alpha^2)$ where α is the real root of X^3+X^2+X-1.

To study the general case, we have described [66] an incremental construction of $\mathbb{P}(v,\Omega(v,\mu),\mu)$. This construction, called *geometric palindromic closure* is directed by an infinite word $\Delta \in \{1,\ldots,d\}^{\mathbb{Z}}$ which describes the behaviour of the algorithm computing the connecting thickness. It generalises in higher dimensions the iterated palindromic closure on words with two letters. In particular, it provides a generalisation of Justin's formula[DJP01].

Using this construction, we have shown [83, 82] that $\mathbb{P}(v,\Omega(v,\mu),\mu)$ is almost always disconnected, unless v belongs to the fractal set K_d. In this case, $\Omega(v,\mu)$ does not depend on μ and $\mathbb{P}(v,\Omega(v),\mu)$ may be connected or not according to the value of μ. In particular, $\mathbb{P}(v,\Omega(v),0)$ is connected while $\mathbb{P}(v,\Omega(v),\Omega(v))$ is disconnected.

We also have studied more deeply the properties of the objects generated by the geometric palindromic closure. They are finite subsets of $\mathbb{Z}^d$ with a tree structure where vertices are points of $\mathbb{Z}^d$ and edges represent the adjacency relation. Each edge is labeled with the direction in which the ends of this edge are neighbours. Doing so, each path in the tree may be encoded as a word on $\{1,\ldots,d\}^\star$. We have shown [65] that this encoding is non-ambiguous in the sense that it allows to rebuild entirely the geometry of the path. We have also shown that the language of all paths of a given object is rich in the sense that it contains exactly as many palindromes as the numbers of vertices in the object.

Recognition of parallel strip in gray level image

Most of the available tools developed in digital geometry adress binary images. Some of them take noise into account through the concept of blurred primitives. The blurred segments[DRFRD06] are based on thick digital straight line segments. An extension of a blurred segment recognition algorithm was proposed to process gray level images by using image gradient information[KE]. In the continuity of this previous approach, we have proposed an algorithm of parallel strip segment recognition [77]. Instead of using classical image gradient information, the proposed algorithm relies on the comparison of image intensity profiles. Such strategy is robust to detect tubular objects composed of specular material and was exploited in industrial collaboration given in a CIFRE PhD thesis.

Discrete lines and cellular automata

In 2011, the CNRS delegation of Maurice Margenstern permitted a collaboration and we looked at the possibility to implement algorithms of discrete geometry in cellular automata. We focused on the construction of discrete lines. It turns out that such an implementation is feasible [80, 63].

Combinatorial structure of digital rigid transformation

Rigid transformations are involved in many digital image processing tasks, in which such transformations are usually performed on $\mathbb{R}^n$, and followed by a digitization process to produce digital transformed images in $\mathbb{Z}^n$. In [NKPT13][73], we have proposed to study rigid transformations on $\mathbb{Z}^2$ as fully discrete processes. In particular, we have investigated a combinatorial structure, namely *discrete rigid transfor-*

[DJP01] X. Droubay, J. Justin, and G. Pirillo. Episturmian words and some constructions of de Luca and Rauzy. *Theoret. Comput. Sci.*, 255:539–553, 2001.

[DRFRD06] I. Debled-Rennesson, F. Feschet, and J. Rouyer-Degli. Optimal blurred segments decomposition of noisy shapes in linear time. *Computers & Graphics*, 30(1):30–36, 2006.

[KE] B. Kerautret and Ph. Even. Blurred Segments in Gray Level Images for Interactive Line Extraction. In *Proc. of IWCIA 2009*, volume 5852 of *LNCS*, pages 176–186.

[NKPT13] P. Ngo, Y. Kenmochi, N. Passat, and H. Talbot. Combinatorial structure of rigid transformations in 2D digital images. *Computer Vision and Image Understanding*, 117:393–408, 2013.

mation graph, modelling the whole space of digital rigid transformations. Such a structure is applied in [84] to solve image registration problems.

Analysis of Discrete Objects

Description The study of arithmetical, geometrical and combinatorial properties of the discrete primitives is crucial to obtain efficient algorithms (recognition, scanning, ...) and to extract geometrical parameters (perimeter, curvature, normal vector, area, ...) on the curves and surfaces. We used in this part the obtained recognition algorithms of discrete primitives such as digital straight line segments, blurred segments [DRFRD06], pieces of blurred digital planes, ... The principal idea, used in several of the presented works, is to decompose a discrete curve (or surface) in a sequence of maximal primitives, it permits to obtain a significant information about the structure of the studied curve or surface.

We then develop new tools to analyse discrete objects and to reconstruct some continuous representations of them. Two main axes can be distinguished:

- the ***multi-resolution analysis*** of discrete curves and surfaces provides progressive analysis and new information. This analysis is useful for the comparison, the classification or the simplification;
- the ***reconstruction of geometrical models*** with a controlled precision with respect to the original discrete curves or surfaces opens perspectives for the use of a post-processing task based on Euclidean geometry.

From these approaches, several applications are deduced.

Main results

Noise detection

We address the problem of noise detection in discrete contours (curves). For this purpose we have defined an unsupervised approach to measure the **meaningful scale** of a discrete contour by exploiting the asymptomatic properties of maximal straight line segments [68, 69]. The application of this detection permits to remove the parameter, associated to the detected level of noise, as for instance for circle arc detection [NKDRL] or for automatic polygonalization [76]. This concept of meaningful scale was extended to the definition of **meaningful thickness** in relation with the width parameter of the blurred segments [88]. This result can be useful both to process not only connected digital contours but also sequences of points with floating coordinates.

Dominant Point Detection

We proposed a new and fast method for dominant point detection and polygonal representation of a discrete curve [74]. For a given width, the dominant points of a curve C are deduced from the sequence of maximal blurred segments of C. Comparisons with other methods of the literature prove the efficiency of this approach. However, an heuristic strategy is used to identify the dominant points. We proposed in [97] a modified algorithm without heuristics but with a simple measure of angle. In addition, an application of polygonal simplification is as well proposed to reduce the number of detected dominant points by associating a weight to each of them.

From this work, we propose a new notion, named Adaptive Tangential Cover, to study noisy digital contours. It relies on the meaningful thickness, calculated at each point of the contour, which permits to

[DRFRD06] I. Debled-Rennesson, F. Feschet, and J. Rouyer-Degli. Optimal blurred segments decomposition of noisy shapes in linear time. *Computers & Graphics*, 30(1):30–36, 2006.

[NKDRL] T. Ph. Nguyen, B. Kerautret, I. Debled-Rennesson, and J.-O. Lachaud. Unsupervised, Fast and Precise Recognition of Digital Arcs in Noisy Images. In *Proc. of ICCVG 2010*.

locally estimate the noise level. The Adaptive Tangential Cover is then composed of maximal blurred segments with appropriate widths, deduced from the noise level estimation. We present a parameter-free algorithm for computing the Adaptive Tangential Cover (ATC) [96].

Arc and segment detection - reconstruction
We propose a linear algorithm for the detection of digital arcs and digital circles [98]. This method uses an original representation of digital arcs and digital circles[LL00], we transform the problem of digital arc recognition into a problem of digital straigth line recognition. We then deduce an algorithm to decompose a curve into arcs and straight line segments [99] in $O(n \log n)$ time. A reconstruction of the initial curve is also proposed.

Center line extraction from 3D shapes and representation
In the framework of the industrial collaboration with the Numalliance company, we have studied a new method to analyse the shape of tubular objects [85]. The proposed method is based on surface normal accumulation and is able to extract a center line from various data types (from digital surface to 3d mesh of full or partial scan). From this center line we extend the previous method of arc/segment detection in 3d.

Knot detection and measurements on wood images from X-Ray CT scanners
This work is a collaboration with INRA, started in 2011 by master students and continued by A. Krähenbühl during his PhD thesis (defended in December 2014). It consists in studying 3D CT images of trunks in order to segment wood knots. To achieve this, several algorithms were developed using discrete geometry tools developed in our team (dominant point detector, curvature estimator, ...). Firstly, a detection method was proposed based on the analysis of accumulation of local intensity changes according to the main direction of the wood trunk [90, 91, 70]. Another segmentation approach was proposed, by generating slices tangent [75, 95, 92]. The proposed methods were tested and validated through the development of the TKDetection software[Krä14].

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis				1			1
Journal	2	4	2	5	1	2	16
Conference proceedings	6	7	3	4	6	1	27
Book or special issue (edited)	1	2		1			4

List of top journals in which we have published
Theoretical Computer Science (TCS) (2) [65, 67]
Discrete Applied Mathematics (DAM) (1) [64]
IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI) (1) [68]
Pattern Recognition (PR) (2) [74, 70]
Computer Vision and Image Understanding (CVIU) (1) [76]
Image Processing On Line (IPOL) (2) [69, 62]

List of top conferences in which we have published
International Conf. on Discrete Geometry for Computer Imagery (DGCI) (5) [82, 91, 84, 86, 102]
International Workshop on Combinatorial Image Analysis (IWCIA) (4) [97, 93, 77, 103]

[LL00] L.J. Latecki and R. Lakamper. Shape similarity measure based on correspondence of visual parts. *PAMI, IEEE Transactions on*, 22(10):1185–1190, Oct 2000.

[Krä14] A. Krähenbühl. https://github.com/adrien057/TKDetection/tags/, 2012-2014.

International Conf. on Image Analysis and Processing (ICIAP) (3) [85, 81, 101]
International Conf. on Computer Analysis of Images and Patterns (CAIP) (1) [98]
Scandinavian Conf. on Image Analysis (SCIA)(1) [99]
Reconnaissance de Formes et Intelligence Artificielle (RFIA) (3) [95, 100, 87]

7 Software

TKDetection
All the results related to the knot segmentation presented in section 5 were included in a main software ***TKDetection***[Krä14] which was a base to share and reproduce results in the framework of an active collaboration with INRA researchers.
DGtal library
Bertrand Kerautret belongs to the main development team of the open source library for Digital Geometry programming (`DGtal`). The main objective is to structure different developments from the digital geometry and topology community.
Image Processing On Line (IPOL): Partnership on Geometry
A new partnership with the IPOL journal and the LORIA has been proposed. IPOL is a research journal on image processing and image analysis, publishing algorithm description and source code with an online demonstration (`http://ipol.im`). The aim of this collaboration is to open the research domain of the journal to the topic of geometry and to facilitate/encourage journal submission on this field. This initiative was materialized by the purchase and the installation of a new specialized server to host geometry based demonstrations. It is hosted at LORIA by the ADAGIo team (`http://ipol-geometry.loria.fr/~kerautre/ipol_demo/`).

Academic reputation and appeal

8 Prizes and Distinctions

During the 17th IAPR International Conference on Discrete Geometry for Computer Imagery (DGCI'13), members of the team won the ***best demonstration award*** for the TKDetection software [71] (`http://dgci2013.us.es/bestDemo.php`).
A. Krähenbühl won in 2014 the ***prize of the Lorraine region*** for his PhD thesis.
B. Kerautret received the "Symposium on Geometry Processing Software Award 2016" as main contributor of the DGtal Library[1].
Invited talks: a tutorial talk at IWCIA (Nov. 2015, India), an invited talk on the KIDOCO ANR meeting (June 2015) and on the DigitalSnow ANR meeting (July 2015).

9 Editorial and organizational activities

The ADAGIo team was in charge of the ***organisation of the 16th international DGCI conference*** that was held in Nancy from 6th to 8th April 2011 (LNCS proceedings [104]). Members of the team have supported the publication of three special issues in the DAM, CVIU and IPOL Journals [105, 106, 107]. Members of team participated to the organization of the following events:

[1] `http://awards.geometryprocessing.org/`

[Krä14] A. Krähenbühl. https://github.com/adrien057/TKDetection/tags/, 2012-2014.

The Mons Theoretical Computer Science Days which was held at Loria in September 2014 (around 80 participants). A special issue of RAIRO - Theoretical Informatics and Applications will be published.
Journées Informatiques et Géométries (JIG, nov. 2013, LORIA).
IPOL Tutorial at the national conference RFIA (Juin 2014 Rouen).
Members of ADAGIo team served as members of ***Steering Committee*** or ***Program Committee*** of international conferences (DGCI, IWCIA, ICPR, ICCVG, WPS-QCAV, CIARP), as member of the ***Editorial Board*** of international journal (IPOL). They also participated to the review process of the international journals: PAMI, JMIV, PR, PRL, CVIU, DAM, TCS, RAIRO-TIA.

10 Services as expert or evaluator

Members of ADAGIo team participated to 7 PhD committees and were reviewers in 2 jurys. They were also asked to evaluate ANR projects.
From September 2011 to August 2014, a team member has been an elected member of the *conseil scientifique* of the INS2I CNRS institute.

11 Collaborations

A. Vacavant (ISIT lab, Le Puy en Velay), T. Roussillon (LIRIS, Lyon): work on contour representation on irregular grid [76, 103].
J.-O. Lachaud (LAMA, Chambery): works related to noise estimators [68, 88, 69, 85, 86]
L. Vuillon, X. Provençal (LAMA, Chambéry), V. Berthé (LIAFA, Paris): work on digital hyperplanes [61, 83, 66, 82, 65].
D. Coeurjolly: work on the DGtal library and nD extraction of connected component [62].
M. Colom, N. Limare, P. Monasse, J-M. Morel (CMLA, Cachan): IPOL development [79].
L. Wendling (LIPADE, Paris) : applications in image analysis [81].
M. Margenstern (LITA, Metz) : discrete line segments and cellular automata [80, 63].
F. Longuetaud, F Mothe (INRA, Champenoux): work on the knot segmentation [60, 70, 90, 94, 72, 95, 75]
F. Feschet (IGCNC, Clermont): work on knot detection [93].
Y. Kenmochi (LIGM, Paris-Est): digital rigid transformations [73, 84].

12 External support and funding

In the framework of the CIFRE collaboration with the *Numalliance* company, our team received a grant during three years.

Involvement with social, economic and cultural environment

In September 2013, a new collaboration was initiated with the *Numalliance* company through a project related to the segmentation and the measure of metal pipe generated by machine tools. Nicolas Aubry started a PhD thesis on this topic with an ANRT grant.

Involvement in training through research

Our team is implied in the IPAC specialty of the computer science Master and more precisely in the modules *Initiation au Traitement d'Images et à la Vision* and *Description et Reconnaissance de Formes*. I. Debled-Rennesson is member of the committee for computer science in the Doctoral school IAEM of UL.

Geometry Processing and Additive Manufacturing

Synopsis

ALICE is a team that does research in *geometry processing* and in *additive manufacturing*. In geometry processing, ALICE develops algorithm to transform and optimize the geometric representations of 3D objects. The targeted applications are meshing for numerical simulation and 3D rendering. In additive manufacturing, ALICE develops algorithm for making 3D fabrication easy to use for a widest possible audience. In particular, they focus on easy generation of 3D content for casual users, and integrating physical constraints of fabrication into geometry processing tools.

1 Team Composition

Permanents

Laurent Alonso (CR Inria), Xavier Antoine (PR Mines Nancy, delegation Sept 2013 - Sept 2014) Dobrina Boltcheva (MCF), Xavier Cavin (CR Inria, “disponibilité”, CEO Scalable Graphics), Samuel Hornus (CR Inria), Bruno Jobard (MCF U. Pau, delegation, 09/11-06/12) Sylvain Lefebvre (CR Inria, HDR), Jean-Claude Paul (DR Inria, HDR, left in 2016 - retired), Bruno Lévy (DR Inria, HDR), Nicolas Ray (CR Inria), Dmitry Sokolov (MCF), Rhaleb Zayer (CR Inria, left since March. 2015 - “disponibilité” MPII Saarebruck)

	PR	MCF	DR	CR	Total
2011		3	2	6	11
2016		2	1	5	8

Post-docs, and engineers

Nicolas Bonneel (post-doc 09/11-09/12), Frederic Claux (engineer, 09/14-08/15), Shi Kanle (post-doc 12/11-12/13), Jonas Martines (post-doc, 04/2014-now), Tim Reiner (post-doc 03/15-now), Haichuan Song (post-doc, 09/15-now), Atsushi Suzuki (post-doc, 05/14-05/15), Lionel Unterreiner (post-doc 09/14-08/15), Thierry Valentin (engineer, 07/13-05/14),

Doctoral students

Arnaud Botella (Gocad consortium, 09/12-04/16), Nicolas Cherpeau (Gocad consortium, 10/08-04/12), Jeremie Dumas (ENS, 09/13-now), Patricio Galindo (ANR Chaire Excellence PHYSIGRAPHICS, 10/10-01/15), Jean Hergel (ERC StG SHAPEFORGE,09/13-now), Anass Lasram (ERC StG SHAPEFORGE, 10/09-12/12), Kun Liu (ANR Chaire Excellence PHYSIGRAPHICS, 09/10-12/15), Maxence Reberol (ERC StG SHAPEFORGE and Region Lorraine, 09/15-now), Julien Renaudau (CIFRE Schlumberger, 10/15-now), Romain Merland (Gocad consortium, 10/09-04/13), Vincent Nivoliers (ENS, 10/08-11/12) Jeanne Pellerin (Gocad consortium, 09/10-03/14),

Phd's defended	8	On-going PhD's	4

Team evolution

- Dobrina Boltcheva (Assistant Professor), hired 09/11. Specialities: computational geom.;
- Jean-Claude Paul (DR Inria), joined Tsinghua U. (China) in 2004. Came back in 2013 and was hosted by ALICE until 2016 when he retired;
- Xavier Antoine (prof. mathematics). Associated with ALICE ("delegation", for 1 years, Sept. 2013 - Sept. 2014), to develop some joined research projects (BECASIM);
- Bruno Jobard (Assistant Professor, U. Pau) joined us on a 1-year "deletation" position (09/11-06/12) to work on scientific visualization aspects;
- Rhaleb Zayer (CR Inria) went on "disponibilité" leave this year and joined MPII Saarebruck on a temporary position (for familly reasons);
- Xavier Cavin (CR Inria), on "disponibilité" leave, he created a startup *ScalableGraphics*.

Between 2005 and 2011 (previous evaluation period), the team has known a fast expansion, boosted by the European Research Council grant GOODSHAPE (1.1 M Euros) obtained by B. Lévy, and by 3 new Inria researchers (Sylvain Lefebvre, Rhaleb Zayer and Samuel Hornus) and 1 new associate professor (Dmitry Sokolov). The team reached a "critical mass" in 2010.

After this fast expansion, between 2011 and 2016 (this evaluation period), we hired (2011) a new associate professor (Dobrina Boltcheva) and we worked on structuring the team.

2 Life of the team

An important aspect was to prepare the emergence of new leaders within the team. Rhaleb Zayer advised two Ph.D. theses (Alejandro Galindo and Kun Liu, both defended), funded by his 300K Euros ANR "chaire d'excellence". Sylvain Lefebvre proposed to extend his "by-example" approach for designing textures to real fabricated 3D objects. He obtained an ERC grant (SHAPEFORGE, 1.3 M Euros) that allowed him to start hiring Ph.D. students. He defended his HdR in 2014 and is now ready to create a new team on additive manufacturing.

In the other research axis (geometry processing), our specificity is to "talk the same language" as the applied mathematics community, and bring new mathematical tools to the geometry processing community and vice-versa. We first started to publish in applied math. journals, then we continued digging the numerical analysis foundations deeper and deeper. Now we are shifting the center of gravity of this research axis more and more towards the mathematics community. We launched cooperative projects with mathematicians, with X. Antoine, math. prof., who joined the team on a "delegation" (2013-2014) and started the BECASIM ANR project on plasma physics. This year, we started an "Inria Explorative Project" with mathematicians working on Optimal Transport (Quentin Merigot, Jean-David Benamou, Yann Brenier), and we also proposed with them an ANR project (submitted, currently under evaluation).

3 Research topics

Geometry Processing – Keywords: *mesh generation, parameterization, optimal sampling, scientific computing* We study and develop new solutions to *transform and optimize geometric representations*. Our original approach to both issues is to restate the problems in terms of *numerical optimization*. We try to develop solutions that are *provably correct*, *scalable* and *numerically stable*. To reach these goals, our approach consists in transforming the geometric problem into a numerical optimization problem, studying the properties of the objective function and designing efficient minimization algorithms. Besides Computer Graphics, our goal is to develop cooperations with researchers and people from the industry, who experiment applications of our general solutions to various domains, comprising CAD, industrial design, oil exploration and plasma physics.

Additive Manufacturing – Keywords: *by-example generation, texture synthesis* Our goal is to make rapid manufacturing technology (i.e., "3D printing") usable by anyone, without requiring to master specific skills. The challenge we are tacking is to automatically produce new objects visually similar to a set of examples, while ensuring that the generated objects can enforce a specific purpose, such as supporting weight distributed in space, affording for seating space or allowing for light to go through. This properties are crucial for someone designing furniture, lamps, containers, stairs and many of the common objects surrounding us. The originality of our approach is to cast a new view on the problem of 'by–example' shape synthesis, formulating it as the joint optimization of 'by–example' objectives, semantic descriptions of the content, as well as structural and fabrication objectives.

4 Main Achievements

- **Additive Manufacturing** We developed a whole set of algorithms to make it easy to design complicated 3D shapes from examples, as well as techniques that take into account some combinations of physical constraints (constructibility, resistance, balance). Our originality is to discretize the shape to model *on the fly*, using dedicated data structures, optimized for GPU implementation. This makes it possible to manufacture objects with extremely complicated internal structure at a low memory cost;
- **Geometry Processing** We proposed new algorithms for sampling shapes under various conditions. Our sampling point of view results in algorithms that are very resistant to degeneracies in the input, making it possible to generate different types of meshes (anisotropic triangular meshes and hex-dominant meshes), that are very difficult to generate and important for some numerical simulations. We used also our methodology to design the first algorithm that computes optimal transport in 3D;

- **Potential societal/economic impact** Our results in both research axes stemming for our two ERC starting grand projects, that we made available through our prototype softwares, were both selected by the ERC for "pre-industrialization" grants.
- Bruno Lévy received the **Inria Young Researcher Award** in 2011

5 Research activities

Additive Manufacturing

We obtained several results on the modeling process for generating 3D objects, for controlling their topology [169] and for optimizing their rigidity and appearance [141, 144]. Considering physical constraints, we proposed algorithms for generating 3D objects with moving parts, such as mechanisms [132] (best paper honorable mention), and for creating inner cavities and inconspicuously deforming shapes to ensure that they are well balanced after fabrication [158].

Considering fabrication processes, we developed an algorithm that automatically generates "scaffoldings" for handling features that are overhanging during the fabrication [128].

We also improved tools path planning to avoid defects when fabricating multi-color objects with dual head printers, and developed an algorithm to generate protecting shields against oozing filaments during fabrication [131].

Geometry Processing

Structured meshes: We developed algorithms for structured meshing (quad dominant, hex dominant), and we made progresses on the problem of robustly tracing streamlines to generate the elements [159]. We also developed a volumetric parameterization method, based on dihedral angles [151], that may be used to design base domains for hexahedral meshing.

Unstructured meshes: We developed efficient algorithms for sampling surfaces and volumes embedded in arbitrary dimensions, which resulted in an anisotropic meshing algorithm [168, 148]. In a cooperation with the School of Geology, we developed applications to 3D meshing for oil exploration [155] (2015 journal's best paper award).

Optimal Transport: Since the optimal sampling problem that we studied (previous item) is similar to optimal transport, we were approached by mathematicians working on this topic and started meeting them on a regular basis. We developed the first numerical algorithm to compute L_2 semi-discrete Optimal Transport in 3D [138]. This is a fundamental component for solving a class of Partial Derivative Equations (those that involve the Monge Ampere operator). We started exploring this latter direction with mathematicians (Dauphine U. and Polytechnique) and launched an "Inria Explorative Project" in 2016;

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis		3	1	1	2	1	8
H.D.R				1			1
Journal	13	8	13	8	11		53
Conference proceedings	6	6	3	4	1		20
Book chapter				2			2
Book or special issue (edited)			1	1			2
Patent	1		3	1	1		6

List of top journals / conferences in which we have published

In Computer Graphics, all the proceedings of the top conferences are published as a special issue of a journal (SIGGRAPH and SIGGRAPH ASIA → ACM Transactions on Graphics, EUROGRAPHICS and ACM Symposium on Geometry Processing → Computer Graphics Forum).

- ACM Transactions on Graphics [130, 122, 143, 151, 158, 168, 159, 128, 141, 144, 129] (including 6 SIGGRAPH and 2 SIGGRAPH ASIA)
- Computer Graphics Forum [169, 142, 149, 150, 137, 132, 131] (including 5 EUROGRAPHICS and 2 ACM Symposium on Geometry Processing)
- IEEE Transactions on Visualization and Computer Graphics [161, 136]

- Computers and Graphics [145, 160, 167, 140]
- *Applied math. journals:* SIAM J. on Scientific Computing [125], ESAIM M2AN Mathematical Modeling and Analysis [138], J. of Computational and Applied Mathematics [148]

7 Software

Geogram-Vorpaline-Graphite *Geogram* is an open-source programming library with geometric algorithms. It implements classical data structures and algorithms, as well as our new research results (such as the ones stemming from ERC Starting Grant project Goodshape on optimal sampling). In particular, it has reconstruction, remeshing, Delaunay triangulation in 3D, Lloyd relaxation in nD, restricted Voronoi diagram in nD, numerical solvers (OpenNL) and a language to automatically generate geometric predicates from their formulas (PCK: Predicate Construction Kit). Its development follows strict quality norms, including systematic documentation of all parameters and all functions, systematic non-regression testing, memchecker with a continuous integration platform (Jenkins). *Vorpaline* is a proprietary extension of Geogram, its development was funded by a ERC Proof of Concept grant. It contains hexahedral dominant meshing algorithms. Vorpaline evaluation licenses are proposed to the sponsors of the GOCAD consortium, that groups all the major oil companies. *Graphite* is a Graphical User Interface on top of Geogram and Vorpaline, giving an easy access to remeshing and reconstruction algorithms in Geogram. These softwares have been developped since year 2000 and have an archive of most of our research results since then.

IceSL is both a 3D modeler and a slicer for 3D printers. It contains new research results stemming from ERC Starting Grant Shapeforge. The main idea is to use a volume representation to unify the whole modeling chain (more precisely, it uses ”dexels”), created on the fly just before visualization and fabrication as opposed to existing methods. Thus, it always exists at the optimal resolution (i.e. screen or printer resolution), and there is no loss of quality due to re-sampling. The input objects always remain in their natural representation (mesh, volume, equation) and are only converted whenever required. We developed novel data-structures optimized for GPU implementation (spatial hashing and hierarchies created concurrently on multi-processors), as well as efficient Constructive Solid Geometry operations, accessible through an interpreted language (Lua). This makes it possible to generate complicated 3D models, with internal structures and details of micro-metric size without needing to pay the associated memory cost if we would have used meshes. IceSL also includes the new algorithms developed by the team to take into account fabrication constraints in the modeling process. We recently received on ERC Proof of Concept grant (named IceXL) to further develop the software and study its industrial potential via a number of existing partnerships in the medical, automotive and design industries.

Academic reputation and appeal

8 Prizes and Distinctions

- Jean Hergel, Best Eurographics presentation award [132]
- Jeanne Pellerin, J. Computers and Geosciences best article award [155]
- S. Lefebvre and B. Lévy gave several invited and keynote talks (full list in appendix)
- Bruno Levy reveiced the Inria young researcher award 2011

9 Editorial and organizational activities

- S. Lefebvre is associate editor of ACM Transactions on Graphics
- B. Levy was co-chair of several events (including Eurographics 2014, see appendix)
- B. Levy is associate editor of several journals (see appendix)
- S. Lefebvre and B. Levy were PC members of the major conferences (see appendix)

10 Services as expert or evaluator

- B. Levy was member of the HCERES visiting commitee for LABRI (Bordeaux) in 2014
- B. Levy was president of the Inria hiring commitee in Nancy in 2013 and 2014
- B. Levy and S. Lefebvre were commitee member for 32 Ph.Ds and 9 HdRs (2011-2016)
- B. Levy and Sylvain Lefebvre reviewed projects submitted to ANR and ERC

11 Cooperations

- **Hong-Kong U.:** our two research axes (additive fabrication and geometry processing) have a co-operation with two researchers in Hong-Kong U. (W. Wang and L.-Y. Wei). We have an Inria Associate Team with them. Our cooperation resulted in several joint publications on sampling and meshing [161, 164, 166, 168, 125] and on texturing and additive fabrication [143, 144];

- **Dauphine U. / Inria Paris:** We started in 2014 to establish cooperations with mathematicians working on optimal sampling (Q. Merigot, J.-D. Benamou, Y. Brenier), through joint meetings and workshops (Jacques Louis Lions lab., Banff center for math. innovation, Bonn workshop on OT, Summer School on calculus of variations in Grenoble). The goal is to develop both the theory and efficient numerical algorithms to solve a certain class of non-linear partial derivative equations, with our original "semi-discrete" point of view. We started this year (2016) a new cooperative project EXPLORAGRAM (see below).

- **Other cooperations** We cooperate on a regular basis with Pierre Poulin (U. Montréal) and Alla Sheffer (UBC) [151, 150, 142]. We also have on-going cooperations with Marc Alexa (T.U. Berlin) and Niloy Mitra (University College London).

12 External support and funding

- **2008-2015 GOODSHAPE ERC Starting** (project lead) on shape sampling
- **2015-2016 VORPALINE ERC Proof of Concept** (project lead) pre-industrialization of the results of GOODSHAPE
- **2014-1019 SHAPEFORGE ERC Starting** (project lead) on additive manufacturing
- **2015-2016 ICEXL ERC Proof of Concept** (project lead) pre-industrialization of the results of SHAPEFORGE
- **2009-2012 PHYSIGRAPHICS ANR chaire d'excellence** (project lead) on computer vision and geometry processing
- **2010-2014 MORPHO ANR** (as project member) on acquisition of human motion
- **2013-2017 BECASIM ANR** (as project member) on computational physics
- **2014-2017 BLUEPRINT Region Lorraine** on additive manufacturing
- **2014-2020 CPER** S. Levebvre coordinates a project with several labs. in Nancy (IJL, LRGP, ERPI) on software and material interactions in filament-based 3D printers

- **2016-2017 EXPLORAGRAM** B. Levy coordinates an Inria Exploratory Project on Optimal Transport (coop. with Q. Merigot, J.-D. Benamou, Y. Brenier)

Involvement with social, economic and cultural environment

- **GOCAD consortium** we have a long-term cooperation with the numerical geology lab. (Nancy School of Geology) leader of the GOCAD consortium, that regroups all the major companies in oil and gas industry. The consortium funded 5 Ph.D. theses during the evaluation period. The result of our Vorpaline ERC Proof of Concept is a sofware that is proposed to the sponsors of the consortium (two of them are in the process of acquiring a license). During the evaluation period, 3 of our co-advised Ph.D. thesis student were hired by these companies right after their defense (A. Botella, N. Cherpeau and R. Merland);
- **PIC** (Polymères Innovants Composites) is a collaboration between Inria, Institut Jean Lamour and Ateliers Cini, funded by Région Lorraine. The goal is to develop a new additive manufaturing process using filament of composite materials with applications in mechanical engineering and in the medical domain.
- 6 patents filed during the evaluation period (full list in appendix)

Involvement in training through research

- D. Sokolov organizes several Master courses (graphics, programming, optimization)
- S. Lefebvre teaches “videogames technology” in Ecole des Mines
- B. Lévy teaches numerical methods in School of Geology and Ecole des Mines
- We submitted in 2016 an H2020 ITN project (with U. Louvain and the SIMULA compagny)

Cryptology, arithmetic: algebraic methods for better algorithms

Synopsis

1 Team Composition

Permanents

Jérémie Detrey (CR INRIA), Pierrick Gaudry (DR CNRS), Pierre-Jean Spaenlehauer (CR INRIA, arrived 01/01/14), Emmanuel Thomé (DR INRIA, promoted 01/10/15), Marion Videau (MCF UL, on secondment to Quarkslab since 01/01/15), Paul Zimmermann (DR INRIA).

	PR	MCF	DR	CR	Total
2011		1	2	2	5
2016			3	2	5

Post-docs, and engineers

Nicholas Coxon (postdoc 2014-2015), Stéphane Glondu (engineer 2012-2014), Sorina Ionica (postdoc 2011-2012), Alexander Kruppa (engineer 2012-2015), Maike Massierer (postdoc 2014-2015), Pascal Molin (postdoc 2010-2011), Lionel Muller (engineer 2009-2011).

Doctoral students

Simon Abelard (UL / ENS, 2015-), Razvan Barbulescu (UL / ENS, 2011-2013), Gaëtan Bisson (UL / ENS / TU Eindhoven, 2008-2011), Cyril Bouvier (UL / ENS, 2012-2015), Romain Cosset (INRIA/DGA, 2008-2011), Svyatoslav Covanov (UL / X, 2014-), Nicolas Estibals (UL, 2009-2013), Laurent Grémy (INRIA, 2013-), Hamza Jeljeli (UL, 2011-2015), Hugo Labrande (UL / ENS / Univ. of Calgary, 2013-).

PhD's defended	6	On-going PhD's	4

Team evolution

Marion Videau was part of the team for most of the evaluation period. From January 2015, she is on secondment to the Quarkslab company. Pierre-Jean Spaenlehauer was hired and joined the team in January 2014.

2 Life of the team

The Caramba team is a follow-up of the Caramel team (2010-2015), which was itself the successor of the Cacao team. The short life-time of our teams is mostly due to the INRIA rule of starting a new team each time the leader changes.

The scientific life of the team is ensured by a team seminar, on a more or less monthly basis, and some residential team workshops "Journées au vert" that we try to organize every 18 months. We have also a less formal meeting during the noon coffee-break on Mondays, where a member of the team explains an article he recently read.

3 Research topics

Keywords

Integer factorization, discrete logarithm, (hyper)elliptic curve cryptography, arithmetic.

Research area and main goals

One of the main applications for our project is public-key cryptography, where most of the deployed solutions use systems based on number theory such as RSA, ElGamal, DSA or elliptic curves. Although all these are known to be vulnerable to an hypothetical quantum computer, alternative systems, such as those based on Euclidean lattices or coding theory are still far from being mature enough for large scale usage. Therefore, one of our main topics is the study of algorithmic problems in number theory that are related to their use in cryptography, in particular integer factorization and the discrete logarithm problem. On the algebraic curve side, we go one step further than just elliptic curve and study also problems related to the potential use of genus 2 hyperelliptic curves that could provide a competitive cryptosystems compared to those based on elliptic curves.

Over the evaluation period, we have concentrated our efforts in 3 main directions. The first one is the large family of algorithms that follow the number field sieve (NFS) strategy: these are well suited for factoring RSA keys and for computing discrete logarithms in finite fields. Second, we have worked on algorithms for curves: point counting, discrete logarithms, and effective complex multiplication in genus 2. Finally, a third direction is to study arithmetic building blocks, *per se*. A more recent research direction is polynomial systems and their interaction with aforementioned problems (after the recruitment of P.-J. Spaenlehauer).

4 Main Achievements

Our most visible results are those concerning the discrete logarithm problem in finite fields. In collaboration with A. Joux [251], we have proposed an algorithm with a heuristic quasi-polynomial complexity in the case of small characteristic, while all previously known algorithms had a much worse complexity. On the practical side, with many co-authors [244] we have revealed a weakness in the TLS protocol related to the discrete logarithm problem in prime fields, and affecting dozens of thousand of servers. Finally, we hold the current record for the largest public discrete logarithm computations in prime fields and in fields of the form $\mathbb{F}_{p^2}$.

5 Research activities

NFS-like algorithms for factoring and discrete logarithm

Description The number field sieve (NFS) is the best known algorithm for factoring integers used in the RSA cryptosystem, with time and space complexities that are not fully exponential but still far from polynomial[2]. Many variants of NFS have been designed to handle other problems, in particular the discrete logarithm problem in finite fields. At the beginning of the evaluation period, we had acquired a good expertise on NFS for factorization, and we wanted to use it in the context of discrete logarithm which had been far less studied. The problem naturally comes in different flavors depending on the characteristic of the field: for instance, in small characteristic number fields are replaced by function fields, yielding the so-called FFS algorithm. In all cases, a linear algebra step, which is already complicated in the case of integer factorization becomes even more problematic and specialized algorithms have to be used.

In this area, it is important to obtain complexity results, but often these are not precise enough to deduce accurate estimates on the running time for very large instances that occur in cryptography, while there is a huge need for these estimates in order to choose appropriate key sizes corresponding to the target security level. Therefore, a large part of our activity is dedicated to writing efficient software and running computations for setting new records. These records are used by governmental agencies and standardization bodies to justify their recommendations.

Main results In terms of **complexity improvements**, probably the most visible result of the team over the evaluation period is the breakthrough algorithm developed by Barbulescu, Gaudry, Joux and Thomé for discrete logarithms in finite fields of small characteristic [251]. This followed the major improvement made by Joux that led to an $L(1/4)$ complexity. Its complexity (which is estimated using heuristics, but not rigorously proven) is quasi-polynomial: this is considerably better than the previous state of the art, which had not changed for 20 years.

In the realm of medium characteristic, Barbulescu, Gaudry, Guillevic and Morain gave a setting for the NFS algorithm [250], improving its complexity from $L_{p^n}(1/3, \sqrt[3]{128/9})$ to $L_{p^n}(1/3, \sqrt[3]{96/9})$. This is of course less spectacular than the small-characteristic result, but has also important implications in pairing-based cryptography where such fields occur. Other more technical complexity results have been obtained in [208] and in [278].

We have also developed efficient software and run computations leading to several **discrete-logarithm records**. Before the $L(1/4)$ and quasi-polynomial breakthrough, we have used the FFS algorithm to set a new record for discrete-logarithm computation in characteristic 2, with an 809-bit problem [248]. Almost all team members contributed, and various improvements were developed for this record [256, 217, 275, 263, 264]. This prime-degree extension record held for about 18 months, which was a bit longer than expected once Joux's and subsequent complexity improvements were published. We have also set a new record computation in the case of prime fields, reaching 180 decimal digits[3], while the previous record had 160 decimal digits. Again, this was the occasion to improve various parts of the algorithm, while reusing some of the improvements developed for the FFS record (especially in the filtering and linear algebra parts). Finally, we have computed a discrete logarithm in a finite field of the form $\mathbb{F}_{p^2}$, where p^2 has about 180 decimal digits [250]. Quite surprisingly, it ended up being faster than a factorization problem of similar size.

In a collaboration with colleagues from formal methods and internet security [244], we have revealed a new vulnerability in the TLS protocol, leading to what we called **the Logjam attack**. Due to a flaw in the first stage of the protocol, it is possible to downgrade the security to a point where it becomes possible

[2]Complexities are expressed with the function $L_N(\alpha, \beta) = \exp(\beta(\log N)^\alpha(\log\log N)^{1-\alpha})$, with $\alpha = \frac{1}{3}$ for NFS.
[3]The announcement for this record is available at `http://caramel.loria.fr/p180.txt`.

to solve a discrete logarithm instance on-the-fly, provided a large pre-computation has been performed, thus leading to an important breach in the security of the communication. We used our CADO-NFS software to develop a proof-of-concept, demonstrating the feasibility of the attack.

Finally, we have continued to make **progress in integer factorization**, a large part of our work consisting in the development of CADO-NFS (see the Software section). There were also some algorithmic improvements on several parts of the integer factorization NFS algorithm. Thomé designed a CRT-based variant for the square root part [266], which is interesting for special cases where the naive approach can fail, and is easier to parallelize. A series of improvements for the polynomial selection stage have been made by Prest, Zimmermann, Brent, Bai, Thomé, Bouvier, Kruppa, Coxon [216, 240, 215, 277]. Although this is not the most time consuming part of the algorithm, the quality of its output can greatly speed up the relation search. Therefore the runtime estimates for RSA-1024 have been significantly revised.

Algebraic curves and cryptography

Description The main algorithmic problems for algebraic curves in cryptography are: counting the number of elements in the group we want to use, in order to check that it is a prime; trying to solve the discrete logarithm problem; designing fast formulae for the group law; compute important invariants like the ring of endomorphisms.

Over the evaluation period, we have concentrated our activities on only few selected topics, since we chose to reduce the activity on curves in order to have more time to work on the NFS algorithm for discrete logarithm which was a hot topic. The main topic that we studied is therefore the complex multiplication (CM) theory in genus 2.

Main results A. Enge and Thomé worked on the CM method in genus 2 [228]. Building on the work of M. Streng (Leiden), they carefully implemented state-of-the-art algorithms, which they pushed further in order to be able to tackle a record-sized computation[4], namely a class number of more than 20,000. This is the first computation with an implementation with a quasi-linear complexity for the evaluation of the theta functions. The literature contains a lot of theoretical advances (done for a large part around K. Lauter from Microsoft Research) to predict the leading coefficient of the output polynomials. This large example corroborates these theoretical results, but also shows that they are still not precise enough to provide a speed-up in the computation. The software used for this record computation has been released under a free software license.

The CM theory is not too far from the ring of endomorphisms of the corresponding abelian varieties. Ionica [235], and then Ionica and Thomé [281], worked on improving the computation of this important object. They designed a strategy that is reminiscent of Kohel's algorithm based on the volcano-like structure of the graph of isogenies. In genus 2, the structure is more like a Cartesian product of two such volcanoes, and traveling in it is feasible, with, as for genus 1, the Tate pairing being used as some kind of imperfect compass.

Apart from these works on the CM theory, we mention the following two isolated contributions. B. Smith, D. Kohel and Gaudry found a new algorithm to count the number of points of genus-2 curves with real multiplication [261]. A careful use of the knowledge of an explicitly computable endomorphism leads to a complexity similar to what is known for elliptic curves.

Finally, L. Huot, G. Renault, J.-C. Faugère and Gaudry, showed [229] that during an index-calculus algorithm for the elliptic curve discrete logarithm problem, if the curve can be put in Edwards form (which has been very popular in the past few years), then the polynomial systems that occur have an additional structure that can be exploited and this leads to a faster attack.

[4] The announcement for this record is available at `http://cmh.gforge.inria.fr/record.txt`.

Arithmetic

Since arithmetic is a transversal theme for us, with a large part of implementation, our positioning is a bit atypical. We have a strong commitment to publishing and maintaining software libraries, and the corresponding activities are described in the Software section below. We emphasize in particular the GNU MPFR and GNU MPC libraries, that are used by the GCC compiler to compute accurately the constants that are known at compile-time.

Apart from the software development activity and isolated work, for instance on the error function [225] or on the Masser–Gramain constant [238], our contributions are of two types: improve the fundamental building blocks of integer or polynomial arithmetic [222, 262, 249, 276], and study the suitability of non-general-purpose hardware for various applications (see [263] and a contract with the Kalray company).

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis	2		2		2		6
H.D.R		1					1
Journal	9	5	3	5	5	1	28
Conference proceedings	6	5	3	7	4		25
Book chapter	2		1				3
Book (written)			1				1
General audience papers	1						1

List of top journals in which we have published
Mathematics of Computation (5) [215, 217, 226, 216, 238]; Journal of Symbolic Computation (3) [233, 240, 231]; Journal of Cryptology (2) [229, 227]; IEEE Transactions on Computers (2) [222, 218]; Journal of Number Theory (2) [235, 220].

List of top conferences in which we have published
Major crypto / security conferences: ACM CCS, Eurocrypt, Asiacrypt (6, including 3 with Best Paper Awards and 1 paper invited to Journal of Cryptology) [250, 252, 251, 243, 261, 244]; Specialized crypto conferences: SAC, PKC, CT-RSA (3) [248, 245, 260]; ISSAC (2) [258, 259]; ARITH (2) [256, 262]; WAIFI (3) [263, 266, 249].

7 Software

CADO-NFS. This is a complete implementation in C/C++ of the NFS algorithm for factoring integers and computing discrete logarithms in finite fields. Started around 2007, it is released under the LGPL free software license. There are about 200,000 lines of source code. Most of the main developers are members of the team. Over the evaluation period, efforts have been put on efficiency, code quality, scalability, and improving of the discrete logarithm support.

The factorization part is now mature and stable, so that the number of external users (number theorists, cryptographers, or factoring enthusiasts) is constantly increasing.

Arithmetic libraries. We are developing and maintaining libraries for various arithmetic building blocks. The GNU MPFR and GNU MPC are mature projects that provide multiprecision floating point arithmetic with correct rounding up to the last bit. Due to the fact that they are both required to compile GCC, these libraries enjoy a very high visibility.

We also develop the GF2X and MPFQ libraries that are more specialized and less visible. However, both are used by CADO-NFS, and GF2X can be used as an auxiliary package for the widespread software library NTL.

Belenios. This is an open-source private and verifiable electronic-voting protocol, that we develop in collaboration with the PESTO team. Our system is an evolution of an existing system, Helios, developed by Ben Adida, and used e.g., by UCL and the IACR association in real elections. The main differences with Helios are the following: the list of the voters is not publicly exposed as it was with Helios (following the French regulation) and the server hosting the ballot box can no longer add ballot, so we don't have to trust the server.

In the past months, several real-life elections have been run with Belenios (still on an experimental basis): "Comité de Centre" of the Inria Research Center in Rennes; head of the "groupes de travail C2 et calcul formel" of the GDR-IM.

Academic reputation and appeal

8 Prizes and Distinctions.

Our quasi-polynomial algorithm for discrete logarithm in small characteristic obtained the Best Paper Award at Eurocrypt 2014. This result was much commented in the blogosphere, and Ravzan Barbulescu received the "Prix de thèse Le Monde" for this work.

The work on the Logjam attack [244] received large media coverage (especially in the USA); the article got the Best Paper Award at the ACM CCS conference, which is one of the best conferences in computer security, and we received a Pwnie award in the category "Most innovative research" during the BlackHat 2015 conference.

Implication in major conferences.

We have an important involvement in the ECC workshop series (the main conference about elliptic curve cryptography, since 1997). We organized it in Nancy in 2011 (more than 120 participants); P. Gaudry is a member of the steering committee since 2014; J. Detrey (2012), P. Gaudry (2013) and E. Thomé (2014) gave invited talks. The ANTS conference (Algorithmic Number Theory Symposium) is also strongly connected to our research topics. E. Thomé is a member of the steering committee.

Among our invitations to international conferences, we highlight: Pairing 2013 (Gaudry), SAC 2014 (Gaudry), WAIFI 2012 (Thomé).

Members of the team have been PC members for many conferences, including: Eurocrypt 2011, 2016, Asiacrypt 2013, PKC 2015, FSE 2011, Pairing 2012, 2013, SAC 2014, Waifi 2012, 2014, 2016, ISSAC 2013.

9 Editorial and organizational activities

The complete detail of our activities regarding this topic can be found in the appendix.

Over the evaluation period, we organized one international conference in Nancy which included a summer school, and more recently one mini-workshop.

Two members participate in steering committees of international conference series. One is also a member of the editorial board for an international journal.

We participated, collectively, to 29 program committees over the evaluation period.

10 Services as expert or evaluator

The complete list of evaluation and hiring committees as well as thesis juries to which we took part can be found in the appendix.

Collectively, we participated to 20 hiring committees at the assistant professor or professor positions, or juries for junior or senior research scientist positions.

In total, team members had 34 participations in PhD or habilitation thesis juries, including 11 as advisor or co-advisor, and 11 as referees.

P. Gaudry was deputy head of the LORIA lab from January 2011 to December 2012. P. Zimmermann was appointed (and still is) “délégué scientifique´´ of the INRIA Nancy research center from September 2013.

P. Gaudry was a member of HCERES Evaluation panel for the LITIS laboratory (Rouen) in 2015. He coordinated the INRIA evaluation seminar in 2015 for the team Algorithmics, Computer Algebra and Cryptology.

11 Collaborations

We have formalized collaborations (through funded ANR projects, or otherwise long-running research projects) with teams in Palaiseau, Montpellier, Bordeaux, Rennes, Lyon. We co-supervised PhD theses with colleagues from other countries: Calgary (Canada), Eindhoven (The Netherlands), or also in France (Paris 6).

12 External support and funding

Over the evaluation period, the team received support from two ANR grants: CHIC (2009-2012) and CATREL (2013-2015), as well as a contract with the HTCS company.

Involvement with social, economic and cultural environment

Activities related to cryptanalysis. Our work on integer factorization and discrete logarithm is of interest for governmental agencies and standardization bodies for tuning accurately their key size recommendations. We do not have any formal relation with the French ANSSI or the German BSI, but we know them very well. Our work on the Logjam attack had a more direct real life impact and was complemented by a CVE entry: CVE-2015-4000; many software updates followed.

Since 2012, we have a yearly contract with the HTCS company, which is renewed each year (the new contract for 2016 is just starting). It consists of training and consulting activities. Due to confidentiality clauses, we cannot say much.

Activities related to e-voting. In connection with our work on the Belenios software, we have participated to two contracts (with Voxaly in 2013, and Docapost in 2015), where we evaluated the e-voting solutions of the companies and proposed them directions for improvements.

Involvement in training through research

We wish to emphasize the activity of M. Videau as the head of the engineering master's degree in "Services, security of systems and network" within the Master 2 in computer science of the Université de Lorraine in 2013–2014. A joint seminar with the LORIA laboratory was created with about two sessions per month. During the first semester, sessions are especially crafted to meet the interest of a broad audience. The speakers are mostly from the industry or from governmental agencies with an emphasis on strong research and development profiles. This seminar, which started in 2013, is very successful in terms of attendance, and fosters the relations between the teaching at the master level and the research activities in the laboratory.

Visual augmentation of complex environments

Synopsis

1 Team Composition

Permanents

Marie-Odile Berger (DR INRIA), Erwan Kerrien (CR1 INRIA), Gilles Simon (Assistant Prof., UL), Frédéric Sur (Assistant Prof., UL), Pierre-Frédéric Villard (Assistant Prof., UL), Brigitte Wrobel-Dautcourt (Assistant Prof., UL).

	PR	MCF	DR	CR	Total
2011		4	0	2	6
2016		4	1	1	6

Post-docs, and engineers

Pierre-Jean Petitprez (engineer 2014-2016), Christel Léonet (engineer 2012-2014).

Doctoral students

Raffaela Trivisonne (INRIA, 2015-..., co-supervised with MIMESIS), Jaime Garcia Guevara (Region, 2015-..., co-supervised with MIMESIS), Antoine Fond (UL, 2014-...), Pierre Rolin (UL, 2013-...), Charlotte Delmas (UL, CIFRE with GE Healthcare, 2013-...), Nazim Haouchine (Université de Lille, 2012-2015, co-supervised with MIMESIS), Ahmed Yureidini (Université de Lille, 2010-2014, co-supervised with Shacra), Srikrishna Bhat (UL, 2008-2012), Nicolas Noury (UL, 2007-2011).

Phd's defended	4	On-going PhD's	5

Team evolution

There was no evolution of the staff members during the evaluation period.

2 Life of the team

Frédéric Sur benefited from a full time CNRS delegation during 2012-2013 and from a half-time INRIA delegation during 2013-2014. Pierre-Frédéric Villard spent 18 months in 2014-2015 in the Harvard Biorobotics Laboratory thanks to a CNRS and then a INRIA delegation.

3 Research topics

Keywords

Augmented reality, matching, localization, 3D modeling, estimation, image processing, image analysis.

Research area and main goals

The basic concept of augmented reality (AR) is to place information correctly registered with the environment into the user's perception. What makes AR stand out is that this new technology offers the potential for big changes in many application fields such as industrial maintenance, creative technologies, image guided medical gestures, entertainment…

Augmented reality technologies have made major advancements recently, both in terms of capability, mobile development and integration into current mobile devices. Most applications are dedicated to multimedia and entertainment and use rough localization information provided by the sensors of the mobile phones. Cutting-edge Augmented Reality applications which take place in complex environments and require high accuracy in augmentation are less prevalent. There are indeed still technological barriers that prevent applications from reaching the robustness and the accuracy required by such applications.

The aim of the MAGRIT team is to develop vision based methods which allow significant progress of AR technologies in terms of ease of implementation, reliability and robustness. The team is active in both medical and classical applications of augmented reality for which accurate integration of the virtual objects within the scene is essential. Key requirements of AR systems are the availability of robust matching and registration techniques, both rigid and elastic, that allow the virtual objects to be correctly aligned with the environment, as well as means to build 3D models which are appropriate for pose computation and for handling interactions between the virtual objects and the real scene. Localization and visual modeling are thus our main research topics. Methods are developed with a view to meet the expected robustness and accuracy over time while satisfying the real time achievements required by these procedures.

4 Main Achievements

The development of robust methods for matching and localization under large viewpoint variations through either the design of statistical methods or the use of simulation is a strong point of our activities.

Efforts to produce structured models appropriate to AR tasks must also be put forward. New methods for in-situ modeling in classical environments as well as models supporting real time interactive simulation for medical applications are examples of our contributions.

The period has seen the emergence of significant works about AR for deformable objects in collaboration with the MIMESIS team with promising applications to laparoscopy. The paper [328] was awarded by the best paper-honourable mention at ISMAR 2013.

Denoising and parameter estimation is an important issue in our team since most problems are formulated as parameter estimation from noisy measurements. Noise reduction techniques have been investigated for natural images and original dedicated image processing tools have been designed in the context of characterizing properties of material subject to mechanical constraints.

One last point that should be emphasised in our activity is that we are engaged in stimulating transdisciplinary research, especially in the field of medical imaging and experimental mechanics.

5 Research activities

Matching, localization and 3D tracking

Description The challenge of AR is to compute sequential and near real time pose estimates with a good accuracy whatever the user's motion, the nature of the scene (cluttered, with repeated patterns…) and the variations in experimental conditions (lighting, weather conditions, presence of pedestrians, cars, tools in medical scenes…). Tracking has acquired a certain level of maturity during the last decade and effective toolkits can now be used to create AR systems in simple environments under controlled conditions. However computation of the initial pose, i.e. without any guess on the localization, as well as localization in cluttered environments are still deadlocks which prevent the design of robust AR systems. This is mainly due to the rate of wrong matching hypotheses which is very high in such contexts. During the evaluation period we have addressed various methods that improve the reliability of the localization: design of robust statistical methods, use of tracking-by-synthesis method or introduction of semantic knowledge on the considered environments. Finally, the issue of tracking deformable objects has gained importance in our team during the period. This topic was mainly addressed in the context of medical applications through the design of bio-mechanical models guided by visual features.

Main results

- **Matching and initialization in difficult conditions**
  The goal of N. Noury's PhD thesis [288] was to address matching and localization issues in man-made environments which contain many repetitive patterns. In order to prevent ambiguous correspondences due to repetitive patterns from being removed early as in classical algorithms, we designed a novel a-contrario model in order to impose photometric and geometric constraints in a unified metric [310]. Our efforts then focused on the problem of image/image or image/model matching in presence of large viewpoint changes. We considered the common case where the model is acquired from a sequence using structure from motion techniques. A 3D point was then represented with the class of all interest points and descriptors to which it was associated in the structure-from-motion stage. Matching thus amounts to identify the class which is closest to a particular descriptor. Visual vocabularies where used inS. Bhat's PhD thesis to speed up the image/model matching process[313, 286].

  When pose initialization is considered, the image may be far from the ones used for building the model and matching fails due to the lack of similarity between the classes and the current descriptor. In the context of P. Rolin's PhD thesis, we proposed to enrich the models with keypoints generated from simulated views [357, 335] to ease the matching in presence of large viewpoint changes. Noticeable improvements of the pose reliability have been demonstrated with this method. Progressive sampling strategies are currently investigated to speed up the search for correspondences when confronted to a large outlier rate. A complementary way to fight against large outlier rates when distant views are considered is to take into account contextual information which is likely to filter out some erroneous matching hypotheses. This idea is being investigated in A. Fond's PhD thesis through the exploitation of the Manhattan world hypothesis [321, 338].

- **Tracking-by-synthesis using point features and pyramidal blurring**

Tracking-by-synthesis [RD06] is a promising method for markerless vision-based camera tracking since it is drift-free and easy to combine with physical sensors such as GPS and inertial sensors. However, it is mostly used in urban environments were edges can easily be detected. This is probably due to the fact that real-time corner detectors are weakly repeatable between a camera image and a rendered texture. In [339], we compared the repeatability of commonly used interest point detectors against view synthesis and drew valuable insights about the adaptation of tracking-by-synthesis algorithms to the point feature. Important contributions of this work are (i) the demonstration that adding depth blur to the rendered texture can drastically improve the repeatability of FAST and Harris corner detectors (up to 100% in our experiments) (ii) the design of a method for simulating depth blur on the rendered images using a pre-calibrated depth response curve as well as an original method for calibrating the depth response curve.

- **Tracking 3D deformable objects**
  3D augmentation of deformable objects is a challenging problem with many potential applications in medical augmented reality. Most existing approaches are dedicated to surface augmentation and are based on the inextensibility constraint, for sheet-like materials, or on the use of a model built from representative samples. However, few of them consider in-depth augmentation which is of utmost importance for medical applications. In N. Haouchine's PhD thesis, we have addressed several important limitations that currently hinder the use of augmented reality in the clinical routine of minimally invasive procedures. In collaboration with the MIMESIS team, our main contribution is the design and the validation of an augmented reality framework based on a mechanical model of the organ and guided by features extracted and tracked on the video at the surface of the organ [327, 328, 297]. Specific models which best suit the considered organs, such as a vascularized model of the liver, have been introduced in this framework. Experiments show that the localization error of a virtual tumor was less than 6mm, and thus below the safety margin required by surgery. To our knowledge, we were the first to produce such evaluation for deformable objects. This work has been extended to augment highly elastic objects in a monocular context using a non-linear elastic model constrained by tracking external image points [298]. This method prevents us from formulating restrictive assumptions and specific constraint terms in the minimization which are commonly used in state-of-the-art solutions. Self-occluded regions are handled thanks to the ability of mechanical models to provide appropriate predictions of the shape. This property was also exploited in the context of tongue tracking in ultrasound images [332].

Image-based modeling

Description Making AR applications effective and realistic requires the availability of appropriate models of the scene. By the term *appropriate*, we mean that the model must be relevant for the considered task. It must thus be suited to pose computation but also capable of supporting interactions between the virtual and the real objects such as occlusions, lighting reflections, contacts in real time. If point cloud models are sufficient for pose computation, structured models are required for handling interactions between real and virtual worlds. Designing the complete loop of AR from pose to interaction obviously depends on the specific tasks under consideration. We thus address a restricted number of applications in areas where we have a long term experience: modeling for urban AR applications as well as AR and simulators for interventional radiology.

Main results

[RD06] G. Reitmayr and T. Drummond. Going out: Robust model-based tracking for outdoor augmented reality. In *ISMAR'06*, 2006.

- **In situ modeling**
  If 3D models are generally available for very public spots, this is not the case for smaller or ephemeral AR work-spaces where short-lived applications have to take place (e.g. film set or maintenance applications). We thus developed several original methods for *in situ* modeling allowing a user to directly build a 3D model of his/her surrounding environment and verify the geometry against the physical world in real time [303, 331]. The originality of our approaches is that they are based on the camera-mouse principle, thus preventing us from using an additional device for delineation and that modeling can be achieved without freezing the video. In contrast to existing interactive or automated methods for model building that are computationally intensive, in-situ modeling techniques enable the user to define what is relevant at the time the model is being built during the application. Acquisition of structured models is another important benefit of these methods.

- **Modeling for realistic and real time simulation**
  In interventional radiology, our main research objective is to augment the environment of the physician through several means: first, by superimposing tools onto pre-operative imagery for a better understanding of the pathology [316] and second, by providing realistic patient-based simulators for training or planning an operation. One of our main contributions tackles the particular issue of computational efficiency and concern the automatic modeling of blood vessels from medical data, in order to meet the computational requirements of interactive simulation. The segmentation had to be both user friendly and generate a vascular surface model that is compliant with the computational constraints set in interactive simulation, that is: compact, smooth, and both geometrically and topologically accurate. During A. Yureidini's PhD thesis, a new model was developed consisting of a tree of local implicit blobby models [347]. In collaboration with the MIMESIS and DEFROST team, comparisons were made of simulations using our implicit model against triangular meshes and showed that the computation time was divided by 100 while numerical instabilities encountered with meshes (jaggy motions, unrealistic sticking of the catheter tip on the vessel surface, ...) were not observed with our implicit model [348]. More generally, acquisition of realistic models of organs from multimodal images is an important issue for obtaining realistic and accurate augmentation of pre-operative images or realistic training systems. This problem is an important field of research of the team and has been addressed in the team for modeling ribs motion during surgery [344] and to build realistic simulators of liver biopsy [312].

Denoising and parameter estimation

Most issues addressed by the team are formulated in terms of parameter estimation from image-based measurements corrupted by noise. Particular difficulties are due to the presence of specific noise, to the possibly high non linearity of the relationship between the parameters and the observation or to the large size of the unknowns with respect to the number of observations. A common problem in our field of research is the need to estimate constitutive parameters of the models, such as (bio-)mechanical parameters for instance. Direct measurement methods are destructive and elaborating image based methods for parameter estimation is thus highly desirable. Denoising methods as well as estimation techniques dedicated to specific problems have been addressed during the evaluation period.
In a collaboration with the Pascal Institute (Clermont Ferrand), the metrological performance enhancement for experimental solid mechanics has been addressed. A problem of interest in experimental solid mechanics is to estimate displacement and strain maps on the surface of a specimen subjected to a load or a tensile test. While digital image correlation (DIC) relying on randomly marked patterns is certainly the most popular technique, spectral methods on grid patterns is another possibility. With the goal to characterize the metrological performances of these techniques limited by the sensor noise [296], we

have proved (in the context of the grid method) that it was possible to retrieve a convolved strain map impaired by a correlated noise [305]. The most common analysis windows used in the grid method have been analyzed in [309]. Various restoration techniques have been investigated to enhance the metrological performances of the grid method [293], in spite of vibrations affecting the experimental setup [304, 308]. A complete review of grid methods is the subject of [295]. Moreover, contributions to the characterization of the metrological performance of DIC were recently proposed [291]. In addition, other topics related to noise estimation or noise removal in experimental mechanics as in natural images have been addressed. Various methods were proposed to remove quasi-periodic noise using frequency domain statistics, either in strain fields [294] or in natural images [343, 306]. Noise estimation by stacking natural images affected by illumination flickering was addressed in [307].

In the medical field, specific methods for estimating respiratory parameters have been designed in collaboration with School of Computer Science at Bangor University [311, 353]. The optimized parameters have been eventually applied to an interventional radiology simulator that takes into account the respiration [312].

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis	1		1	1	1		4
Journal	3	1	4	3	7	6	24
Conference proceedings	8	6	11	13	8	2	48
Book chapter	1	1	2				4
Book (written)	1						1
Book or special issue (edited)			1				1
General audience papers			2		1		3

List of top journals in which we have published
SIAM journal on imaging sciences [310, 307], Inverse problems and imaging [305], IEEE Trans. on Visualization and Computer Graphics [297, 298], The Visual Computer [303], Medical Image Analysis [302], IEEE Trans. on Biomedical Engineering [311], JASA [290].

List of top conferences in which we have published
Int. Symp. on Mixed and Augmented Reality (ISMAR) [339, 320, 328, 326], International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI) [348], IEEE International Conference on Image Processing (ICIP) [341, 343], International Conference on Robotics and Automation (ICRA) [329, 335], International Conference on Acoustics, Speech, and Signal Processing (ICASSP)[340], IEEE 3DIM/3DPVT Conference [313].

7 Software

- Our research efforts are integrated in a internal use library called RAlib. This work is now proposed in part in the publicly available Polar library (Portable Library for Augmented Reality, `http://polar.inria.fr`) that offers powerful and state of the art visualization solutions.
- Matlab software implementing the algorithms described in [307, 306, 343] is publicly available.

- A multimodal acquisition system was also developed in the team in the context of the ARTIS project. This project aims at building a realistic head augmented by external and internal articulators with foreseen applications to language learning technologies [290].

Academic reputation and appeal

8 Prizes and Distinctions

- *Best paper-honourable mention* at ISMAR 2013 for the paper [328]: *Image-guided Simulation of Heterogeneous Tissue Deformation For Augmented Reality during Hepatic Surgery*

- Gilles Simon received the *Lasting Impact Award* at ISMAR 2013 for the paper: *Markerless Tracking using Planar Structures in the Scene by Simon Gilles, Andrew W. Fitzgibbon, Andrew Zisserman in Int. Symposium on Augmented Reality, 2000 (ISAR)*

9 Editorial and organizational activities

Marie-Odile Berger was co-president of RFIA 2014.
Members of the team regularly sat on the program committees of ISMAR , MICCAI (Int. Conf. on Medical Image Computing), ISBI (Int. Symposium on Biomedical Imaging), ICPR (Int. Conf. on Pattern Recognition).

10 Services as expert or evaluator

Marie-Odile Berger was external reviewer of 10 PhD thesis during the period. F. Sur and E. Kerrien were member of one PhD thesis. She is president of AFRIF (Association Française pour la reconnaissance et l'interprétation des formes). She was external reviewer for the HCERES evalution of LTSI (Rennes). She is a member of the Inria evaluation committee.

11 Collaborations

- We have built strong collaborations with Nancy University Hospital [365], GE Healthcare [316, 317], and MIMESIS Inria project-team [347, 348, 336]. Such collaborations are vital to our activity driven by the application to interventional radiology and our will to have clinically validated algorithms and solutions. Fruitful collaborations are about the use of biomechanical models in AR medical applications [329, 326, 298].

- Still in the medical field, the collaboration with the University of Banghor aims at improving existing solutions of respiration models based on optimization-driven models [346, 311, 312].

- Collaborations with Institut Pascal (Université de Clermont-Ferrand) are about the design of image processing tools for experimental mechanics. We bring a solid foundation to methods that are used as "off-the-shelf" tools in the experimental mechanics community, and tackle problems that give contributions both in experimental mechanics and in image processing [305, 307, 308].

12 External support and funding

- ANR IDeaS: Image Driven Simulation applied to interventional neuroradiology [336].
- ANR ARTIS: automatic construction of a speaker's model from various imaging modalities [330, 332, 290].
- ANR Visac: acquisition of synchronized audio-visual sequences and face reconstruction at a high frame rate [300].
- TIMEX (funded by GDR ISIS) aims at investigating image processing tools for enhancing the metrological performances of contactless measurement systems in experimental mechanics [305, 296].
- SOFA-InterMedS: aimed at developing the field of Medical Simulation research [289, 287] .
- GE Healthcare: CIFRE grant about reconstruction of tools in interventional neuroradiology [316].
- Region lorraine: funding of Guevara's PhD thesis about AR-based clinical procedures for liver surgery.

Involvement with social, economic and cultural environment

One of our goal is to allow significant progress of AR technologies and to widen the application field of AR. We have thus developed several cutting edge applications where AR is likely to give new and improved ways to perform highly technical tasks:

- in neuroradiology and hepatic surgery, we have promoted the use of AR and simulation in the clinical routine and the training of junior physicians to complex interventional clinical gestures. This was achieved in closed collaboration with clinical partners (CHU Nancy, école de chirurgie) and industrial partners (GE Healthcare).
- in the area of education, we designed an inquiry-based AR learning environment (AIBLE) for teaching and learning astronomy in primary school [319].

Members of the team participate on a regular basis, to scientific awareness and mediation actions. Erwan Kerrien is Chargé de Mission for scientific mediation at Inria Nancy-Grand Est.

Involvement in training through research

Both the four assistant professors and the two researchers of the team have teaching activities at master level in image processing, computer vision, shape recognition, augmented reality mainly in the computer science Master of Nancy and in several Engineering Schools near Nancy (Mines Nancy, SUPELEC Metz, ENSG). Our goal is to attract Master students with good skills in applied mathematics towards the field of computer vision. Overall, about 150 teaching hours are given by the members of the team in the field of image processing and computer vision.

Computational Geometry

Synopsis

1 Team Composition

Faculty staff & researchers.

Olivier Devillers (DR INRIA, since Nov. 2014)
Laurent Dupont (MCF, UL)
Xavier Goaoc (CR INRIA, until)
Sylvain Lazard (DR INRIA)
Guillaume Moroz (CR INRIA)
Sylvain Petitjean (DR INRIA, until Sept. 2012)
Marc Pouget (CR INRIA)
Monique Teillaud (DR INRIA, since Nov. 2014)

	PR	MCF	DR	CR	Total
2011	-	1	2	3	6
2016	-	1	3	2	6

Post-docs and engineers. Marc Fuentes (engineer, 3 months 2011), Rémi Imbach (postdoc Inria, Nov. 2014 - Oct. 2016), Laurent Veysseire (postdoc Inria, Dec. 2014 - Aug. 2015).

Doctoral students. Guillaume Batog (MENESR, 2009-11), Yacine Bouzidi (Inria, 2010-14), Iordan Iordanov (UL, 2016-current). The following PhD students, although not in Nancy, are (co-)supervised by team members: Rémy Thomasse (Inria Sophia Antipolis, 2012-15), Ranjan Jha (Nantes, 2013-current), Sény Diatta (Sénégal, 2014-current).

Phd's defended	3	On-going PhD's	3

Team evolution. Departures: X. Goaoc got a professor position in Paris. S. Petitjean became the director of Inria Nancy Grand Est and as a consequence, he temporarily left the team. Arrivals: M. Teillaud and O. Devillers moved to Vegas from the Geometrica group at Inria Sophia Antipolis - Méditerranée.

2 Life of the team

With 6 faculty members, our team has a reasonable size and we get along very well. As a consequence, we succeed in running the team in a collegial manner, both in terms of administration and research.

3 Research topics

Keywords. Geometric computing, non-linear and effective computational geometry, robustness, computer algebra, algebraic systems, probabilistic analysis.

Research area and main goals. Our main scientific objective is to *contribute to the development of an effective geometric computing* dedicated to *non-trivial geometric objects*. Included among its main tasks are the study and development of new algorithms for the manipulation of geometric objects, the experimentation of algorithms, the production of reliable, quality software. Our main axes of research focus on various aspects of computational geometry, in particular, on problems that deal with non-linear objects and with combinatorial and probabilistic properties of data structures and algorithms.

4 Main Achievements

⋆ *Certified drawing of plane algebraic curves.* Our work on the topology of plane algebraic curves, though not finished, led to both great theoretical and applied results. From a theoretical perspective we succeeded, in a nutshell, to decrease the worst-case bit complexity of solving bivariate algebraic systems via rational parameterizations from $\widetilde{O}_B(d^{12} + d^{10}\tau^2)$[DET09, Thm 19] to $\widetilde{O}_B(d^6 + d^5\tau)$ and we presented even more efficient $\widetilde{O}_B(d^5 + d^4\tau)$ Las Vegas algorithms. Improving further these bounds would essentially require to improve bounds on several other fundamental problems (such as computing resultants, checking the squarefreeness of univariate polynomials, and isolating their roots) that have hold for decades. On the practical side, we are in the process of developing Isotop 3, the third version of our curve isotopy software and preliminary results are impressive; see Section 7 for details.

⋆ *The worst visibility walk in a random Delaunay triangulation is* $O(\sqrt{n})$. We show that the memoryless routing algorithms Greedy Walk, Compass Walk, and all variants of visibility walk based on orientation predicates are asymptotically optimal in the average case on the Delaunay triangulation. This settle a long-standing conjecture in point location using walking algorithms.

⋆ *Multinerves and Helly numbers of acyclic families.* See Section 8.

5 Research activities

Non-linear computational geometry

Description. Our team is one of the few in the world to attack all the aspects, from theory to practice, needed for the *development of certified, effective geometric computing* dedicated to *non-discretized, non-linear* problems.

Among the main characteristics of our project are: the belief that the classical geometric and algebraic machinery, when adroitly set into motion, can dramatically enhance the algorithmic knowledge concerning curved objects; the understanding that practical efficiency is as important as theoretical complexity in algorithmic design; and the willingness to cover the whole spectrum of exact geometric computing going from a proven characterization of geometric degeneracies to the production of versatile, reliable and scalable quality software.

Main results.

⋆ *Topology of real algebraic plane curves and solving bivariate systems.* We addressed the classical and difficult problem of computing the topology/isotopy of an algebraic plane curve, that is, computing an arrangement of polylines isotopic to the input curve. This problem is important as it permits to plot

[DET09] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *J. Symb. Comput.*, 44(7):818–835, 2009.

such curves in a certified way, that is without missing branches or self-intersections. We started working on this problem in 2007 and we distributed the first version of our software, Isotop, in 2010, the second version, Isotop 2, in 2013 and we are currently developing a third version (see Section 7 for details).

Since 2011, we focused our efforts on the key issue of computing the critical points of such curves and we addressed the slightly more general problem of solving bivariate algebraic systems. We are interested in certified numerical approximations or, more precisely, isolating boxes of the solutions. But we are also interested in computing, as intermediate symbolic objects, a Rational Univariate Representation (RUR) that is, roughly speaking, a univariate polynomial and two rational functions that map the roots of the univariate polynomial to the two coordinates of the solutions of the system. RURs are relevant symbolic objects because they allow to turn many queries on the system into queries on univariate polynomials. In this context, solving a system amounts to solving three distinct problems: (i) computing a separating linear form of the input system, that is a linear combination of the two variables that takes different values when evaluated at the distinct solutions of the system, (ii) computing the RUR associated to this separating linear form, and (iii) computing isolating boxes of the solutions from the RUR.

Over the course of the last five years, we presented several algorithms on these problems, which drastically improved the state of the art [377, 382, 403, 404, 405, 423, 431, 444]. Namely, in 2011, the best known bit complexity for solving these three problems were, respectively, (i) $\widetilde{O}(d^{10} + d^9\tau)$, (ii) $\widetilde{O}(d^7 + d^6\tau)$, and (iii) $\widetilde{O}(d^{12} + d^{10}\tau^2)$ in the worst case for input bivariate polynomials of degree at most d with integer coefficients of bitsize at most τ ($\widetilde{O}$ refers to complexities where polylogarithmic factors are omitted).[GVEK96][DET09, Thm 19] We improved these bit complexities to $\widetilde{O}(d^6 + d^5\tau)$ in the worst-case for all three problems and to $\widetilde{O}(d^5 + d^4\tau)$ on average in a Las Vegas setting for the first two problems (no expected Las Vegas complexity better than the worst case was known). Furthermore, these complexities are not likely to be easily improved as it would essentially requires to improve bounds on several fundamental problems (such as computing resultants, checking the squarefreeness of univariate polynomials and isolating their roots) that have hold for decades.

Related to these problems, we also presented algorithms and experimentations on numerical and certified approaches for computing the topology of curves in the restricted settings of the 2D projection of smooth space curves [416, 441]. We also distributed a library (Fast_polynomial, url) for fast polynomial evaluations and compositions [445].

⋆ *Parallel robots.* Parallel manipulators are mechanical systems that uses several linear actuators to control a single end-effector. The best known one is formed from six linear actuators that support a movable platform for devices such as flight simulators. Moving a parallel robot toward specific parametric values can break it and a challenge is to describe these singularities in order to avoid them. Another challenge is to design parallel manipulators that have no singularities in some possibly restricted settings. Using tools from algebra such as CAD and Gröbner bases, we obtained quite a few results in this area.

We showed how to compute the working space and set of singularities of several types of robots, such as simple planar cable robots [409], planar mechanisms with three degrees of freedom [399], spatial mechanisms with six degrees of freedom [384], Delta like family robots [418]. We proposed a method for designing mechanisms with no singularities for a specific family of planar parallel robots with two degrees of freedom [408]. Finally, we proposed a method to check the singularity-free paths for parallel robots [417].

⋆ *Algebraic methods in classical Computational Geometry.* Algebraic methods can help solving problems in classical computational geometry. Using, in particular, polynomials multi-point evaluation, we showed that it is possible to compute efficiently, that is in almost linear time instead of quadratic time,

[GVEK96] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. of Complexity*, 12(4):527–544, 1996.

[DET09] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *J. Symb. Comput.*, 44(7):818–835, 2009.

the distance between two piecewise-linear terrains, each defined over a triangulated domain of size n [419]. Also, using algebraic mixed volume theory and stochastic optimization methods, we succeeded to improve upper and lower bounds on the number of embeddings of a given rigid graph [415].

Combinatorics and combinatorial geometry

Description. The geometry of a problem can often be encapsulated into elementary combinatorial or topological structures that are then studied at a more abstract level. The use of Davenport-Schintzel sequences to study complexity questions on (sub-structures of) arrangements is, perhaps, the most classic example in computational geometry. We study geometric problems along these lines.

Main results.

⋆ *Helly numbers of acyclic families.* The nerve of a family of sets is a simplicial complex that records the intersection pattern of its subfamilies. Nerves are widely used in computational geometry and topology, because the nerve theorem guarantees that the nerve of a family of geometric objects has the same topology as the union of the objects, if they form a good cover.

We relaxed the good cover assumption to the case where each subfamily intersects in a disjoint union of possibly several homology cells, and we proved a generalization of the nerve theorem in this framework, using spectral sequences from algebraic topology. We then deduced a new topological Helly-type theorem that unifies previous results of Amenta, Kalai and Meshulam, and Matoušek. This Helly-type theorem is used to (re)prove, in a unified way, bounds on transversal Helly numbers in geometric transversal theory [388], [410] (best paper award).

⋆ *Set systems and families of permutations with small traces.* How large can be a family of combinatorial objects defined on a finite set if its number of distinct projections/traces on any small subset is bounded? For set systems, we generalized Sauer's Lemma on the size of set systems with bounded VC-dimension. We also obtained a similar result on families of permutations. One motivation for considering these questions is the "geometric permutation problem" in geometric transversal theory, a question that has been open for two decades [387].

⋆ *Simplifying inclusion-exclusion formulas.* The classical *inclusion-exclusion formula* asserts that the measure of a union of n sets can be expressed using measures of various intersections. However, the number of terms in this formula is exponential in n and a lot of research has been devoted to constructing simpler formulas for particular families. We proved that any family of sets admits an inclusion-exclusion formula of size quasi-polynomial in n and in the size of its Venn diagram [424, 396].

Probabilistic computational geometry

Description. In computational geometry, worst-case complexity bounds often fail to capture practical behaviours. As a consequence, when the worst-case analysis is deemed overly pessimistic, average-case analysis of data-structures or algorithms is commonly used. Since such analyses are often intricate, the models of random geometric data that can be handled are often simplistic and far from "realistic inputs". We worked during this evaluation period on probabilistic models and analyses.

Main results.

⋆ *Complexity analysis of random geometric structures made simpler.* We presented a new simple scheme for the analysis of geometric structures. While this scheme only produces results up to a polylog factor, it is much simpler to apply than the classical techniques and therefore succeeds in analyzing new input distributions related to smoothed complexity analysis. We illustrated our method on two classical structures: convex hulls and Delaunay triangulations [412].

⋆ *The worst visibility walk in a random Delaunay triangulation is $O(\sqrt{n})$.* We show that the memoryless routing algorithms Greedy Walk, Compass Walk, and all variants of visibility walk based on ori-

entation predicates are asymptotically optimal in the average case on the Delaunay triangulation. More specifically, we consider the Delaunay triangulation of an unbounded Poisson point process of unit rate and demonstrate that the worst-case path between any two vertices inside a domain of area n has a number of steps that is not asymptotically more than the shortest path between those two vertices with probability converging to one (as long as the vertices are sufficiently far apart.) It follows that the worst-case path has $O(\sqrt{n}\,)$ steps in the limiting case, under the same conditions. Our results have applications in routing in mobile networks and also settle a long-standing conjecture in point location using walking algorithms. Our proofs use techniques from percolation theory and stochastic geometry [437].

⋆ *Smooth analysis of convex hulls.* We establish an upper bound on the smoothed complexity of convex hulls in $\mathbb{R}^d$ under uniform Euclidean (ℓ^2) noise. Namely, given n arbitrary points in the unit ball in $\mathbb{R}^d$, each perturbed independently in the unit ball of radius δ, we bound the expected complexity of their convex hull in terms of n and δ [411].

⋆ *Monotonicity of the number of facets of random polytopes.* We proved a result on the size of the convex hull of n points sampled uniformly in a convex smooth set in $\mathbb{R}^d$: the number of facets (i.e. faces of dimension $d-1$) is asymptotically increasing. This result, although not surprising, is remarkably difficult and requires delicate random sampling arguments [389].

⋆ *Worst-case silhouette size of random polytopes.* We studied the size of the silhouette of a polyhedron from a probabilistic point of view. If the polyhedron is a random approximation of the sphere, we have proven that the expected complexity of the silhouette is also $\Theta(\sqrt{n})$ for the worst possible view point [439]. This work was submitted in 2014 to the *Journal of Computational Geometry* and is conditionally accepted.

Classical computational geometry

Description. Along our lines of research described above, we pursue some research on more classical problems in computational geometry.

Main results.

⋆ *Bounded-Curvature Shortest Paths.* We considered the car-like robots path-planning problem of computing shortest paths having curvature at most one almost everywhere and visiting a sequence of n points in the plane in a given order. We showed that this problem reduces to a family of convex optimization problems over polyhedra in $\mathbb{R}^n$ [394]. This is the first result where convex optimization is shown to be applicable in this context.

⋆ *Geometric graph theory.* A set of points is said universal if it supports a crossing-free drawing of any planar graph (on n vertices). We obtained several results on this topic. In 2010, we exhibited universal point sets of size n if edges can be drawn as polylines with at most one bend, which can be placed arbitrarily. If the bend points are also required to be chosen in the universal set, we proved the existence of universal sets of subquadratic size $O(n^2/\log n)$ [391]. We also proved that, surprisingly, there exist universal point sets of size n if edges can be drawn as a circular arcs [380].

⋆ *Approximating Geodesics in Meshes.* The so-called *Farthest Point Sampling* (FPS) is a classical algorithm used extensively and successfully for isometry-invariant surface processing. We analyzed the stretch factor $\mathcal{F}_{FPS}$ of approximate geodesics computed using FPS, which is the maximum, over all pairs of distinct vertices, of their approximated distance over their geodesic distance in a given graph. We showed that $\mathcal{F}_{FPS}$ can be bounded in terms of the minimal value of the stretch factor obtained using an optimal placement of k sources. This provides some evidence explaining why farthest point sampling has been used successfully for isometry-invariant shape processing. We also showed that it is NP-complete to find k sources that minimize the stretch factor [443]. This work has been conditionally accepted in CGTA.

⋆ *Visibility complex.* We presented two fundamental lower bounds on the worst-case combinatorial complexity of sets of free lines and sets of maximal free line segments in the presence of balls in three dimensions. The main one proves that the visibility complex of n disjoint *unit* balls, or equivalently the set of maximal non-occluded line segments among n disjoint unit balls, has complexity $\Omega(n^4)$, which matches the trivial $O(n^4)$ upper bound. This result settled, negatively, the conjecture that this set of line segments, or, equivalently, the visibility complex, has smaller worst-case complexity for disjoint fat objects than for skinny triangles [393].

⋆ *Qualitative Symbolic Perturbation: a new geometry-based perturbation framework.* In a classical Symbolic Perturbation scheme, degeneracies are handled by substituting some polynomials in ϵ to the input of a predicate. Instead of a single perturbation, we propose to use a sequence of (simpler) perturbations. Moreover, we look at their effects geometrically instead of algebraically; this allows us to tackle cases that were not tractable with the classical algebraic approach [438].

⋆ *Recognizing shrinkable complexes is NP-complete.* We say that a simplicial complex is shrinkable if there exists a sequence of admissible edge contractions that reduces the complex to a single vertex. We prove that it is NP-complete to decide whether a (three-dimensional) simplicial complex is shrinkable [401]. Along the way, we describe examples of contractible complexes which are not shrinkable.

Scientific production and quality

6 Synthesis of publications

	2011	2012	2013	2014	2015	2016	Total
PhD Thesis	1			1	1		3
H.D.R	1						1
Journal	4	4	4	2	2	5	21
Conference proceedings	5	4	5	4	5	2	25
Book chapter				1	1		2
Book or special issue (edited)					3		3

List of top journals in which we have published

Discrete and Computational Geometry (4) [381, 393, 395, 383]
Journal of Symbolic Computation (2) [397, 382]
Computational Geometry: Theory and Applications (3) [385, 398, 391]
ASME Journal of Mechanisms and Robotics (2) [384, 399]
SIAM Journal on Computing (1) [394]
Advances in Mathematics (1) [388]
ACM Transactions on Algorithms (1) [400]

List of top conferences in which we have published

SoCG – Symposium on Computational Geometry (5) [410, 412, 411, 402, 413]
ISSAC –International Symposium on Symbolic and Algebraic Computation (3) [403, 405, 404]
Symposium on Advances in Robot Kinematics (2) [406, 408]
International Design Engineering Technical Conferences & …(3) [407, 409, 417]
SODA – Symposium on Discrete Algorithms (1) [419]
ESA – European Symposium on Algorithms (1) [401]

7 Software

Isotop 2 & 3: Isotopy of plane algebraic curves. We develop the software, Isotop, for computing the topology/isotopy of an implicit algebraic plane curve or, in other words, for plotting such curves in a certified way (without missing connected components, singular points, etc.). See Section 5 for details.

We distributed the first version of our software in 2010, the second version, Isotop 2, in 2013 and we are currently developing a third version. It is is developed with F. Rouillier from INRIA Paris - Rocquencourt, distributed under a free for non-commercial use license and it can also be queried via a web interface (url).

We performed extensive benchmarking with Isotop 2 and, although timings ratio depend substantially on instances, it is quite uniformly faster than its contenders (Regular Chains, 2011, Moreno Maza et al.; Lgp, 2009, Cheng, Gao and Li; CA, 2007, Eigenwillig, Kerber, and Wolpert; FastAnalysis, 2011, Berberich, Emeliyanenko, Kobel, and Sagraloff) [377]. In addition, Isotop 3 is quite drastically faster than Isotop 2.

An interesting example is the so-called *ridge* curve,[CFPR08] which has total degree 84, 1907 monomials with integer coefficients of 53 digits, 1432 extreme points and 909 singlar ones. In 2008, computing its topology, or even just its critical points, was not reachable without manually driving the computations using computer algebra savoir-faire and some information on the structure of the curve. This curve was still out of reach by blackbox software in 2010 when we first distributed Isotop. In 2013, Isotop 2 was able to handle that curve in 10mn on a 8-thread laptop. With Isotop 3, we are now able to handle that curve in less than a minute, while still no contender can handle this curve.

QI: Quadrics intersection. QI is the first and only exact, robust, efficient and usable implementation of an algorithm for parameterizing the intersection of two arbitrary quadrics, given in implicit form with integer coefficients.[DLLP08]

We mostly developed QI during the previous evaluation period. However, it was initially developed on the library LiDIA, which has become deprecated. We hired an engineer for three months in 2011/12 to make QI independent of LiDIA. The new code is running and accessible on the QI webpage (url).

Fast polynomial evaluation and composition. We developed the library *fast_polynomial* to explore different divide-and-conquer strategies for evaluating univariate polynomials and perform polynomial compositions [445] (url). Experimentally, our library is always faster than our implementation of previous state-of-the-art divide-and-conquer scheme. It has been submitted for integration in the computer algebra system *Sage*.

Academic reputation and appeal

Refer to the appendix for details.

8 Prizes and Distinctions

Best papers. Helly numbers of acyclic families: best paper award at SoCG 2012 [410] and published in Advances in mathematics [388]. This paper unifies several Helly-type theorems in and outside geometric transversal theory, and generalizes the nerve theorem, a result that is fundamental in topological data analysis. As a consequence, it was well received in both mathematic and computer science communities. See Section 5 for details.

Invited talks and participations to invitation-only workshops. Team members were invited speakers at the École Jeunes Chercheurs en Informatique Mathématique in 2012 (url) and the ALEA days in 2013

[CFPR08] F. Cazals, J.-C. Faugère, M. Pouget, and F. Rouillier. Ridges and umbilics of polynomial parametric surfaces. In B. Juttler and R. Piene, editors, *Geometric Modeling and Algebraic Geometry*, chapter 3, pages 141–159. Springer, 2008.

[DLLP08] Laurent Dupont, Daniel Lazard, Sylvain Lazard, and Sylvain Petitjean. Near-optimal parameterization of the intersection of quadrics: I. The generic algorithm, II. A classification of pencils, III. Parameterizing singular intersections. *Journal of Symbolic Computation*, 43(3):168–232, 2008.

(url). Team members were invited to 10 (counted with multiplicity) invitation-only workshops such as Dagstuhl, Bellairs, Banff and Oberwolfach workshops.

9 Editorial and organizational activities

Program and Paper Committees. Team members participated to 5 PC committees in Computational Geometry (SoCGx2, WoCG, EuroCGx2); the usual working load in SoCG PCs is about 30+ papers to review, thus the number of participations necessarily small. We also participated to 2 PCs in vision (CVPR and ICCV).

Editorial responsibilities. Team members are editors of the journals *Graphical Models*, *Journal of Computational Geometry* (JoCG), *Computational Geometry: Theory and Applications* (CGTA), and *International Journal of Computational Geometry and Applications* (IJCGA). We are also member of the Cgal Editorial Board and we edited a special issue in *Discrete and Computational Geometry* (DCG).

Steering committees. We are member of the steering committee of the *European Symposium on Algorithms* (ESA) and the one for the colocation of the *Symposium on Theory of Computing* (STOC) and the *Symposium on Computational Geometry* (SoCG) in 2016.

Workshop organizations. Our team regularly organizes various workshops with, in particular, 3 one-week French workshops and 8 one-week international workshops during the evaluation period.

10 Services as expert or evaluator

Thesis and habilitation committees. We participated to 6 PhD committees including 2 as external examiners. We also participated to 1 Habilitation committee. (These number are naturally rather small because of the size of our community.)

Other responsibilities. A non-exhaustive list of our main other responsibilities is as follows: Head of LORIA Department 1. Member of the Executive committee of LORIA. Head of the hiring committee for PhD and postdoc positions at INRIA Nancy Grand Est. LORIA representative in hiring committees for UL MCF positions in 2011, 2012, and 2016. President of hiring committees for UL Prof positions in 2015 and 2016. Member of hiring committees for another UL Prof position and for INRIA CR positions in 2016. Member of the LORIA laboratory council. Member of the Commission Information Scientifique Inria/Loria. LORIA representative in the Council of the Charles Hermite Research Federation. Correspondant Europe of INRIA Nancy Grand-Est. Deputy head of INRIA Nancy – Grand Est in charge of scientific aspects (*Délégué scientifique*). Member of the Executive committee of INRIA Nancy – Grand Est. Member of its *Commission des développements technologiques* (Commission for technologic development). Director of the Department *Services et réseaux de communication* of IUT Charlemagne. Member of the *Commission Pédagogique Nationale* Infocom/SRC. Chairman of the INRIA COST- GTRI committee. Member of INRIA's Evaluation committee. Member of the Scientific Board of the *Société Informatique de France* (SIF).

11 Collaborations

We have a large set of collaborators with 18 co-authors within France and 34 abroad over the evaluation period. Among our strongest collaborations, we maintain a very close collaboration with F. Rouillier [382, 399, 403, 404, 405, 407, 417, 418, 423, 431, 444] and M. Glisse [385, 389, 393, 401, 411, 412, 434, 435, 439] both from Inria Paris. We also have a strong long-term collaboration with O. Cheong (KAIST, Korea) [381, 385, 386, 387, 428] and occasional collaborations with B. Aronov (New York University, USA) [381, 400, 419].

12 External support and funding

ANR Presage (Leader) *Probabilistic methods for the efficiency of geometric structures and algorithms*. ANR Blanc, 2011-2015 with EPI Geometrica and University of Rouen. Budget of 106kE for Vegas and a total budget of 416kE for all partners. (Url.)

PEPS Rupture - INS2I: Manifold (2011). *Mixing Algebraic and Numerical Investigations of maniFOLDS*. PEPS, 2011, with IRCCyN and LINA labs. Total budget of 10 kE.

ANR SingCAST (Leader) *Singular Curves and Surfaces Topology*. Young-researcher ANR, 2014-2017. Total budget of 100kE. (Url.)

Involvement with social, economic and cultural environment

G. Moroz is member of the committee for the Olympiades de mathématiques.

Involvement in training through research

Our group is involved in training of qualified personnel at different levels. S. Lazard is member of the board for computer science in the Doctoral school of Lorraine University. He is also the representative for Nancy of the Inria *Young researcher council* (url), and head of the hiring committee for PhD and postdoc positions at INRIA Nancy Grand Est. We offer a specialty course in the UL Computer Science Master's program and we intervene in the Master's program of the Geology school.

1 References for ABC

Doctoral Dissertations

[1] R. Bonidal, *Model selection using regularization path for quadratic cost support vector machines*, Theses, Université de Lorraine, June 2013, https://hal.archives-ouvertes.fr/tel-01264027.

[2] H. Chouarfia, *Prédiction de la structure protéique*, Thèse de doctorat, USTO (Algérie), 2014.

[3] E. Klein, *Contributions à l'apprentissage par renforcement inverse*, Thèse de doctorat, Université de Lorraine, 2013.

[4] V. L. Le, *Hybrid Dynamical System Identification: Geometry, Sparsity, and Nonlinearities*, PhD Thesis, Université de Lorraine, 2013, https://hal.archives-ouvertes.fr/tel-00874283.

Articles in International Peer-Reviewed Journal

[5] F. Abdat, M. Amouroux, Y. Guermeur, W. C. Blondel, "Hybrid feature selection and SVM-based classification for mouse skin precancerous stages diagnosis from bimodal spectroscopy", *Optics Express 20*, 1, January 2012, p. 228–244, https://hal.archives-ouvertes.fr/hal-00757157.

[6] R. Bonidal, S. Tindel, Y. Guermeur, "Model Selection for the l2-SVM by Following the Regularization Path", *Transactions on Computational Collective Intelligence 13*, 2013, p. 83–112, 34 p., https://hal.archives-ouvertes.fr/hal-00849720.

[7] M. Cadot, A. Lelu, "Combining Explicitness and Classifying Performance via MIDOVA Lossless Representation for Qualitative Datasets", *International Journal On Advances in Software 5*, 1&2, 2012, p. 1–16, accepted, https://hal.archives-ouvertes.fr/hal-00596718.

[8] Cheng Soon Ong, Le Thi Hoai An, "Learning sparse classifiers with difference of convex functions algorithm", *Optimization Methods and Softwar 28*, 4, 2013, p. 830–854.

[9] P. Cuxac, A. Lelu, M. Cadot, "Paving the way for next generation data-stream clustering: towards a unique and statistically valid cluster structure at any time step", *international journal of data mining modelling and management 3*, 4, 2011, p. 341–360, https://hal.archives-ouvertes.fr/hal-00952855.

[10] Y. Guermeur, E. Monfrini, "A Quadratic Loss Multi-Class SVM for which a Radius-Margin Bound Applies", *Informatica (ISSN 0868-4952) International Journal 22*, 1, 2011, p. 73–96, https://hal.archives-ouvertes.fr/hal-00596121.

[11] Y. Guermeur, "A Generic Model of Multi-class Support Vector Machine", *IJIIDS 6*, 6, 2012, p. 555–577, https://hal.archives-ouvertes.fr/hal-00596175.

[12] Y. Guermeur, "Comments on: Support vector machines maximizing geometric margins for multi-class classification", *TOP - An Official Journal of the Spanish Society of Statistics and Operations Research 22*, 2014, p. 844–851, https://hal.archives-ouvertes.fr/hal-01263912.

[13] F. Lauer, G. Bloch, R. Vidal, "A continuous optimization framework for hybrid system identification", *Automatica 47*, 3, January 2011, p. 608–613, https://hal.archives-ouvertes.fr/hal-00559369.

[14] F. Lauer, Y. Guermeur, "MSVMpack: a Multi-Class Support Vector Machine Package", *Journal of Machine Learning Research 12*, 2011, p. 2269–2272, https://hal.archives-ouvertes.fr/hal-00605009.

[15] F. Lauer, H. Ohlsson, "Finding sparse solutions of systems of polynomial equations via group-sparsity optimization", *Journal of Global Optimization 62*, 2, 2015, p. 319–349, https://hal.archives-ouvertes.fr/hal-00908072.

[16] F. Lauer, "Estimating the probability of success of a simple algorithm for switched linear regression", *Nonlinear Analysis: Hybrid Systems 8*, 2013, p. 31–47, https://hal.archives-ouvertes.fr/hal-00743954.

[17] F. Lauer, "On the complexity of piecewise affine system identification", *Automatica 62*, 2015, p. 148–153, https://hal.archives-ouvertes.fr/hal-01195700.

[18] F. Lauer, "On the complexity of switching linear regression", *Automatica*, 2016, provisionally accepted, https://hal.archives-ouvertes.fr/hal-01219794.

[19] V. L. Le, G. Bloch, F. Lauer, "Reduced-size kernel models for nonlinear hybrid system identification", *IEEE Transactions on Neural Networks 22*, 12, December 2011, p. 2398–2405, https://hal.archives-ouvertes.fr/hal-00596049.

[20] V. L. Le, F. Lauer, G. Bloch, "Selective l1 minimization for sparse recovery", *IEEE Transactions on Automatic Control 59*, 11, November 2014, p. 3008–3013, https://hal.archives-ouvertes.fr/hal-00904836.

[21] Le Hoai Minh, Le Thi Hoai An, Pham Dinh Tao, Huynh Van Ngai, "Block Clustering based on DC programming and DCA", *Neural Computation 25*, 10, 2013, p. 2776–2807.

[22] Le Thi Hoai An, Le Hoai Minh, Pham Dinh Tao, Ngai Van Huynh, "Binary classification via spherical separator by DC programming and DCA", *J. Global Optimization 56*, 4, 2013, p. 1393–1407.

[23] Le Thi Hoai An, Le Hoai Minh, Pham Dinh Tao, "New and efficient DCA based algorithms for Minimum Sum-of-Squares Clustering", *Pattern Recognition 47*, 1, 2014, p. 388–401.

[24] T. Pham Dinh, H. M. Le, H. A. Le Thi, F. Lauer, "A Difference of Convex Functions Algorithm for Switched Linear Regression", *IEEE Transactions on Automatic Control*, 2014, https://hal.archives-ouvertes.fr/hal-00931206.

Invited Conferences

[25] W. Blondel, F. Abdat, M. Amouroux, Y. Guermeur, "Spatially resolved multimodality spectroscopy for in vivo diagnosis of skin precancer: recent developments in data extraction and classification", *in : 15th International Conference on Laser Optics 2012, LO 2012*, St Petersburg, Russia, June 2012. Session organisée uniquement avec des invités... http://laseroptics.ru/download/LO2012_Technical_Program_final.pdf, https://hal.archives-ouvertes.fr/hal-00757303.

Major International Conferences

[26] F. Abdat, M. Amouroux, Y. Guermeur, W. Blondel, "DCT-SVM based multi-classification of mouse skin precancerous stages from autofluorescence and diffuse reflectance spectra", *in : European Conferences on Biomedical Optics, ECBO 2011*, p. CDROM, Munich, Germany, May 2011, https://hal.archives-ouvertes.fr/hal-00597255.

[27] L. Bako, V. L. Le, F. Lauer, G. Bloch, "Identification of MIMO switched state-space models", *in : American Control Conference, ACC 2013*, p. CD–ROM, Washington, United States, June 2013, https://hal.archives-ouvertes.fr/hal-00798991.

[28] R. Bonidal, F. Thomarat, Y. Guermeur, "Estimating the class posterior probabilities in biological sequence segmentation", *in : SMTDA 2012*, *SMTDA 2012*, Chania, Greece, June 2012, https://hal.archives-ouvertes.fr/hal-01263982.

[29] J. Busset, M. Cadot, "Démêler les actions des articulateurs en jeu lors de la production de parole avec le logiciel C.H.I.C. : Analyse de séquences de radiographies de la tête.", *in : 6th International Conference Implicative Statistic Analysis - A.S.I. 6 - 2012*, p. 291–305, Caen, France, November 2012, https://hal.archives-ouvertes.fr/hal-00759054.

[30] M. Cadot, A. Lelu, "Representing interaction in multiway contingency tables: MIDOVA, CA and log-linear model", *in : 6th International Conference on Correspondence Analysis and Related Methods - CARME 2011*, J. Blasius, M. Greenacre, J. Pagès (editors), Jérôme Pagès, Rennes, France, February 2011, https://hal.inria.fr/inria-00547886.

[31] B. Delprat, M. Hallab, M. Cadot, A. Lelu, "Processing a Mayan Corpus for Enhancing our Knowledge of Ancient Scripts", *in : 4th International Conference on Information Systems and Economic Intelligence - SIIE'2011*, E.-U. la Manouba (Tunisia), N. U. (France), I. (Morocco), I. M. section (editors), IGA Maroc, p. 198–208, Marrakech, Morocco, February 2011, https://hal.archives-ouvertes.fr/hal-00577958.

[32] E. Didiot, F. Lauer, "Efficient Optimization of Multi-class Support Vector Machines with MSVMpack", *in : Modelling, Computation and Optimization in Information Systems and Management Sciences (MCO 2015)*, N. N. T. Le Thi Hoai An, Pham Dinh Tao (editor), *Modelling, Computation and Optimization in Information Systems and Management Sciences, Proceedings of MCO 2015*, Springer, Metz, France, May 2015, https://hal.archives-ouvertes.fr/hal-01134774.

[33] Y. Guermeur, F. Thomarat, "Estimating the Class Posterior Probabilities in Protein Secondary Structure Prediction", *in : PRIB 2011*, p. 260–271, Delft, Netherlands, November 2011, https://hal.archives-ouvertes.fr/hal-00616640.

[34] E. Klein, M. Geist, O. Pietquin, "Batch, Off-policy and Model-free Apprenticeship Learning", *in : EWRL 2011*, p. 1–12, Athens, Greece, September 2011, https://hal-supelec.archives-ouvertes.fr/hal-00660623.

[35] E. Klein, M. Geist, O. Pietquin, "Batch, Off-policy and Model-Free Apprenticeship Learning", *in : IJCAI Workshop on Agents Learning Interactively from Human Teachers (ALIHT 2011)*, p. 6 pages, Barcelona, Spain, June 2011, https://hal-supelec.archives-ouvertes.fr/hal-00596370.

[36] E. Klein, M. Geist, O. Pietquin, "Reducing the dimentionality of the reward space in the Inverse Reinforcement Learning problem", *in : MLASA 2011*, p. 1–4, Honolulu, United States, December 2011, https://hal-supelec.archives-ouvertes.fr/hal-00660612.

[37] F. Lauer, G. Bloch, “Piecewise smooth system identification in reproducing kernel Hilbert space”, *in : 53rd IEEE Conference on Decision and Control, CDC 2014*, Los Angeles, United States, December 2014, https://hal.archives-ouvertes.fr/hal-01059957.

[38] F. Lauer, V. L. Le, G. Bloch, “Learning smooth models of nonsmooth functions via convex optimization”, *in : 22nd International Workshop on Machine Learning for Signal Processing, IEEE-MLSP 2012*, p. CDROM, Santander, Spain, September 2012, https://hal.archives-ouvertes.fr/hal-00719188.

[39] V. L. Le, F. Lauer, L. Bako, G. Bloch, “Learning nonlinear hybrid systems: from sparse optimization to support vector regression”, *in : 16th International Conference on Hybrid systems: computation and control, HSCC 2013*, ACM, p. 33–42, Philadelphia, United States, April 2013, https://hal.archives-ouvertes.fr/hal-00801145.

[40] V. L. Le, F. Lauer, G. Bloch, “Identification of linear hybrid systems: a geometric approach”, *in : American Control Conference, ACC 2013*, p. CD–ROM, Washington, United States, June 2013, https://hal.archives-ouvertes.fr/hal-00799147.

[41] A. Lelu, M. Cadot, “A Proposition for Fixing the Dimensionality of a Laplacian Low-rank Approximation of any Binary Data-matrix”, *in : The Fifth International Conference on Information, Process, and Knowledge Management - eKNOW 2013*, IARIA, p. 70–73, Nice, France, February 2013, https://hal.archives-ouvertes.fr/hal-00773436.

[42] L. Maxim, M. Cadot, P. Mansier, “Should scientists communicate uncertainty to the public in health controversies? The case of endocrine disrupters’ effects on male fertility”, *in : GPSSA Conference (Great Plains society for the study of arGumentation): Between Scientists & Citizens: Assessing Expertise In Policy Controversies - 2012*, J. Goodwin (editor), CreateSpace, p. 263–274, Iowa State University, Ames, IA, United States, June 2012. ISBN : 978-1478152347, https://hal.archives-ouvertes.fr/hal-00701749.

[43] F. Thomarat, F. Lauer, Y. Guermeur, “Cascading discriminant and generative models for protein secondary structure prediction”, *in : IAPR International Conference on Pattern Recognition in Bioinformatics, Lecture Notes in Bioinformatics, 7632*, p. 166–177, Tokyo, Japan, 2012, https://hal.archives-ouvertes.fr/hal-01253809.

Articles in National Peer-Reviewed Journal

[44] M. Cadot, D. El Haj Ali, “Modélisation et extraction des liens complexes entre variables. Application à des données socio-économiques”, *Revue des Nouvelles Technologies de l’Information RNTI-E-21*, 2011, p. 27–52, ISBN : 978270568181, https://hal.archives-ouvertes.fr/hal-00596719.

[45] A. Lelu, M. Cadot, “Espace intrinsèque d’un graphe et recherche de communautés.”, *Information - Interaction - Intelligence 2011*, 1, October 2011, p. 1–25, https://hal.archives-ouvertes.fr/hal-00641128.

National Peer-Reviewed Conferences

[46] J. Busset, M. Cadot, “Fouille d’images animées : cinéradiographies d’un locuteur”, *in : FOSTA 2013, atelier de EGC 2013*, p. 1–12, Toulouse, France, January 2013, https://hal.archives-ouvertes.fr/hal-00773448.

[47] M. Cadot, S. Aubin, A. Lelu, “Indexer, comparer, apparier des textes et leurs résumés : une exploration.”, *in : TALN 2011, Atelier DEFT*, l. L. Université Paris-Sud Orsay (editor), p. pages 85–95, Montpellier, France, June 2011. 11 pages, https://hal.archives-ouvertes.fr/hal-00630405.

[48] M. Cadot, Y. Laprie, “Méthodologie 3-way d’extraction d’un modèle articulatoire de la parole à partir des données d’un locuteur”, *in : Atelier Fouille de Données Complexes des 14èmes Journées Francophones ”Extraction et Gestion des Connaissances”*, p. 1–12, Rennes, France, January 2014, https://hal.archives-ouvertes.fr/hal-00934436.

[49] A. Faiza, M. Amouroux, Y. Guermeur, W. Blondel, “Diagnostic in vivo et classification automatique d’états précancéreux cutanés par spectroscopie d’autofluorescence résolue spatialement”, *in : 7ème Journée Claude Huriet de la Recherche médicale de la faculté de médecine et du CHU de Nancy*, Nancy, France, March 2012, https://hal.archives-ouvertes.fr/hal-00757411.

[50] A. Faiza, M. Amouroux, Y. Guermeur, W. Blondel, “Spectroscopie d’AutoFluorescence in vivo résolue spatialement : multiclassification SVM d’états précancéreux améliorée par fusion de sources”, *in : 8ème colloque national Diagnostic et Imagerie Optique en Médecine et Biologie Biophotonique, OPT-DIAG 2012*, Paris XV, France, May 2012, https://hal.archives-ouvertes.fr/hal-00757392.

[51] M. Geist, E. Klein, B. Piot, Y. Guermeur, O. Pietquin, “Around Inverse Reinforcement Learning and Score-based Classification”, *in : 1st Multidisciplinary Conference on Reinforcement Learning and Decision Making (RLDM 2013)*, Princeton, New Jersey, United States, October 2013, https://hal-supelec.archives-ouvertes.fr/hal-00916936.

[52] E. Klein, M. Geist, O. Pietquin, “Apprentissage par imitation dans un cadre batch, off-policy et sans modèle”, *in : JFPDA 2011*, p. 1–9, Rouen, France, June 2011, https://hal-supelec.archives-ouvertes.fr/hal-00652762.

[53] E. Klein, B. Piot, M. Geist, O. Pietquin, “Classification structurée pour l’apprentissage par renforcement inverse”, *in : Conférence Francophone sur l’Apprentissage Automatique - CAp 2012*, p. 1–16, Nancy, France, May 2012. http://cap2012.loria.fr/pub/Papers/13.pdf, https://hal-supelec.archives-ouvertes.fr/hal-00701947.

Book chapters

[54] F. Abdat, M. Amouroux, Y. Guermeur, W. Blondel, “Spectroscopie d’autofluorescence in vivo résolue spatialement : multiclassification SVM d’états précancéreux améliorée par fusion de sources”, *in : Biophotonique Générale Optique & Imageries pour le Diagnostic dans les Sciences du Vivant et en Médecine*, S. Mottin and G. Lelièvre (editors), *Intégrations des savoirs et des savoir-faire*, Publications Mission ressources et compétences technologiques CNRS, Meudon (Hauts-de-Seine), May 2013, p. 556, https://hal.archives-ouvertes.fr/hal-00918854.

[55] M. Cadot, “Modèle des données à base de règles : de la construction au pilotage”, *in : L’analyse statistique implicative - Méthode exploratoire et confirmatoire à la recherche de causalités - 2e édition*, R. Gras, J.-C. Régnier, C. Marinica, and F. Guillet (editors), Cépaduès, March 2013, p. 299–312, https://hal.archives-ouvertes.fr/hal-00801618.

[56] Y. Guermeur, F. Lauer, “A generic approach to biological sequence segmentation problems, application to protein secondary structure prediction”, *in : Pattern Recognition in Computational Molecular Biology: Techniques and Approaches*, M. Elloumi, C. Iliopoulos, J. T. L. Wang,

and A. Y. Zomaya (editors), Wiley, 2016, p. 114–128, https://hal.archives-ouvertes.fr/hal-01253820.

[57] A. Lelu, M. Cadot, "Détecter les ruptures thématiques dans les discours : synergie entre supervision et non-supervision", *in : DEFT*, Hermès, September 2012, p. 49–63, https://hal.archives-ouvertes.fr/hal-00728105.

Other Publications

[58] F. Lauer, H. Ohlsson, "Sparse phase retrieval via group-sparse optimization", working paper or preprint, February 2014, https://hal.archives-ouvertes.fr/hal-00951158.

[59] K. Musayeva, *Statistical Learning for Biological Sequence Segmentation*, Mémoire, Master Informatique de l'UL, 2014.

2 References for ADAGIo

Doctoral Dissertations

[60] A. Krähenbühl, *Segmentation and geometric analysis: application to CT images of wood.*, Theses, Université de Lorraine, December 2014, https://hal.archives-ouvertes.fr/tel-01262056.

Articles in International Peer-Reviewed Journal

[61] V. Berthé, E. Domenjoud, D. Jamet, X. Provençal, "Fully Subtractive Algorithm, Tribonacci numeration and connectedness of discrete planes", *RIMS Kôkyûroku Bessatsu*, B46, 2014, p. 159–174, https://hal.archives-ouvertes.fr/hal-01262173.

[62] D. Coeurjolly, B. Kerautret, J.-O. Lachaud, "Extraction of Connected Region Boundary in Multidimensional Images", *Image Processing On Line 4*, March 2014, p. pp. 30–43, https://hal.archives-ouvertes.fr/hal-01112943.

[63] I. Debled-Rennesson, M. Margenstern, "Cellular Automata and Naive Discrete Lines ", *Journal of Cellular Automata 8*, 1-2, 2013, p. 113–129, https://hal.archives-ouvertes.fr/hal-01262157.

[64] E. Domenjoud, D. Jamet, D. Vergnaud, L. Vuillon, "Enumeration formula for (2,n)-cubes in discrete planes", *Discrete Applied Mathematics 160*, 15, October 2012, p. 2158–2171, https://hal.archives-ouvertes.fr/hal-00752236.

[65] E. Domenjoud, X. Provençal, L. Vuillon, "Palindromic language of thin discrete planes", *Theoretical Computer Science*, 2016, https://hal.archives-ouvertes.fr/hal-01262289.

[66] E. Domenjoud, L. Vuillon, "Geometric Palindromic Closure", *Uniform Distribution Theory 7*, 2, December 2012, p. 109–140, http://www.boku.ac.at/MATH/udt/vol07/no2/06DomVuillon13-12.pdf, https://hal.archives-ouvertes.fr/hal-00753935.

[67] D. Jamet, G. Paquin, G. Richomme, L. Vuillon, "On the fixed points of the iterated pseudopalindromic closure operator", *Theoretical Computer Science 412*, 27, June 2011, p. 2974–2987, https://hal.archives-ouvertes.fr/hal-00580665.

[68] B. Kerautret, J.-O. Lachaud, "Meaningful Scales Detection along Digital Contours for Unsupervised Local Noise Estimation", *IEEE Transactions on Pattern Analysis and Machine Intelligence 34*, 12, December 2012, p. 2379–2392, https://hal.archives-ouvertes.fr/hal-00780689.

[69] B. Kerautret, J.-O. Lachaud, "Meaningful Scales Detection: an Unsupervised Noise Detection Algorithm for Digital Contours", *Image Processing On Line 4*, May 2014, p. 18, https://hal.inria.fr/hal-01112936.

[70] A. Krähenbühl, B. Kerautret, I. Debled-Rennesson, F. Mothe, F. Longuetaud, "Knot segmentation in 3D CT images of wet wood", *Pattern Recognition 47*, 12, September 2014, p. 3852–3869, https://hal.inria.fr/hal-01062639.

[71] A. Krähenbühl, B. Kerautret, I. Debled-Rennesson, "TKDetection: a software to detect and segment wood knots", *imagen-a 3*, 5, March 2016, https://hal.archives-ouvertes.fr/hal-01265531.

[72] F. Longuetaud, F. Mothe, B. Kerautret, A. Krähenbühl, L. Hory, J. M. Leban, I. Debled-Rennesson, "Automatic knot detection and measurements from X-ray CT images of wood: A review and validation of an improved algorithm on softwood samples", *Computers and Electronics in Agriculture 85*, 2012, p. 77–89, https://hal.archives-ouvertes.fr/hal-00780761.

[73] P. Ngo, Y. Kenmochi, N. Passat, H. Talbot, "On 2D constrained discrete rigid transformations", *Annals of Mathematics and Artificial Intelligence*, 2015, https://hal-upec-upem.archives-ouvertes.fr/hal-00838184.

[74] T. P. Nguyen, I. Debled-Rennesson, "A discrete geometry approach for dominant point detection", *Pattern Recognition*, January 2011, p. 32–44, https://hal.inria.fr/inria-00526714.

[75] J.-R. Roussel, F. Mothe, A. Krähenbühl, B. Kerautret, I. Debled-Rennesson, F. Longuetaud, "Automatic knot segmentation in CT images of wet softwood logs using a tangential approach", *Computers and Electronics in Agriculture 104*, June 2014, p. 46–56, https://hal.inria.fr/hal-00981419.

[76] A. Vacavant, T. Roussillon, B. Kerautret, J.-O. Lachaud, "A combined multi-scale/irregular algorithm for the vectorization of noisy digital contours", *Computer Vision and Image Understanding 117*, 4, April 2013, p. 438–450, https://hal.archives-ouvertes.fr/hal-00943821.

Major International Conferences

[77] N. Aubry, B. Kerautret, I. Debled-Rennesson, P. Even, "Parallel Strip Segment Recognition and Application to Metallic Tubular Object Measure", *in : 17th International Workshop, IWCIA, Combinatorial Image Analysis - 17th International Workshop, IWCIA 2015, Kolkata, India, November 24-27, 2015. Proceedings, 9448*, Springer, p. 311–322, Kolkata, India, November 2015, https://hal.archives-ouvertes.fr/hal-01263234.

[78] V. Berthé, E. Domenjoud, D. Jamet, X. Provençal, J.-L. Toutant, "On the topology of discrete hyperplanes", *in : Numeration and Substitution*, Kyoto, Japan, June 2012. https://sites.google.com/site/numeration2012/DamienJamet-abstract.pdf?attredirects=0, https://hal.archives-ouvertes.fr/hal-00754713.

[79] M. Colom, B. Kerautret, N. Limare, P. Monasse, J.-M. Morel, "IPOL: a new journal for fully reproducible research; analysis of four years development", *in : Workshop NTMS 2015*

on Reproducibility in Computation Based Research, Proceedings of the 7th International Conference on New Technologies, Mobility and Security (NTMS 2015), Paris, France, July 2015, https://hal-enpc.archives-ouvertes.fr/hal-01181282.

[80] I. Debled-Rennesson, M. Margenstern, "Cellular Automata and Discrete Geometry", *in : CAAA 2011*, p. 333, Istanbul, Turkey, July 2011, https://hal.archives-ouvertes.fr/hal-00610383.

[81] I. Debled-Rennesson, L. Wendling, "Extraction of Successive Patterns in Document Images by a New Concept Based on Force Histogram and Thick Discrete Lines.", *in : 18th International Conference on Image Analysis and Processing, Image analysis and Processing - ICIAP 2015, 9379*, springer, p. 387–397, Genova, Italy, September 2015, https://hal.archives-ouvertes.fr/hal-01262145.

[82] E. Domenjoud, L. Vuillon, X. Provençal, "Facet Connectedness of Discrete Hyperplanes with Zero Intercept: The General Case", *in : 18th IAPR International Conference, DGCI 2014*, S. R. Elena Barcucci, Andrea Frosini (editor), *18th IAPR International Conference, DGCI 2014, Siena, Italy, September 10-12, 2014. Proceedings, 8668*, Springer International Publishing, p. 1–12, Siena, Italy, September 2014, https://hal.archives-ouvertes.fr/hal-01083101.

[83] E. Domenjoud, L. Vuillon, "Facet Connectedness of Discrete Hyperplanes", *in : SubTile 2013*, Marseille, France, January 2013, https://hal.archives-ouvertes.fr/hal-01264421.

[84] Y. Kenmochi, P. Ngo, H. Talbot, N. Passat, "Efficient Neighbourhood Computing for Discrete Rigid Transformation Graph Search", *in : 18th IAPR International Conference on Discrete Geometry for Computer Imagery, DGCI 2014, Lecture Notes in Computer Science, 8668*, Springer, p. 99–110, Sienne, Italy, September 2014, https://hal-upec-upem.archives-ouvertes.fr/hal-01067537.

[85] B. Kerautret, A. Krähenbühl, I. Debled-Rennesson, J.-O. Lachaud, "3D Geometric Analysis of Tubular Objects based on Surface Normal Accumulation", *in : 18th International Conference on Image Analysis and Processing*, Genova, Italy, September 2015, https://hal.archives-ouvertes.fr/hal-01139374.

[86] B. Kerautret, J.-O. Lachaud, T. P. Nguyen, "Circular arc reconstruction of digital contours with chosen Hausdorff error", *in : Discrete Geometry for Computer Imagery, LNCS, 6607*, Springer, p. 250–262, Nancy, France, April 2011, https://hal.archives-ouvertes.fr/hal-00579467.

[87] B. Kerautret, J.-O. Lachaud, M. Said, "Détection d'épaisseur significative sur une courbe polygonale", *in : RFIA 2012 (Reconnaissance des Formes et Intelligence Artificielle)*, p. 978–2–9539515–2–3, Lyon, France, January 2012. Session "Posters", https://hal.archives-ouvertes.fr/hal-00656573.

[88] B. Kerautret, J.-O. Lachaud, M. Said, "Meaningful Thickness Detection on Polygonal Curve", *in : ICPRAM - International Conference on Pattern Recognition Applications and Methods - 2012*, SciTePress, p. 372–379, Vilamoura, Portugal, February 2012, https://hal.archives-ouvertes.fr/hal-00780710.

[89] M. Kowalczyk, B. Kerautret, B. Naegel, J. Weber, "Revisiting Component Tree Based Segmentation Using Meaningful Photometric Informations", *in : International Conference on Computer Vision and Graphics (ICCVG, 7594*, p. 475–482, Varsovie, Poland, September 2012, https://hal.archives-ouvertes.fr/hal-00761303.

[90] A. Krähenbühl, B. Kerautret, I. Debled-Rennesson, F. Longuetaud, F. Mothe, "Knot Detection in X-Ray CT Images of Wood", *in : ISVC - 8th International Symposium on Visual Computing - 2012*, G. Bebis, R. Boyle, B. Parvin, D. Koracin, C. Fowlkes, S. Wang, M.-H. Choi, S. Mantler, J. P. Schulze, D. Acevedo, K. Mueller, M. E. Papka (editors), *LNCS - Lecture Notes in Computer Science*, *7432*, Springer, p. 209–218, Rethymnon, Greece, July 2012, https://hal.archives-ouvertes.fr/hal-00780731.

[91] A. Krähenbühl, B. Kerautret, I. Debled-Rennesson, "Knot Segmentation in Noisy 3D Images of Wood", *in : 17th IAPR International Conference on Discrete Geometry for Computer Imagery - 2013*, R. Gonzalez-Diaz, M.-J. Jimenez, B. Medrano (editors), *7749*, Springer Berlin Heidelberg, p. 383–394, Sevilla, Spain, March 2013, https://hal.inria.fr/hal-00804070.

[92] A. Krähenbühl, B. Kerautret, I. Debled-Rennesson, "Segmentation de noeuds de bois à partir d'images tomodensitométriques : approches transversales et tangentielles", *in : Reims Image*, p. 5, Reims, France, November 2014, https://hal.inria.fr/hal-01098131.

[93] A. Krähenbühl, B. Kerautret, F. Feschet, "Knot Detection from Accumulation Map by Polar Scan", *in : IWCIA*, *Combinatorial Image Analysis*, *9448*, 0302-9743, Kolkata, India, November 2015, https://hal.archives-ouvertes.fr/hal-01261651.

[94] A. Krähenbühl, F. Longuetaud, J.-B. Morisset, F. Colin, I. Debled-Rennesson, B. Kerautret, F. Mothe, "Knot shape assessment on various species through X-ray CT scanning", *in : International Union of Forest Research Organisation (IUFRO)*, Lisbon, Portugal, July 2012, https://hal.inria.fr/hal-00768816.

[95] A. Krähenbühl, J.-R. Roussel, B. Kerautret, I. Debled-Rennesson, F. Mothe, F. Longuetaud, "Segmentation robuste de nœuds à partir de coupes tangentielles issues d'images tomographiques de bois", *in : Reconnaissance de Formes et Intelligence Artificielle (RFIA) 2014*, France, June 2014, https://hal.archives-ouvertes.fr/hal-00989126.

[96] P. Ngo, H. Nasser, I. Debled-Rennesson, B. Kerautret, "Adaptive Tangential Cover for Noisy Digital Contours", *in : DGCI 2016 - 19th international conference on Discrete Geometry for Computer Imagery*, Nantes, France, April 2016, https://hal.inria.fr/hal-01266033.

[97] P. Ngo, H. Nasser, I. Debled-Rennesson, "Efficient dominant point detection based on discrete curve structure", *in : IWCIA 2015*, Kolkata, India, November 2015, https://hal.inria.fr/hal-01218285.

[98] T. P. Nguyen, I. Debled-Rennesson, "Arc segmentation in linear time", *in : 14th International Conference on Computer Analysis of Images and Patterns - CAIP 2011*, p. 8, Seville, Spain, August 2011, https://hal.archives-ouvertes.fr/hal-00594835.

[99] T. P. Nguyen, I. Debled-Rennesson, "Decomposition of a curve into arcs and line segments based on dominant point detection", *in : Scandinavian Conference on Image Analysis - SCIA 2011*, Ystad Saltsjöbad, Sweden, May 2011, https://hal.inria.fr/inria-00580123.

[100] T. P. Nguyen, I. Debled-Rennesson, "Décomposition d'une courbe discrète en arcs de cercle et segments de droite", *in : RFIA 2012 (Reconnaissance des Formes et Intelligence Artificielle)*, p. 978–2–9539515–2–3, Lyon, France, January 2012. Session "Posters", https://hal.archives-ouvertes.fr/hal-00656539.

[101] T. P. Nguyen, B. Kerautret, "Ellipse detection through decomposition of circular arcs and line segments", *in : International Conference on Image Analysis and Processing*, p. xxx, Ravenna, Italy, September 2011, https://hal.archives-ouvertes.fr/hal-00601877.

[102] J.-L. Toutant, A. Vacavant, B. Kerautret, "Arc Recognition on Irregular Isothetic Grids and Its Application to Reconstruction of Noisy Digital Contours", *in : 17th IAPR International Conference, DGCI 2013*, *DGCI 2013*, *7749*, springer, p. 265–276, Seville, France, March 2013, https://hal.inria.fr/hal-01266128.

[103] A. Vacavant, T. Roussillon, B. Kerautret, "Unsupervised Polygonal Reconstruction of Noisy Contours by a Discrete Irregular Approach", *in : 14th International Workshop on Combinatorial Image Analysis - IWCIA'11*, *LNCS*, *6636*, Springer, p. 398–409, Madrid, Spain, May 2011, https://hal.archives-ouvertes.fr/hal-00579472.

Books or Proceedings Editing

[104] *16th international conference on Discrete Geometry for Computer Imagery*, *LNCS*, Springer-verlag, March 2011, 529p., https://hal.archives-ouvertes.fr/hal-00580197.

[105] Isabelle Debled-Rennesson, Eric Domenjoud, Bertrand Kerautret, Philippe Even, *Discrete Geometry for Computer Imagery*, *Discrete Applied Mathematics*, *161*, 15, Nancy, France, elsevier, October 2013, https://hal.archives-ouvertes.fr/hal-01262818.

[106] Isabelle Debled-Rennesson, Eric Domenjoud, Bertrand Kerautret, Philippe Even, *Special Issue on Discrete Geometry for Computer Imagery*, *Computer Vision and Image Understanding*, *117*, 4, Nancy, France, elsevier, April 2013, https://hal.archives-ouvertes.fr/hal-01263222.

[107] J. Batenburg, D. Coeurjolly, B. Kerautret, U. Kathe J.-O Lachaud, T. Lewiner, *Image Processing Online (IPOL) : Special issue on DGCI 2011*, *4*, Nancy, France, March 2014, https://hal.archives-ouvertes.fr/hal-01262776.

3 References for Alice

Doctoral Dissertations

[108] *Habilitation à Diriger les Recherches - Synthèse de Textures par l'Exemple*, PhD Thesis, INPL, October 2014.

[109] A. Botella, *Génération de maillages non-structurés volumiques de modèles géologiques pour la simulation de phénoènes physiques*, PhD Thesis, RP2E Nancy, April 2016.

[110] A. Galindo, *Mise en correspondance d'images pour la reconstruction 3D utilisant des informations optiques et géométriques*, PhD Thesis, IAEM Nancy, January 2015.

[111] A. Lasram, *Exploration et rendu de textures synthétisées*, PhD Thesis, IAEM Nancy, December 2012.

[112] K. Liu, *Reconstruction de surfaces orientée multi-vue*, PhD Thesis, IAEM Nancy, December 2015.

[113] R. Merland, *Génération de grilles de type volumes finis : adaptation à un modèle structural, pdétrophysique et dynamique*, PhD Thesis, RP2E Nancy, april 2013.

[114] V. Nivoliers, *Echantillonnage pour l'approximation de fonctions sur des maillages*, PhD Thesis, IAEM Nancy, November 2011.

[115] J. Pellerin, *Prise en compte de la complexité géométrique des modèles structuraux dans des méthodes de maillage fondées sur le diagramme de Voronoi*, PhD Thesis, RP2E Nancy, march 2014.

[116] S. Podkorytov, *Espaces tangents pour les formes auto-similaires*, PhD Thesis, Sciences pour l'Ingenieur Besançon, December 2013.

Articles in International Peer-Reviewed Journal

[117] L. Alonso, E. M. Reingold, "Improved bounds for cops-and-robber pursuit", *Computational Geometry 44*, 8, October 2011, p. 365–369, https://hal.inria.fr/hal-00756031.

[118] L. Alonso, E. M. Reingold, "Analysis of Boyer and Moore's MJRTY algorithm", *Information Processing Letters*, July 2013, p. 495–497, https://hal.inria.fr/hal-00926106.

[119] X. Antoine, R. Duboscq, "Robust and Efficient Preconditioned Krylov Spectral Solvers for Computing the Ground States of Fast Rotating and Strongly Interacting Bose-Einstein Condensates", *Journal of Computational Physics 258*, 1, 2014, p. 509–523, https://hal.archives-ouvertes.fr/hal-00931117.

[120] D. Boltcheva, D. Canino, S. Merino Aceituno, J.-C. Léon, L. De Floriani, F. Hétroy, "An iterative algorithm for homology computation on simplicial shapes", *Computer-Aided Design 43*, 11, November 2011, p. 1457–1467, https://hal.inria.fr/hal-00644410.

[121] D. Bommes, L. Bruno, N. Pietroni, E. Puppo, C. Silva, M. Tarini, D. Zorin, "State of the Art in Quad Meshing", *Computer Graphics Forum*, May 2012, https://hal.inria.fr/hal-00804550.

[122] N. Bonneel, M. Van De Panne, S. Paris, W. Heidrich, "Displacement interpolation using Lagrangian mass transport", *ACM Transactions on Graphics 30*, 6, 2011, p. Article n.158, https://hal.inria.fr/hal-00763270.

[123] M. Chavent, B. Lévy, M. Krone, K. Bidmon, J.-P. Nominé, T. Ertl, M. Baaden, "GPU-powered tools boost molecular visualization.", *Briefings in Bioinformatics 12*, 6, November 2011, p. 689–701, https://hal.archives-ouvertes.fr/hal-00645161.

[124] M. Chavent, A. Vanel, A. Tek, B. Levy, S. Robert, B. Raffin, M. Baaden, "GPU-accelerated atom and dynamic bond visualization using hyperballs: a unified algorithm for balls, sticks, and hyperboloids.", *Journal of Computational Chemistry 32*, 13, October 2011, p. 2924–35, https://hal.archives-ouvertes.fr/hal-00645162.

[125] Z. Chen, W. Wang, B. Lévy, L. Liu, F. Sun, "Revisiting Optimal Delaunay Triangulation for 3D Graded Mesh Generation", *SIAM Journal on Scientific Computing*, May 2014, p. A930–A954, https://hal.inria.fr/hal-01101627.

[126] O. Cheong, H. Everett, M. Glisse, J. Gudmundsson, S. Hornus, S. Lazard, M. Lee, H.-S. Na, "Farthest-Polygon Voronoi Diagrams", *Computational Geometry 44*, 4, 2011, p. 14 pages, https://hal.inria.fr/inria-00442816.

[127] L. Devendeville, S. Dumont, O. Goubet, S. Lefebvre, "Algorithms for Constrained Best-fit Alignment", *Journal of Informatics and Mathematical Sciences 5*, 2, 2013, p. 77–100, https://hal.archives-ouvertes.fr/hal-00999255.

[128] J. Dumas, J. Hergel, S. Lefebvre, "Bridging the Gap: Automated Steady Scaffoldings for 3D Printing", *ACM Transactions on Graphics 33*, 4, July 2014, p. 98:1 – 98:10, https://hal.inria.fr/hal-01100737.

[129] B. Galerne, A. Lagae, S. Lefebvre, G. Drettakis, "Gabor Noise by Example", *ACM Transactions on Graphics (TOG) - SIGGRAPH 2012 Conference Proceedings 31*, 4, July 2012, p. Article No. 73, https://hal.archives-ouvertes.fr/hal-00695670.

[130] I. García, S. Lefebvre, S. Hornus, A. Lasram, "Coherent Parallel Hashing", *ACM Transactions on Graphics 30*, 6, December 2011, https://hal.inria.fr/inria-00624777.

[131] J. Hergel, S. Lefebvre, "Clean Colors", *Computer Graphics Forum (Eurographics 2014 conf. proc.)*, April 2014, https://hal.inria.fr/hal-00927291.

[132] J. Hergel, S. Lefebvre, "3D Fabrication of 2D Mechanisms", *Computer Graphics Forum*, 2015, https://hal.inria.fr/hal-01240344.

[133] T. Hoang, X. Cavin, P. Schultz, D. Ritchie, "gEMpicker: a highly parallel GPU-accelerated particle picking tool for cryo-electron microscopy", *BMC Structural Biology 13*, 1, 2013, p. 25, https://hal.inria.fr/hal-00955580.

[134] T. V. Hoang, X. Cavin, D. Ritchie, "gEMfitter: A highly parallel FFT-based 3D density fitting tool with GPU texture memory acceleration", *Journal of Structural Biology*, September 2013, https://hal.inria.fr/hal-00866871.

[135] S. Hornus, D. Larivière, B. Lévy, É. Fourmentin, "Easy DNA Modeling and More with GraphiteLifeExplorer", *PLoS ONE 8*, 1, January 2013, p. e53609, https://hal.inria.fr/hal-00924190.

[136] A. Lagae, S. Lefebvre, P. Dutre, "Improving Gabor Noise", *IEEE Transactions on Graphics and Visualization 17*, 8, August 2011, p. 1096–1107., https://hal.inria.fr/hal-01062522.

[137] A. Lasram, S. Lefebvre, C. Damez, "Procedural texture preview", *Computer Graphics Forum 31*, 2pt2, May 2012, p. 413–420, https://hal.inria.fr/hal-00748521.

[138] B. Lévy, "A numerical algorithm for L2 semi-discrete optimal transport in 3D", *ESAIM: Mathematical Modelling and Analysis 49*, 6, November 2015, p. 1693 – 1715, https://hal.inria.fr/hal-01105021.

[139] B. Lévy, "Robustness and Efficiency of Geometric Programs The Predicate Construction Kit (PCK)", *Computer-Aided Design*, 2015, https://hal.inria.fr/hal-01225202.

[140] E. R. Li, B. Lévy, X. Zhang, W.-J. Che, W. Dong, J.-C. Paul, "Meshless quadrangulation by global parameterization", *Computers and Graphics 35*, 5, 2011, p. 992–1000, https://hal.inria.fr/hal-00763290.

[141] A. Lu, S. Lefebvre, J. Dumas, J. Wu, C. Dick, "By-example synthesis of structurally sound patterns", *ACM Transactions on Graphics*, 2015, https://hal.inria.fr/hal-01240392.

[142] C. Ma, N. Vining, S. Lefebvre, A. Sheffer, "Game Level Layout from Design Specification", *Computer Graphics Forum*, April 2014, p. 95–104, https://hal.inria.fr/hal-00927311.

[143] C. Ma, L.-Y. Wei, S. Lefebvre, X. Tong, "Dynamic Element Textures", *ACM Transactions on Graphics 32*, 4, 2013, p. Article No. 90, https://hal.inria.fr/hal-00926846.

[144] J. Martínez, J. Dumas, S. Lefebvre, L.-Y. Wei, "Structure and appearance optimization for controllable shape design", *ACM Transactions on Graphics 34*, 6, November 2015, p. 12, https://hal.inria.fr/hal-01240642.

[145] J. Martínez, S. Hornus, F. Claux, S. Lefebvre, "Chained segment offsetting for ray-based solid representations", *Computers and Graphics 46*, 1, February 2015, p. 36 – 47, https://hal.inria.fr/hal-01080614.

[146] A. Mishkinis, C. Gentil, S. Lanquetin, D. Sokolov, "Approximate convex hull of affine iterated function system attractors", *Chaos, Solitons and Fractals 45*, 11, November 2012, p. 1444–1451, https://hal.inria.fr/hal-00755842.

[147] V. Nivoliers, C. Gérot, V. Ostromoukhov, N. F. Stewart, "L-system specification of knot-insertion rules for non-uniform B-spline subdivision", *Computer Aided Geometric Design 29*, 2, February 2012, p. 150–161, https://hal.archives-ouvertes.fr/hal-00659465.

[148] V. Nivoliers, B. Lévy, C. Geuzaine, "Anisotropic and feature sensitive triangular remeshing using normal lifting", *Journal of Computational and Applied Mathematics*, 2015, https://hal.archives-ouvertes.fr/hal-01202738.

[149] V. Nivoliers, B. Lévy, "Approximating Functions on a Mesh with Restricted Voronoi Diagrams", *Computer Graphics Forum 32*, 5, 2013, p. 83–92, Also Proceedings of the Annual Symposium on Geometry Processing, https://hal.inria.fr/hal-00929994.

[150] G.-P. Paillé, P. Poulain, B. Lévy, "Fitting Polynomial Volumes to Surface Meshes with Voronoï Squared Distance Minimization", *Computer Graphics Forum 32*, 5, August 2013, p. 103–112, Also Proceedings of the Annual Symposium on Geometry Processing, https://hal.inria.fr/hal-00930030.

[151] G.-P. Paillé, N. Ray, P. Poulin, A. Sheffer, B. Lévy, "Dihedral angle-based maps of tetrahedral meshes", *ACM Transactions on Graphics (SIGGRAPH 2015 conf. proc.)*, August 2015, https://hal.inria.fr/hal-01245593.

[152] C. Paulus, L. Untereiner, H. Courtecuisse, S. Cotin, D. Cazier, "Virtual Cutting of Deformable Objects based on Efficient Topological Operations", *The Visual Computer, Springer-Verlag Publ., ISSN 0178-2789 (Print) 1432-2315 (Online) 31*, 6-8, 2015, p. 831–841, https://hal.archives-ouvertes.fr/hal-01162099.

[153] J. Pellerin, G. Caumon, C. Julio, P. Mejia-Herrera, A. Botella, "Elements for measuring the complexity of 3D structural models: Connectivity and geometry", *COMPUTERS & GEOSCIENCES 76*, March 2015, p. 130–140, https://hal-univ-lorraine.archives-ouvertes.fr/hal-01276849.

[154] J. Pellerin, B. Lévy, G. Caumon, A. Botella, "Automatic surface remeshing of 3D structural models at specified resolution: A method based on Voronoi diagrams", *Computers and Geosciences 62*, September 2013, p. 103–116, https://hal.inria.fr/hal-00924622.

[155] J. Pellerin, B. Lévy, G. Caumon, A. Botella, "Automatic surface remeshing of 3D structural models at specified resolution: A method based on Voronoi diagrams", *Computers and Geosciences*, January 2014, p. 103–116, https://hal.inria.fr/hal-01105039.

[156] S. Podkorytov, C. Gentil, D. Sokolov, S. Lanquetin, "Geometry control of the junction between two fractal curves", *Computer-Aided Design 45*, 2, February 2013, p. 424–431, https://hal-univ-bourgogne.archives-ouvertes.fr/hal-01137726.

[157] S. Podkorytov, C. Gentil, D. Sokolov, S. Lanquetin, "Joining primal/dual subdivision surfaces", *Mathematical Methods for Curves and Surfaces volume 8177 of Lecture Notes in Computer Science*, November 2014, p. 403–424, https://hal-univ-bourgogne.archives-ouvertes.fr/hal-01137721.

[158] R. Prévost, E. Whiting, S. Lefebvre, O. Sorkine-Hornung, "Make It Stand: Balancing Shapes for 3D Fabrication", *ACM Transactions on Graphics 32*, 4, 2013, p. Article No. 81, https://hal.inria.fr/hal-00926855.

[159] N. Ray, D. Sokolov, "Robust polylines tracing for N-symmetry direction field on triangulated surfaces", *ACM Transactions on Graphics*, May 2014, p. 11, https://hal.inria.fr/hal-01092823.

[160] T. Reiner, S. Lefebvre, L. Diener, I. García, B. Jobard, C. Dachsbacher, "A Runtime Cache for Interactive Procedural Modeling", *Computers and Graphics 36*, 5, August 2012, p. 366–375, https://hal.inria.fr/hal-00748542.

[161] G. Rong, Y. Liu, W. Wang, X. Yin, X. Gu, X. Guo, "GPU-Assisted Computation of Centroidal Voronoi Tessellation", *IEEE Transactions on Visualization and Computer Graphics 17*, 3, March 2011, p. 345–356, https://hal.inria.fr/inria-00602490.

[162] D. Sokolov, C. Gentil, H. Bensoudane, "Tangents to fractal curves and surfaces", *Curves and Surfaces 6920*, 2012, p. 663–680, https://hal-univ-bourgogne.archives-ouvertes.fr/hal-00798910.

[163] D. Sokolov, C. Gentil, "Intuitive modeling of vapourish objects", *Chaos, Solitons and Fractals*, December 2015, https://hal.inria.fr/hal-01244616.

[164] F. Sun, Y.-K. Choi, W. Wang, D.-M. Yan, Y. Liu, B. Lévy, "Obtuse triangle suppression in anisotropic meshes", *Computer Aided Geometric Design 28*, 9, 2011, p. 537–548, https://hal.inria.fr/hal-00763324.

[165] T. Viard, G. Caumon, B. Levy, "Adjacent versus coincident representations of geospatial uncertainty: Which promote better decisions?", *Computers and Geosciences 37*, 4, April 2011, p. 511–520, https://hal-insu.archives-ouvertes.fr/insu-00593625.

[166] D.-M. Yan, W. Wang, B. Lévy, Y. Liu, "Efficient computation of clipped Voronoi diagram for mesh generation", *Computer-Aided Design*, September 2011, https://hal.inria.fr/hal-00647979.

[167] R. Zayer, "A nonlinear static approach for curve editing", *Computers and Graphics 36*, 5, 2012, p. 514–520, https://hal.inria.fr/hal-00763434.

[168] Z. Zhong, X. Guo, W. Wang, B. Lévy, F. Sun, Y. Liu, W. Mao, "Particle-based Anisotropic Surface Meshing", *ACM Transactions on Graphics 32*, 4, 2013, p. 99:1–99:14, https://hal.inria.fr/hal-00930147.

[169] S. Zhou, A. Lasram, S. Lefebvre, "By-example synthesis of curvilinear structured patterns", *Computer Graphics Forum 32*, 2, 2013, p. 355–360, https://hal.inria.fr/hal-00926839.

Invited Conferences

[170] B. Lévy, R. H. Zhang, "Elements of geometry processing", *in : 4th ACM SIGGRAPH Conference and Exhibition on Computer Graphics and Interactive Techniques in Asia - SiggraphAsia 2011, Proceedings of ACM SIGGRAPH Asia 2011Courses*, ACM, p. Article n.5, Hong Kong, China, December 2011, https://hal.inria.fr/hal-00763332.

Major International Conferences

[171] D. Boltcheva, E. Casella, R. Cumont, F. Hétroy, "A spectral clustering approach of vegetation components for describing plant topology and geometry from terrestrial waveform LiDAR data", *in : FSPM2013 - 7th International Conference on Functional-Structural Plant Models*, A. Lintunen (editor), Saariselkä, Finland, June 2013. Poster, https://hal.inria.fr/hal-00817508.

[172] L. Bruno, N. Bonneel, "Variational Anisotropic Surface Meshing with Voronoi Parallel Linear Enumeration", *in : IMR - 21st International Meshing Roundtable - 2012*, San José, United States, October 2012, https://hal.inria.fr/hal-00804558.

[173] X. Cavin, O. Demengeon, "Shift-Based Parallel Image Compositing on InfiniBand Fat-Trees", *in : PGV - Eurographics Symposium on Parallel Graphics and Visualization*, p. 129–138, Cagliari, Italy, May 2012, https://hal.inria.fr/hal-00726501.

[174] M. Chajdas, S. Lefebvre, M. Stamminger, "Assisted Texture Assignment", *in : ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games - I3D 2011*, ACM, Washington, D.C., United States, February 2011, https://hal.inria.fr/inria-00547769.

[175] P. A. Galindo, R. Zayer, "Complementary geometric and optical information for match-propagation-based 3D reconstruction", *in : Proceedings on ACCV 2014*, Singapore, Singapore, November 2014, https://hal.inria.fr/hal-01088426.

[176] P. A. Galindo, R. Zayer, "Distortion driven variational multi-view reconstruction", *in : Proceedings on International Conference in 3D Vision (3DV)*, Tokyo, Japan, December 2014, https://hal.inria.fr/hal-01088428.

[177] A. Lasram, S. Lefebvre, C. Damez, "Scented Sliders for Procedural Textures", *in : EUROGRAPHICS short papers, Proceedings of the Eurographics conference (short papers)*, Cagliari, Italy, May 2012, https://hal.inria.fr/hal-00748188.

[178] A. Lasram, S. Lefebvre, "Parallel Patch-based Texture Synthesis", *in : Eurographics/ ACM SIGGRAPH Symposium on High Performance Graphics*, ACM, p. 115–124, Paris, France, June 2013, https://hal.inria.fr/hal-00748535.

[179] S. Lefebvre, "IceSL: A GPU Accelerated CSG Modeler and Slicer", *in : AEFA'13, 18th European Forum on Additive Manufacturing*, Paris, France, June 2013, https://hal.inria.fr/hal-00926861.

[180] K. Liu, R. Zayer, P. A. Galindo, "Sphere Packing Aided Surface Reconstruction for Multi-view Data", *in : 10th International Symposium on Visual Computing, Advances in Visual Computing - 10th International Symposium, ISVC 2014, Las Vegas, NV, USA, December 8-10, 2014, Proceedings*, Las Vegas, NV, United States, December 2014, https://hal.inria.fr/hal-01093210.

[181] K. Liu, R. Zayer, "Bundle Adjustment Constrained Smoothing for Multi-view Point Cloud Data", *in : ISVC 2012, 8th International Symposium on Visual Computing, 7431*, p. 126–137, Rethymnon, Crete, Greece, July 2012, https://hal.inria.fr/hal-00763442.

[182] D. Lopez, L. Bruno, "Dynamic Mesh Optimization for Free Surfaces in Fluid Simulation", *in : IMR - 21th international meshing roundtable - 2012, reseach notes*, Xiangmin Jiao and Jean-Christophe Weill, p. 1–5, San José, United States, October 2012, https://hal.inria.fr/hal-00764267.

[183] R. Merland, B. Lévy, G. Caumon, "Building PEBI Grids Conforming To 3D Geological Features Using Centroidal Voronoi Tessellations", *in : IAMG 2011 - Mathematical Geosciences at the Crossroads of Theory and Practice*, R. Marschallinger, R. Zolb (editors), *IAMG 2011 Proceedings*, p. 254–265, Salzburg, Austria, September 2011, https://hal.inria.fr/hal-00763403.

[184] V. Nivoliers, D.-M. Yan, B. Lévy, "Fitting Polynomial Surfaces to Triangular Meshes with Voronoi Squared Distance Minimization", *in : 20th International Meshing Roundtable - IMR 2012*, W. R. Quadros (editor), *Proceedings of the 20th International Meshing Roundtable*, Springer, p. 601–617, Paris, France, October 2011. The original publication is available at www.springerlink.com, https://hal.inria.fr/hal-00763898.

[185] C. Paulus, L. Untereiner, H. Courtecuisse, S. Cotin, D. Cazier, "Virtual Cutting of Deformable Objects based on Efficient Topological Operations", *in : Computer Graphics International*, Strasbourg, France, 2015, https://hal.archives-ouvertes.fr/hal-01208546.

[186] J. Pellerin, G. Caumon, B. Lévy, "Toward Mixed-element Meshing based on Restricted Voronoi Diagrams", *in : 23rd International Meshing Roundtable (IMR23)*, london, United Kingdom, October 2014, https://hal.inria.fr/hal-01105033.

[187] J. Pellerin, B. Lévy, G. Caumon, "Topological control for isotropic remeshing of non-manifold surfaces with varying resolution: application to 3D structural models", *in : IAMG 2011 - Mathematical Geosciences at the Crossroads of Theory and Practice*, R. Marschallinger, R. Zolb (editors), *IAMG 2011 Proceedings*, p. 678–688, Salzburg, Austria, September 2011, https://hal.inria.fr/hal-00763409.

[188] S. Podkorytov, C. Gentil, D. Sokolov, S. Lanquetin, "Geometry control of the junction between two fractal curves", *in : Symposium on Solid and Physical Modeling - SPM 2012*, Dijon, France, October 2012, https://hal.inria.fr/hal-00755851.

[189] D.-M. Yan, K. Wang, B. Lévy, L. Alonso, "Computing 2D Periodic Centroidal Voronoi Tessellation", *in : 8th International Symposium on Voronoi Diagrams in Science and Engineering - ISVD2011*, Qingdao, China, June 2011, https://hal.inria.fr/inria-00605927.

National Peer-Reviewed Conferences

[190] S. Hornus, D. Larivière, "Graphite-MicroMégas, a tool for DNA modeling", *in : Journée Visu 2011*, Bruyères le Chatel, France, October 2011, https://hal.inria.fr/hal-00756029.

[191] R. Merland, B. Lévy, G. Caumon, P. Collon-Drouaillet, "Building Centroidal Voronoi Tesselations for Flow Simulation in Reservoirs Using Flow Information", *in : SPE Reservoir Simulation Symposium - 2011*, *SPE 2011 Conference Proceedings*, Society of Petroleum Engineers, The Woodlands, United States, February 2011, https://hal.inria.fr/hal-00763400.

[192] A. Mishkinis, C. Gentil, S. Lanquetin, D. Sokolov, "Méthodes d'approximation d'opérations géométriques sur des objets fractals", *in : Groupe de Travail en Modélisation Géométrique*, Marseille, France, March 2015, https://hal-univ-bourgogne.archives-ouvertes.fr/hal-01137735.

Books or Proceedings Editing

[193] B. Levy, J. Kautz (editors), *Computer Graphics Forum - special issue Eurographics 2014 conf. proc.*, Eurographics Association, 2014, https://diglib.eg.org/handle/10.2312/11784.

[194] B. Levy, X. Tong, K. K. Yin (editors), *Computer Graphics Forum - special issue Pacific Graphic 2013 conf. proc.*, Eurographics Association, 2013, https://diglib.eg.org/handle/10.2312/185.

Book chapters

[195] S. Lefebvre, S. Hornus, A. Lasram, "Per-Pixel Lists for Single Pass A-Buffer", *in : GPU Pro 5: Advanced Rendering Techniques*, W. Engel (editor), A K Peter / CRC Press, March 2014, https://hal.inria.fr/hal-01093158.

[196] D. Sokolov, G. Gouaty, C. Gentil, A. Mishkinis, "Boundary Controlled Iterated Function Systems", *in : Curves and Surfaces, Lecture Notes in Computer Science - 8th International Conference, Paris, France, June 12-18, 2014, Revised Selected Papers*, Springer, August 2015, https://hal.inria.fr/hal-01244612.

Other Publications

[197] S. Hornus, S. Lefebvre, J. Dumas, F. Claux, "Tight printable enclosures for additive manufacturing", *Research Report number RR-8712*, Inria, April 2015, https://hal.inria.fr/hal-01141706.

[198] S. Hornus, "Intersection detection via Gauss maps; a review and new techniques", *Research Report number RR-8730*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; INRIA, June 2015, https://hal.inria.fr/hal-01157239.

[199] B. Jobard, N. Ray, D. Sokolov, "Visualizing 2D Flows with Animated Arrow Plots", working paper or preprint, May 2012, https://hal.inria.fr/hal-00700822.

[200] S. Lefebvre, S. Hornus, A. Lasram, "HA-Buffer: Coherent Hashing for single-pass A-buffer", *Research Report number RR-8282*, INRIA, April 2013, https://hal.inria.fr/hal-00811585.

[201] J. Martinez, F. Claux, S. Lefebvre, "Raster2Mesh: Rasterization based CVT meshing", *Research Report number RR-8684*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; INRIA, February 2015, https://hal.inria.fr/hal-01117655.

[202] J. Pellerin, L. Bruno, G. Caumon, "A Voronoi-Based Hybrid Meshing Method", October 2012, 21st IMR, San Jose, CA, https://hal.inria.fr/hal-00770939.

[203] N. Ray, D. Sokolov, "Illustration of iterative linear solver behavior on simple 1D and 2D problems", *Research report*, LORIA, October 2015, https://hal.inria.fr/hal-01211410.

[204] N. Ray, D. Sokolov, "On Smooth Frame Field Design", working paper or preprint, January 2016, https://hal.inria.fr/hal-01245657.

[205] A. Rousseau, A. Darnaud, B. Goglin, C. Acharian, C. Leininger, C. Godin, C. Holik, C. Kirchner, D. Rives, E. Darquie, E. Kerrien, F. Neyret, F. Masseglia, F. Dufour, G. Berry, G. Dowek, H. Robak, H. Xypas, I. Illina, I. Gnaedig, J. Jongwane, J. Ehrel, L. Viennot, L. Guion, L. Calderan, L. Kovacic, M. Collin, M.-A. Enard, M.-H. Comte, M. Quinson, M. Olivi, M. Giraud, M. Dorémus, M. Ogouchi, M. Droin, N. Lacaux, N. P. Rougier, N. Roussel, P. Guitton, P. Peterlongo, R.-M. Cornus, S. Vandermeersch, S. Maheo, S. Lefebvre, S. Boldo, T. Viéville, V. Poirel, A. Chabreuil, A. Fischer, C. Farge, C. Vadel, I. Astic, J.-P. Dumont, L. Féjoz, P. Rambert, P. Paradinas, S. De Quatrebarbes, S. Laurent, "Médiation Scientifique : une facette de nos métiers de la recherche", *Interne*, none, March 2013, https://hal.inria.fr/hal-00804915.

[206] D. Sokolov, N. Ray, L. Untereiner, B. Lévy, "Hexahedral-dominant meshing", working paper or preprint, October 2015, https://hal.inria.fr/hal-01203544.

[207] D. Sokolov, N. Ray, "Fixing normal constraints for generation of polycubes", *Research report*, LORIA, October 2015, https://hal.inria.fr/hal-01211408.

4 References for Caramba

Doctoral Dissertations

[208] R. Barbulescu, *Algorithms of discrete logarithm in finite fields*, Theses, Université de Lorraine, December 2013, https://tel.archives-ouvertes.fr/tel-00925228.

[209] G. Bisson, *Endomorphism Rings in Cryptography*, Theses, Institut National Polytechnique de Lorraine - INPL ; Technische Universiteit Eindhoven, July 2011, https://tel.archives-ouvertes.fr/tel-00609211.

[210] C. Bouvier, *Algorithms for integer factorization and discrete logarithms computation*, Theses, Université de Lorraine, June 2015, https://tel.archives-ouvertes.fr/tel-01167281.

[211] R. Cosset, *Applications of theta functions for hyperelliptic curve cryptography*, Theses, Université Henri Poincaré - Nancy I, November 2011, https://tel.archives-ouvertes.fr/tel-00642951.

[212] N. Estibals, *Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques*, Theses, Université de Lorraine, October 2013, https://tel.archives-ouvertes.fr/tel-00924743.

[213] H. Jeljeli, *Hardware and Software Accelerators for Sparse Linear Algebra over Finite Fields*, Theses, Université de Lorraine, July 2015, https://tel.archives-ouvertes.fr/tel-01178931.

[214] E. Thomé, *Algorithmic Number Theory and Applications to the Cryptanalysis of Cryptographical Primitives*, Habilitation à diriger des recherches, Université de Lorraine, December 2012, https://tel.archives-ouvertes.fr/tel-00765982.

Articles in International Peer-Reviewed Journal

[215] S. Bai, C. Bouvier, A. Kruppa, P. Zimmermann, "Better polynomials for GNFS", *Mathematics of Computation*, December 2015, p. 12, https://hal.inria.fr/hal-01089507.

[216] S. Bai, R. Brent, E. Thomé, "Root optimization of polynomials in the number field sieve", *Mathematics of Computation 84*, 2015, p. 2447–2457, https://hal.inria.fr/hal-00919367.

[217] R. Barbulescu, "Selecting polynomials for the Function Field Sieve", *Mathematics of Computation*, March 2015, p. S0025–5718–2015–02940–8, https://hal.inria.fr/hal-00798386.

[218] J.-L. Beuchat, J. Detrey, N. Estibals, E. Okamoto, F. Rodríguez-Henríquez, "Fast architectures for the η_T pairing over small-characteristic supersingular elliptic curves", *IEEE Transactions on Computers 60*, 2, February 2011, p. 266–281, https://hal.inria.fr/inria-00424016.

[219] G. Bisson, A. V. Sutherland, "A low-memory algorithm for finding short product representations in finite groups", *Designs, Codes and Cryptography*, 2011, 12 pages, https://hal.inria.fr/inria-00560256.

[220] G. Bisson, A. V. Sutherland, "Computing the endomorphism ring of an ordinary elliptic curve over a finite field", *Journal of Number Theory 131*, 5, 2011, p. 815–831, https://hal.inria.fr/inria-00383155.

[221] G. Bisson, "Computing endomorphism rings of elliptic curves under the GRH", *Journal of Mathematical Cryptology 5*, 2, June 2011, p. 101–113, 11 pages, 1 figure, https://hal.inria.fr/inria-00560258.

[222] C. Bouvier, P. Zimmermann, "Division-Free Binary-to-Decimal Conversion", *IEEE Transactions on Computers 63*, 8, August 2014, p. 1895–1901, https://hal.inria.fr/hal-00864293.

[223] R. P. Brent, P. Zimmermann, "The Great Trinomial Hunt", *Notices of the AMS 58*, 2, 2011, p. 233–239, https://hal.inria.fr/inria-00443797.

[224] S. Chevillard, J. Harrison, M. M. Joldes, C. Lauter, "Efficient and accurate computation of upper bounds of approximation errors", *Journal of Theoretical Computer Science 412*, 16, 2011, p. 1523–1543, https://hal-ens-lyon.archives-ouvertes.fr/ensl-00445343.

[225] S. Chevillard, "The functions erf and erfc computed with arbitrary precision and explicit error bounds", *Information and Computation 216*, 2012, p. 72 – 95, The version available on the HAL server is slightly different from the published version because it contains full proofs., https://hal-ens-lyon.archives-ouvertes.fr/ensl-00356709.

[226] R. Cosset, D. Robert, "Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves", *Mathematics of Computation 84*, 294, 2015, p. 1953–1975, https://hal.archives-ouvertes.fr/hal-00578991.

[227] A. Enge, P. Gaudry, E. Thomé, "An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves", *Journal of Cryptology 24*, 2011, p. 24–41, https://hal.inria.fr/inria-00383941.

[228] A. Enge, E. Thomé, "Computing class polynomials for abelian surfaces", *Experimental Mathematics 23*, 2014, p. 129–145, https://hal.inria.fr/hal-00823745.

[229] J.-C. Faugère, P. Gaudry, L. Huot, G. Renault, "Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm", *Journal of Cryptology*, May 2013, p. 1–40, 40 pages, https://hal.archives-ouvertes.fr/hal-00700555.

[230] J.-C. Faugère, D. Lubicz, D. Robert, "Computing modular correspondences for abelian varieties", *Journal of Algebra 343*, 1, October 2011, p. 248–277, https://hal.archives-ouvertes.fr/hal-00426338.

[231] J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer, "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity", *Journal of Symbolic Computation 46*, 4, April 2011, p. 406–437, https://hal.inria.fr/inria-00596631.

[232] S. Galbraith, P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem", *Designs, Codes and Cryptography 78*, 1, 2016, p. 51–72, https://hal.inria.fr/hal-01215623.

[233] P. Gaudry, É. Schost, "Genus 2 point counting over prime fields", *Journal of Symbolic Computation 47*, 4, 2012, p. 368–400, https://hal.inria.fr/inria-00542650.

[234] E. Gioan, S. Burckel, E. Thomé, "Computation with No Memory, and Rearrangeable Multicast Networks", *Discrete Mathematics and Theoretical Computer Science 16*, 1, February 2014, p. 121–142, http://hal-lirmm.ccsd.cnrs.fr/lirmm-00959964.

[235] S. Ionica, "Pairing-based algorithms for Jacobians of genus 2 curves with maximal endomorphism ring", *Journal of Number Theory 133*, July 2013, p. 3755–3770, https://hal.archives-ouvertes.fr/hal-00675045.

[236] T. Kleinjung, J. W. Bos, A. K. Lenstra, D. A. Osvik, K. Aoki, S. Contini, J. Franke, E. Thomé, P. Jermini, M. Thiémard, P. Leyland, P. L. Montgomery, A. Timofeev, H. Stockinger, "A Heterogeneous Computing Environment to Solve the 768-bit RSA Challenge", *Cluster Computing 15*, 1, 2012, p. 53–68, https://hal.inria.fr/inria-00535765.

[237] D. Lubicz, D. Robert, "Computing isogenies between Abelian Varieties", *Compositio Mathematica 148*, 05, September 2012, p. 1483–1515, 47 pages, https://hal.archives-ouvertes.fr/hal-00446062.

[238] G. Melquiond, W. G. Nowak, P. Zimmermann, "Numerical Approximation of the Masser-Gramain Constant to Four Decimal Digits: delta=1.819...", *Mathematics of Computation 82*, 2013, p. 1235–1246, https://hal.inria.fr/hal-00644166.

[239] G. Ottaviani, P.-J. Spaenlehauer, B. Sturmfels, "Exact Solutions in Structured Low-Rank Approximation", *SIAM Journal on Matrix Analysis and Applications 4*, 2014, p. 1521–1542, https://hal.archives-ouvertes.fr/hal-00953702.

[240] T. Prest, P. Zimmermann, "Non-Linear Polynomial Selection for the Number Field Sieve", *Journal of Symbolic Computation 47*, 4, 2012, p. 401–409, https://hal.inria.fr/inria-00540483.

[241] É. Schost, P.-J. Spaenlehauer, "A Quadratically Convergent Algorithm for Structured Low-Rank Approximation", *Foundations of Computational Mathematics*, March 2015, p. 1–36, https://hal.archives-ouvertes.fr/hal-00953684.

[242] P.-J. Spaenlehauer, "On the Complexity of Computing Critical Points with Gröbner Bases", *SIAM Journal on Optimization 24*, 3, 2014, p. 1382–1401, 25 pages, https://hal.archives-ouvertes.fr/hal-01017032.

Major International Conferences

[243] M. A. Abdelraheem, C. Blondeau, M. Naya-Plasencia, M. Videau, E. Zenner, "Cryptanalysis of ARMADILLO2", *in : Advances in cryptology - ASIACRYPT 2011*, D. H. Lee, X. Wang (editors), *7073*, Springer, p. 308–326, Séoul, South Korea, December 2011, https://hal.inria.fr/inria-00619236.

[244] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. Vandersloot, E. Wustrow, S. Zanella-Béguelin, P. Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", *in : ACM CCS 2015, 2015 ACM SIGSAC Conference on Computer and Communications Security*, p. 14, Denver, Colorado, United States, October 2015, https://hal.inria.fr/hal-01184171.

[245] D. Aranha, J.-L. Beuchat, J. Detrey, N. Estibals, "Optimal Eta pairing on supersingular genus-2 binary hyperelliptic curves", *in : Cryptographer's Track at the RSA Conference 2012 (CT-RSA 2012)*, O. Dunkelman (editor), Springer, p. 19, San Francisco, United States, February 2012, https://hal.inria.fr/inria-00540002.

[246] C. Arene, R. Cosset, "Construction of a k-complete addition law on abelian surfaces with rational theta constants", *in : AGCT 2011, Arithmetic, Geometry, Cryptography and Coding Theory, 574*, AMS, Marseille, France, 2011, https://hal.inria.fr/hal-00645652.

[247] R. Barbulescu, J. W. Bos, C. Bouvier, T. Kleinjung, P. L. Montgomery, "Finding ECM-friendly curves through a study of Galois properties", *in : ANTS-X 10th Algorithmic Number Theory Symposium - 2012*, University of California, San Diego, United States, July 2012, https://hal.inria.fr/hal-00671948.

[248] R. Barbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, P. Zimmermann, "Discrete logarithm in GF(2^{809}) with FFS", *in : PKC 2014 - International Conference on Practice and Theory of Public-Key Cryptography*, H. Krawczyk (editor), *LNCS*, Springer, Buenos Aires, Argentina, 2014, https://hal.inria.fr/hal-00818124.

[249] R. Barbulescu, J. Detrey, N. Estibals, P. Zimmermann, "Finding Optimal Formulae for Bilinear Maps", *in : International Workshop of the Arithmetics of Finite Fields*, F. Özbudak, F. Rodríguez-Henríquez (editors), *7369*, Ruhr Universitat Bochum, Bochum, Germany, July 2012, https://hal.inria.fr/hal-00640165.

[250] R. Barbulescu, P. Gaudry, A. Guillevic, F. Morain, "Improving NFS for the discrete logarithm problem in non-prime finite fields", *in : Eurocrypt 2015*, M. Fischlin, E. Oswald (editors), *Eurocrypt 2015, 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, p. 27, Sofia, Bulgaria, April 2015, https://hal.inria.fr/hal-01112879.

[251] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé, "A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic", *in : Eurocrypt 2014*, P. Q. Nguyen, E. Oswald (editors), *8441*, Springer, p. 1–16, Copenhagen, Denmark, May 2014, https://hal.inria.fr/hal-00835446.

[252] R. Barbulescu, P. Gaudry, T. Kleinjung, "The Tower Number Field Sieve", *in : ASIACRYPT 2015*, T. Iwata, J. H. Cheon (editors), *Advances in cryptology-Asiacrypt 2015, 9453*, International Association of Cryptologic Research, Springer, p. 31–58, Auckland, New Zealand, November 2015, https://hal.archives-ouvertes.fr/hal-01155635.

[253] V. Cortier, J. Detrey, P. Gaudry, F. Sur, E. Thomé, M. Turuani, P. Zimmermann, "Ballot stuffing in a postal voting system", *in : Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems*, IEEE, p. 27 – 36, Trento, Italy, 2011, https://hal.inria.fr/inria-00612418.

[254] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, "Distributed ElGamal à la Pedersen - Application to Helios", *in : WPES 2013 - Proceedings of the 12th ACM workshop on privacy in the electronic society - 2013*, ACM, p. 131–142, Berlin, Germany, November 2013, https://hal.inria.fr/hal-00881076.

[255] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, "Election Verifiability for Helios under Weaker Trust Assumptions", *in : Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS'14)*, Wroclaw, Poland, September 2014, https://hal.inria.fr/hal-01080292.

[256] J. Detrey, P. Gaudry, M. Videau, "Relation collection for the Function Field Sieve", *in : ARITH 21 - 21st IEEE International Symposium on Computer Arithmetic*, A. Nannarelli, P.-M. Seidel, P. T. P. Tang (editors), *ARITH 21*, IEEE, p. 201–210, Austin, Texas, United States, April 2013, https://hal.inria.fr/hal-00736123.

[257] J.-C. Faugère, P. Gaudry, L. Huot, G. Renault, "Using Symmetries and Fast Change of Ordering in the Index Calculus for Elliptic Curves Discrete Logarithm", *in : SCC 2012 - Third international conference on Symbolic Computation and Cryptography*, Castro Urdiales, Spain, July 2012, https://hal.inria.fr/hal-00793097.

[258] J.-C. Faugère, P. Gaudry, L. Huot, G. Renault, "Sub-cubic Change of Ordering for Gröner Basis: A Probabilistic Approach", *in : ISSAC '14 - Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, *ISSAC '14*, ACM, p. 170–177, Kobe, Japan, July 2014, https://hal.inria.fr/hal-01064551.

[259] J.-C. Faugère, P.-J. Spaenlehauer, J. Svartz, "Sparse Gröbner Bases: the Unmixed Case", *in : ISSAC 2014*, Kobe, Japan, July 2014. 20 pages, Corollary 6.1 has been corrected, https://hal.archives-ouvertes.fr/hal-00953501.

[260] T. Fuhr, H. Gilbert, J.-R. Reinhard, M. Videau, "Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3", *in : 18th International Workshop on Selected Areas in Cryptography SAC 2011*, A. Miri, S. Vaudenay (editors), *7118*, Springer, p. 230–242, Toronto, Canada, August 2011, https://hal.inria.fr/inria-00619235.

[261] P. Gaudry, D. Kohel, B. Smith, "Counting Points on Genus 2 Curves with Real Multiplication", *in : ASIACRYPT 2011*, D. H. Lee, X. Wang (editors), *7073*, International Association for Cryptologic Research, Springer, p. 504–519, Seoul, South Korea, December 2011, https://hal.inria.fr/inria-00598029.

[262] D. Harvey, P. Zimmermann, "Short Division of Long Integers", *in : 20th IEEE Symposium on Computer Arithmetic (ARITH-20)*, E. Antelo, D. Hough, P. Ienne (editors), IEEE, p. 7–14, Tuebingen, Germany, July 2011, https://hal.inria.fr/inria-00612232.

[263] H. Jeljeli, "Accelerating Iterative SpMV for Discrete Logarithm Problem Using GPUs", *in : International Workshop on the Arithmetic of Finite Fields WAIFI 2014*, Gebze, Turkey, September 2014, https://hal.inria.fr/hal-00734975.

[264] H. Jeljeli, "Resolution of Linear Algebra for the Discrete Logarithm Problem Using GPU and Multi-core Architectures", *in : Euro-Par 2014 Parallel Processing*, Porto, Portugal, August 2014, https://hal.inria.fr/hal-00946895.

[265] A. K. Lenstra, T. Kleinjung, E. Thomé, "Universal Security; From bits and mips to pools, lakes - and beyond", *in : Number Theory and Cryptography*, M. Fischlin, S. Katzenbeisser (editors), *Lecture Notes in Computer Science*, *8260*, Springer, p. 121–124, Darmstadt, Germany, November 2013. Humoristic, https://hal.inria.fr/hal-00925622.

[266] E. Thomé, "Square root algorithms for the number field sieve", *in : 4th International Workshop on Arithmetic in Finite Fields - WAIFI 2012*, F. Özbudak, F. Rodríguez-Henríquez (editors), *7369*, Springer, p. 208–224, Bochum, Germany, July 2012. The original publication is available at www.springerlink.com, https://hal.inria.fr/hal-00756838.

Articles in National Peer-Reviewed Journal

[267] P. Gaudry, E. Thomé, P. Zimmermann, "RSA : la fin des clés de 768 bits", *Techniques de l'Ingenieur*, IN131, 2011, https://hal.inria.fr/hal-00641592.

National Peer-Reviewed Conferences

[268] H. Labrande, “Crack me, I’m famous!: Cracking weak passphrases using freely available sources”, *in : SSTIC 2015*, Rennes, France, June 2015, https://hal.inria.fr/hal-01238600.

Books

[269] A. Casamayou, N. Cohen, G. Connan, T. Dumont, L. Fousse, F. Maltey, M. Meulien, M. Mezzarobba, C. Pernet, N. M. Thiéry, P. Zimmermann, *Calcul mathématique avec Sage*, CreateSpace, 2013, electronic version available under Creative Commons license, https://hal.inria.fr/inria-00540485.

Book chapters

[270] P. Gaudry, “Algorithmes de comptage de points d’une courbe définie sur un corps fini”, *in : Explicit Methods in Number Theory Rational Points and Diophantine Equations*, K. Belabas (editor), *Panoramas et synthèses*, *36*, SMF, 2013, https://hal.inria.fr/hal-00840136.

[271] E. Thomé, “Function Field Sieve”, *in : Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia (editors), Springer, 2011, p. 501–502, https://hal.inria.fr/hal-00942002.

[272] E. Thomé, “Sieving in Function Fields”, *in : Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia (editors), Springer, 2011, p. 1205–1206, https://hal.inria.fr/hal-00942003.

Other Publications

[273] S. Bai, E. Thomé, P. Zimmermann, “Factorisation of RSA-704 with CADO-NFS”, working paper or preprint, 2012, https://hal.inria.fr/hal-00760322.

[274] F. Bihan, P.-J. Spaenlehauer, “Sparse Polynomial Systems with many Positive Solutions from Bipartite Simplicial Complexes”, working paper or preprint, October 2015, https://hal.inria.fr/hal-01217547.

[275] C. Bouvier, “The filtering step of discrete logarithm and integer factorization algorithms”, working paper or preprint, June 2013, https://hal.inria.fr/hal-00734654.

[276] S. Covanov, E. Thomé, “Fast arithmetic for faster integer multiplication”, working paper or preprint, January 2015, https://hal.inria.fr/hal-01108166.

[277] N. Coxon, “Montgomery’s method of polynomial selection for the number field sieve”, working paper or preprint, December 2014, https://hal.inria.fr/hal-01097069.

[278] J. Detrey, “FFS Factory: Adapting Coppersmith’s ”Factorization Factory” to the Function Field Sieve”, working paper or preprint, May 2014, https://hal.inria.fr/hal-01002419.

[279] J.-G. Dumas, E. Kaltofen, E. Thomé, “Interactive certificate for the verification of Wiedemann’s Krylov sequence: application to the certification of the determinant, the minimal and the characteristic polynomials of sparse matrices”, working paper or preprint, July 2015, https://hal.archives-ouvertes.fr/hal-01171249.

[280] P. Gaudry, "Integer factorization and discrete logarithm problems", Notes d'un cours donné aux Journées Nationales de Calcul Formel, 2014, https://hal.inria.fr/hal-01215553.

[281] S. Ionica, E. Thomé, "Isogeny graphs with maximal real multiplication", working paper or preprint, January 2015, https://hal.archives-ouvertes.fr/hal-00967742.

[282] H. Labrande, "Computing Jacobi's θ in quasi-linear time", working paper or preprint, November 2015, https://hal.inria.fr/hal-01227699.

[283] P. Lacharme, A. Rock, V. Strubel, M. Videau, "The Linux Pseudorandom Number Generator Revisited", 2012, déposé sur Cryptology ePrint Archive (http://eprint.iacr.org/), https://hal.archives-ouvertes.fr/hal-01005441.

[284] M. Massierer, "Some experiments investigating a possible L(1/4) algorithm for the discrete logarithm problem in algebraic curves", working paper or preprint, December 2014, https://hal.inria.fr/hal-01097362.

[285] P. Molin, "Multi-precision computation of the complex error function", working paper or preprint, March 2011, https://hal.archives-ouvertes.fr/hal-00580855.

5 References for Magrit

Doctoral Dissertations

[286] S. Bhat, *Visual words for pose computation*, Theses, Université de Lorraine, January 2013, https://tel.archives-ouvertes.fr/tel-00794630.

[287] N. Haouchine, *Image-guided Simulation for Augmented Reality during Hepatic Surgery*, Theses, Université de Lille1, January 2015, https://hal.inria.fr/tel-01254439.

[288] N. Noury, *A Contrario matching of interest points through both geometric and photometric constraints*, Theses, Université Henri Poincaré - Nancy I, October 2011, https://tel.archives-ouvertes.fr/tel-00640168.

[289] A. Yureidini, *Robust blood vessel surface reconstruction for interactive simulations from patient data*, Theses, Université des Sciences et Technologie de Lille - Lille I, May 2014, https://tel.archives-ouvertes.fr/tel-01010973.

Articles in International Peer-Reviewed Journal

[290] M. Aron, M.-O. Berger, E. Kerrien, B. Wrobel-Dautcourt, B. Potard, Y. Laprie, "Multimodal acquisition of articulatory data: geometrical and temporal registration", *Journal of the Acoustical Society of America*, 2016.

[291] B. Blaysat, M. Grediac, F. Sur, "Effect of interpolation on noise propagation from images to DIC displacement maps", *International Journal for Numerical Methods in Engineering*, 2016, https://hal.inria.fr/hal-01255944.

[292] B. Blaysat, M. Grediac, F. Sur, "On the propagation of camera sensor noise to displacement maps obtained by DIC - an experimental study", *Experimental Mechanics*, 2016, https://hal.inria.fr/hal-01269655.

[293] M. Grediac, F. Sur, C. Badulescu, J.-D. Mathias, “Using deconvolution to improve the metrological performance of the grid method”, *Optics and Lasers in Engineering 51*, 6, 2013, p. 716–734, WOS, https://hal.inria.fr/hal-00801133.

[294] M. Grediac, F. Sur, B. Blaysat, “Removing quasi-periodic noise in strain maps by filtering in the Fourier domain”, *Experimental Techniques*, 2015, p. 13, https://hal.inria.fr/hal-01163838.

[295] M. Grédiac, F. Sur, B. Blaysat, “The grid method for in-plane displacement and strain measurement: a review and analysis”, *Strain*, 2016, To be published.

[296] M. Grediac, F. Sur, “Effect of Sensor Noise on the Resolution and Spatial Resolution of Displacement and Strain Maps Estimated with the Grid Method”, *Strain 50*, 1, February 2014, p. 1–27, https://hal.inria.fr/hal-00937972.

[297] N. Haouchine, S. Cotin, I. Peterlik, J. Dequidt, M. Sanz-Lopez, E. Kerrien, M.-O. Berger, “Impact of Soft Tissue Heterogeneity on Augmented Reality for Liver Surgery”, *IEEE Transactions on Visualization and Computer Graphics 21*, 5, 2015, p. 584 – 597, https://hal.inria.fr/hal-01136728.

[298] N. Haouchine, J. Dequidt, M.-O. Berger, S. Cotin, “Monocular 3D Reconstruction and Augmentation of Elastic Surfaces with Self-occlusion Handling”, *IEEE Transactions on Visualization and Computer Graphics*, 2015, p. 14, https://hal.inria.fr/hal-01186011.

[299] S. Johnson, C. Hunt, H. Woolnough, M. Crawshaw, C. Kilkenny, D. Gould, A. Sinha, A. England, P.-F. Villard, “Virtual Reality, Ultrasound-guided Liver Biopsy Simulator: Development and Performance Discrimination”, *British Journal of Radiology*, 2011, https://hal.inria.fr/inria-00560487.

[300] S. Ouni, V. Colotte, U. Musti, A. Toutios, B. Wrobel-Dautcourt, M.-O. Berger, C. Lavecchia, “Acoustic-visual synthesis technique using bimodal unit-selection”, *EURASIP Journal on Audio, Speech, and Music Processing*, 2013:16, June 2013, https://hal.inria.fr/hal-00835854.

[301] F. P. Vidal, P.-F. Villard, “Development and Validation of Real-time Simulation of X-ray Imaging with Respiratory Motion”, *Computerized Medical Imaging and Graphics 49*, April 2016, p. 15, https://hal.inria.fr/hal-01266065.

[302] N. Padoy, T. Blum, A. Ahmadi, H. Feussner, M.-O. Berger, N. Navab, “Statistical Modeling and Recognition of Surgical Workflow”, *Medical Image Analysis*, 2011, https://hal.inria.fr/inria-00526493.

[303] G. Simon, M.-O. Berger, “Interactive Building and Augmentation of Piecewise Planar Environments Using the Intersection Lines”, *Visual Computer 27*, 9, February 2011, p. 827–841, https://hal.inria.fr/inria-00565129.

[304] F. Sur, M. Grediac, “Sensor Noise Modeling by Stacking Pseudo-Periodic Grid Images Affected by Vibrations”, *IEEE Signal Processing Letters 21*, 4, April 2014, p. 432–436, https://hal.inria.fr/hal-00955709.

[305] F. Sur, M. Grediac, “Towards deconvolution to enhance the grid method for in-plane strain measurement”, *Inverse Problems and Imaging 8*, 1, March 2014, p. 259–291, https://hal.inria.fr/hal-00955703.

[306] F. Sur, M. Grediac, "Automated removal of quasiperiodic noise using frequency domain statistics", *Journal of Electronic Imaging 24*, 1, February 2015, p. 013003/1–19, https://hal.inria.fr/hal-01116309.

[307] F. Sur, M. Grediac, "Measuring the Noise of Digital Imaging Sensors by Stacking Raw Images Affected by Vibrations and Illumination Flickering", *SIAM J. on Imaging Sciences 8*, 1, March 2015, p. p. 611–643, https://hal.inria.fr/hal-01133358.

[308] F. Sur, M. Grediac, "On noise reduction in strain maps obtained with the grid method by averaging images affected by vibrations", *Optics and Lasers in Engineering 66*, March 2015, p. 210–222, https://hal.inria.fr/hal-01075764.

[309] F. Sur, M. Grédiac, "Influence of the analysis window on the metrological performance of the grid method", *Journal of Mathematical Imaging and Vision*, 2016, To be published.

[310] F. Sur, N. Noury, M.-O. Berger, "An A Contrario Model for Matching Interest Points under Geometric and Photometric Constraints", *SIAM Journal on Imaging Sciences 6*, 4, 2013, p. 1956–1978, https://hal.inria.fr/hal-00876215.

[311] F. P. Vidal, P.-F. Villard, E. Lutton, "Tuning of patient specific deformable models using an adaptive evolutionary optimization strategy", *IEEE Transactions on Biomedical Engineering 59*, 10, October 2012, p. 2942 – 2949, https://hal.inria.fr/hal-00731910.

[312] P.-F. Villard, F. P. Vidal, L. Ap Cenydd, R. Holbrey, S. Pisharody, S. Johnson, A. Bulpitt, N. W. John, F. Bello, D. A. Gould, "Interventional radiology virtual simulator for liver biopsy", *International Journal of Computer Assisted Radiology and Surgery*, 2013, p. 1–13, https://hal.inria.fr/hal-00849184.

Major International Conferences

[313] S. Bhat, M.-O. Berger, F. Sur, "Visual words for 3D reconstruction and pose computation", *in : The First Joint 3DIM/3DPVT Conference*, p. 326 – 333, Hangzhou, China, May 2011, https://hal.inria.fr/inria-00576915.

[314] B. Blaysat, M. Grediac, F. Sur, "On noise prediction in maps obtained with global DIC", *in : SEM Annual Conference & Exposition on Experimental and Applied Mechanics - 2015*, H. Jin, S. Yoshida, L. Lamberti, M.-T. Lin (editors), *Advancement of Optical Methods in Experimental Mechanics*, 3, SEM, Springer, p. 211–216, Costa Mesa, CA, United States, June 2015, https://hal.inria.fr/hal-01163331.

[315] A. Bonneau, B. Wrobel-Dautcourt, "Efficiency of five labial correlates for /i/ and /y/ in adverse contexts", *in : The ninth International Seminar on Speech Production - ISSP'11*, Montreal, Canada, June 2011, https://hal.inria.fr/inria-00579160.

[316] C. Delmas, M.-O. Berger, E. Kerrien, C. Riddell, Y. Trousset, R. Anxionnat, S. Bracard, "Three-dimensional curvilinear device reconstruction from two fluoroscopic views", *in : SPIE, Medical Imaging 2015: Image-Guided Procedures, Robotic Interventions, and Modeling, 9415*, p. 94150F, San Diego, CA, France, February 2015, https://hal.inria.fr/hal-01139284.

[317] C. Delmas, C. Riddell, Y. Trousset, E. Kerrien, M.-O. Berger, "Intra-operative 3D micro-coil imaging using subsampled tomographic acquisition patterns on a biplane C-arm system ", *in : 4th International Conference on Image Formation in X-Ray Computed Tomography*, Bamberg, Germany, 2016.

[318] A. Eryildirim, M.-O. Berger, "A guided approach for automatic segmentation and modeling of the vocal tract in MRI images", *in : European Signal Processing Conference (EUSIPCO-2011)*, Barcelone, Spain, August 2011, https://hal.inria.fr/inria-00630642.

[319] S. Fleck, G. Simon, C. Bastien, "AIBLE: An Inquiry-Based Augmented Reality Environment for Teaching Astronomical Phenomena", *in : 13th IEEE International Symposium on Mixed and Augmented Reality - ISMAR 2014*, Munich, Germany, September 2014, https://hal.inria.fr/hal-01009548.

[320] S. Fleck, G. Simon, "An Augmented Reality Environment for Astronomy Learning in Elementary Grades: An Exploratory Study", *in : 25ème conférence francophone sur l'Interaction Homme-Machine, IHM'13*, AFIHM, ACM, Bordeaux, France, November 2013, https://hal.inria.fr/hal-00870478.

[321] A. Fond, M.-O. Berger, G. Simon, "Prior-based facade rectification for AR in urban environment", *in : ISMAR workshop on Urban Augmented Reality*, Fukuoka, Japan, September 2015, https://hal.archives-ouvertes.fr/hal-01235842.

[322] M. Grediac, F. Sur, C. Badulescu, J.-D. Mathias, "Deconvolving Strain Maps Obtained With the Grid Method", *in : SEM Annual Conference & Exposition on Experimental and Applied Mechanics - 2013*, H. Jin, C. Sciammarella, S. Yoshida, L. Lamberti (editors), *Advancement of Optical Methods in Experimental Mechanics*, *3*, Springer, p. 21–26, Lombard, Illinois, United States, June 2013, https://hal.inria.fr/hal-00830091.

[323] M. Grediac, F. Sur, "Stabilizing Heteroscedastic Noise With the Generalized Anscombe Transform. Application to Accurate Prediction of the Resolution in Displacement and Strain Maps Obtained With the Grid Method.", *in : SEM Annual Conference & Exposition on Experimental and Applied Mechanics - 2014*, H. Jin, C. Sciammarella, S. Yoshida, L. Lamberti (editors), *Advancement of Optical Methods in Experimental Mechanics*, *3*, Springer, p. 225–230, Greenville, SC, United States, June 2014, https://hal.inria.fr/hal-01001869.

[324] N. Hald, S. K. Sarker, P. Ziprin, P.-F. Villard, F. Bello, "Open surgery simulation of inguinal hernia repair.", *in : Medicine Meets Virtual Reality (MMVR)*, J. D. Westwood, S. W. Westwood, L. Felländer-Tsai, R. S. Haluck, H. M. Hoffman, R. A. Robb, S. Senger, K. G. Vosburgh (editors), *163*, IOS Press, p. 202–208, Newport Beach, California, United States, February 2011, https://hal.inria.fr/inria-00570250.

[325] N. Haouchine, J. Dequidt, M.-O. Berger, S. Cotin, "Deformation-based Augmented Reality for Hepatic Surgery", *in : Medicine Meets Virtual Reality, MMVR 20*, San Diego, United States, February 2013, https://hal.inria.fr/hal-00768372.

[326] N. Haouchine, J. Dequidt, M.-O. Berger, S. Cotin, "Single View Augmentation of 3D Elastic Objects", *in : International Symposium on Mixed and Augmented Reality - ISMAR*, Munich, Germany, September 2014, https://hal.inria.fr/hal-01056323.

[327] N. Haouchine, J. Dequidt, E. Kerrien, M.-O. Berger, S. Cotin, "Physics-based Augmented Reality for 3D Deformable Object", *in : VRIPHYS - Virtual Reality Interaction and Physical Simulation*, Darmstadt, Germany, December 2012, https://hal.inria.fr/hal-00768362.

[328] N. Haouchine, J. Dequidt, I. Peterlik, E. Kerrien, M.-O. Berger, S. Cotin, "Image-guided Simulation of Heterogeneous Tissue Deformation For Augmented Reality during Hepatic Surgery", *in : ISMAR - IEEE International Symposium on Mixed and Augmented Reality 2013*, Adelaide, Australia, October 2013, https://hal.inria.fr/hal-00842855.

[329] N. Haouchine, J. Dequidt, I. Peterlik, E. Kerrien, M.-O. Berger, S. Cotin, "Towards an Accurate Tracking of Liver Tumors for Augmented Reality in Robotic Assisted Surgery", *in : International Conference on Robotics and Automation (ICRA)*, Hong Kong, China, June 2014, https://hal.inria.fr/hal-01003262.

[330] Y. Laprie, M. Aron, M.-O. Berger, B. Wrobel-Dautcourt, "Studying MRI acquisition protocols of sustained sounds with a multimodal acquisition system", *in : 10th International Seminar on Speech Production (ISSP)*, Köln, Germany, May 2014, https://hal.inria.fr/hal-01002121.

[331] C. Léonet, G. Simon, M.-O. Berger, "In-Situ Interactive Modeling Using a Single-Point Laser Rangefinder Coupled with a New Hybrid Orientation Tracker", *in : 12th IEEE International Symposium on Mixed and Augmented Reality - ISMAR 2013*, Adelaide, Australia, October 2013, https://hal.inria.fr/hal-00870491.

[332] M. Loosvelt, P.-F. Villard, M.-O. Berger, "Using a biomechanical model for tongue tracking in ultrasound images", *in : ISBMS - 6th International Symposium on Biomedical Simulation*, Strasbourg, France, October 2014, https://hal.inria.fr/hal-01057861.

[333] U. Musti, V. Colotte, S. Ouni, C. Lavecchia, B. Wrobel-Dautcourt, M.-O. Berger, "Automatic Feature Selection for Acoustic-Visual Concatenative Speech Synthesis: Towards a Perceptual Objective Measure", *in : AVSP - Audio Visual Speech Processing*, Annecy, France, September 2013, https://hal.inria.fr/hal-00925115.

[334] U. Musti, C. Lavecchia, V. Colotte, S. Ouni, B. Wrobel-Dautcourt, M.-O. Berger, "ViSAC : Acoustic-Visual Speech Synthesis: The system and its evaluation", *in : FAA: The ACM 3rd International Symposium on Facial Analysis and Animation*, p. –, Vienne, Austria, September 2012, https://hal.archives-ouvertes.fr/hal-00762568.

[335] P. Rolin, M.-O. Berger, F. Sur, "Viewpoint simulation for camera pose estimation from an unstructured scene model", *in : International Conference on Robotics and Automation*, Seattle, United States, May 2015, https://hal.archives-ouvertes.fr/hal-01166785.

[336] M. Sanz-Lopez, J. Dequidt, E. Kerrien, C. Duriez, M.-O. Berger, S. Cotin, "Testbed for assessing the accuracy of interventional radiology simulations", *in : ISBMS - 6th International Symposium on Biomedical Simulation, LNCS*, Springer, Strasbourg, France, October 2014, https://hal.inria.fr/hal-01059892.

[337] C. Savariaux, P. Badin, S. Ouni, B. Wrobel-Dautcourt, "Étude comparée de la précision de mesure des systèmes d'articulographie électromagnétique 3D : Wave et AG500", *in : 29e Journées d'Études sur la Parole (JEP-TALN-RECITAL'2012)*, ATALA-AFCP (editor), p. 513–520, Grenoble, France, June 2012, https://hal.archives-ouvertes.fr/hal-00724682.

[338] G. Simon, A. Fond, M.-O. Berger, "A Simple and Effective Method to Detect Orthogonal Vanishing Points in Uncalibrated Images of Man-Made Environments", *in : Eurographics 2016*, Lisbon, Portugal, May 2016, https://hal.inria.fr/hal-01275628.

[339] G. Simon, "Tracking-by-Synthesis Using Point Features and Pyramidal Blurring", *in : 10th IEEE International Symposium on Mixed and Augmented Reality - ISMAR 2011*, Basel, Switzerland, October 2011, https://hal.inria.fr/inria-00614867.

[340] F. Sur, M. Grediac, "Enhancing with deconvolution the metrological performance of the grid method for in-plane strain measurement", *in : ICASSP - 38th International Conference on Acoustics, Speech, and Signal Processing*, p. 1563–1567, Vancouver, Canada, May 2013, https://hal.inria.fr/hal-00804719.

[341] F. Sur, M. Grediac, "Sensor noise measurement in the presence of a flickering illumination", *in : ICIP - IEEE International Conference on Image Processing*, p. p. 1763–1767, Paris, France, October 2014, https://hal.inria.fr/hal-01022379.

[342] F. Sur, "Illumination-invariant representation for natural colour images through SIFT matching", *in : ICASSP - 38th International Conference on Acoustics, Speech, and Signal Processing*, p. 1962 – 1966, Vancouver, Canada, May 2013, https://hal.inria.fr/hal-00804736.

[343] F. Sur, "An a-contrario approach to quasi-periodic noise removal", *in : ICIP - IEEE International Conference on Image Processing, Proceedings of ICIP 2015*, Québec City, Canada, September 2015, https://hal.inria.fr/hal-01211397.

[344] P.-F. Villard, P. Escamilla, E. Kerrien, S. Gorges, Y. Trousset, M.-O. Berger, "Preliminary Study of Rib Articulated Model based on Dynamic Fluoroscopy Images", *in : SPIE Medical Imaging*, p. 90361Y, San Diego, United Kingdom, February 2014, https://hal.archives-ouvertes.fr/hal-00933638.

[345] P.-F. Villard, N. Koenig, C. Perrenot, M. Perez, P. Boshier, "Toward a Realistic Simulation of Organ Dissection", *in : MMVR - Medicine Meets Virtual Reality 21*, p. 452–458, Manhattan Beach, United States, February 2014, https://hal.archives-ouvertes.fr/hal-00933621.

[346] P.-F. Villard, F. Vidal, F. Bello, N. W. John, "A Method to Compute Respiration Parameters for Patient-based Simulators", *in : MMVR - Medicine Meets Virtual Reality 19*, J. W. et al. (Eds.) (editor), *Medicine Meets Virtual Reality 19*, IOS Press, p. 529–533, Newport Beach (CA), United States, February 2012. Best Poster Award, https://hal.inria.fr/hal-00670512.

[347] A. Yureidini, E. Kerrien, S. Cotin, "Robust RANSAC-based blood vessel segmentation", *in : SPIE Medical Imaging*, D. R. Haynor, S. Ourselin (editors), *Image Processing, 8314*, SPIE Press, p. 8314M, San Diego, CA, United States, February 2012, https://hal.inria.fr/hal-00642003.

[348] A. Yureidini, E. Kerrien, J. Dequidt, C. Duriez, S. Cotin, "Local implicit modeling of blood vessels for interactive simulation", *in : MICCAI - 15th International Conference on Medical Image Computing and Computer-Assisted Intervention*, N. Ayache, H. Delingette, P. Golland, K. Moria (editors), *7510*, Springer, p. 553–560, Nice, France, October 2012, https://hal.inria.fr/hal-00741307.

Secondary International Conferences

[349] B. Blaysat, M. Grediac, F. Sur, "An experimental study of camera sensor noise propagation to displacement maps obtained by DIC", *in : Photomechanics*, Delft, Netherlands, May 2015, https://hal.inria.fr/hal-01163323.

[350] V. Cortier, J. Detrey, P. Gaudry, F. Sur, E. Thomé, M. Turuani, P. Zimmermann, "Ballot stuffing in a postal voting system", *in : Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems*, IEEE, p. 27 – 36, Trento, Italy, 2011, https://hal.inria.fr/inria-00612418.

[351] M. Grediac, F. Sur, C. Badulescu, J.-D. Mathias, "Improving the spatial resolution of the grid method with deconvolution", *in : PhotoMechanics - International conference on full-field measurement techniques and their applications in experimental solid mechanics - 2013*, Montpellier, France, May 2013, https://hal.inria.fr/hal-00829962.

[352] M. Grediac, F. Sur, "How noise propagates from camera sensor to displacement and strain maps obtained with the grid method", *in : ICEM16 - 16th International Conference on Experimental Mechanics*, Cambridge, United Kingdom, July 2014, https://hal.inria.fr/hal-01022373.

[353] F. P. Vidal, P.-F. Villard, E. Lutton, "Automatic tuning of respiratory model for patient-based simulation", *in : MIBISOC 2013 - International Conference on Medical Imaging using Bio-inspired and Soft Computing*, p. 225–231, Brussels, Belgium, May 2013, https://hal.inria.fr/hal-00824228.

[354] F. P. Vidal, P.-F. Villard, "Simulated Motion Artefact in Computed Tomography", *in : Eurographics Workshop on Visual Computing for Biology and Medicine*, Chester, United Kingdom, 2015, https://hal.inria.fr/hal-01237833.

[355] P.-F. Villard, P. E. Hammer, D. P. Perrin, P. J. Del Nido, R. Howe, "Individual-Based Mitral Valve Finite-Element Model", *in : Innovation, Design, and Emerging Alliances in Surgery*, Boston, United States, March 2015, https://hal.inria.fr/hal-01237756.

[356] A. Yureidini, J. Dequidt, E. Kerrien, C. Duriez, S. Cotin, "Computer-based simulation for the endovascular treatment of intracranial aneurysms", *in : LIVIM Imaging Worshop*, Strasbourg, France, December 2011, https://hal.inria.fr/hal-00641990.

Articles in National Peer-Reviewed Journal

[357] P. Rolin, M.-O. Berger, F. Sur, "Simulation de point de vue pour la mise en correspondance et la localisation.", *Traitement du Signal*, October 2015, https://hal.archives-ouvertes.fr/hal-01214374.

National Peer-Reviewed Conferences

[358] S. Alayrangues, G. Dowek, E. Kerrien, J. Mairesse, T. Viéville, "Médiation en sciences du numériques : un levier pour comprendre notre quotidien ?", *in : Science & You*, Nancy, France, June 2015, https://hal.inria.fr/hal-01211457.

[359] M. Gautier, B. Wrobel-Dautcourt, "Visualisation dynamique de programmes, artEoz : l'outil qui manquait", *in : Sciences et technologies de l'information et de la communication (STIC) en milieu éducatif*, B. Drot-Delange, G.-L. Baron, E. Bruillard (editors), Clermont-Ferrand, France, 2013, https://hal.inria.fr/edutice-00875615.

[360] N. Haouchine, S. Cotin, J. Dequidt, E. Kerrien, M.-O. Berger, "Réalité augmentée pour la chirurgie minimalement invasive du foie utilisant un modèle biomécanique guidé par l'image", *in : Reconnaissance de Formes et Intelligence Artificielle (RFIA) 2014*, France, June 2014, https://hal.archives-ouvertes.fr/hal-00988767.

[361] P. Rolin, M.-O. Berger, F. Sur, "Simulation de point de vue pour la localisation d'une caméra à partir d'un modèle non structuré", *in : Reconnaissance de formes et intelligence artificielle (RFIA) 2014*, France, June 2014, https://hal.archives-ouvertes.fr/hal-00988604.

[362] A. Yureidini, E. Kerrien, S. Cotin, "Reconstruction robuste des vaisseaux sanguins par surfaces implicites locales", *in : Orasis*, Praz-sur-Arly, France, June 2011, https://hal.inria.fr/inria-00579814.

Books

[363] P.-F. Villard, *Simulation du Mouvement Pulmonaire pour un Traitement Oncologique - Application à la Radiothérapie et à l'Hadronthérapie*, Editions universitaires europeennes, May 2011, ISBN-13: 978-613-1-56604-2 ISBN-10:6131566046, https://hal.archives-ouvertes.fr/hal-00595549.

Books or Proceedings Editing

[364] C. Linte, E. Chen, M.-O. Berger, J. Moore, D. Holmes, *Augmented Environments for Computer-Assisted Interventions*, *Lecture Notes in Computer Science*, *7815*, Springer, 2013, https://hal.inria.fr/hal-00865724.

Book chapters

[365] R. Anxionnat, M.-O. Berger, E. Kerrien, "Time to Go Augmented in Vascular Interventional Neuroradiology?", *in : Augmented Environments for Computer-Assisted Interventions*, C. Linte, E. Chen, M.-O. Berger, J. Moore, and D. H. III (editors), *Lecture Notes in Computer Sciences*, *7815*, Springer, 2013, p. 3–8, https://hal.inria.fr/hal-00865726.

[366] G. Simon, M.-O. Berger, "Réalité Augmentée et/ou Mixte", *in : Vidéo 3D : Capture, traitement et diffusion*, L. Lucas, C. Loscos, and Y. Remion (editors), *Hermes Science - Traité IC2, série Signal et image*, Hermes-Lavoisier, September 2013, https://hal.inria.fr/hal-00871730.

[367] P.-F. Villard, P. Boshier, F. Bello, D. Gould, "Virtual Reality Simulation of Liver Biopsy with a Respiratory Component", *in : Liver Biopsy*, H. Takahashi (editor), InTech, 2011, https://hal.inria.fr/inria-00621263.

[368] Y. Wei, S. Cotin, J. Dequidt, C. Duriez, J. Allard, E. Kerrien, "A (Near) Real-Time Simulation Method of Aneurysm Coil Embolization", *in : Aneurysm*, Y. Murai (editor), InTech, August 2012, p. 223–248, https://hal.inria.fr/hal-00736865.

Other Publications

[369] M. Grediac, F. Sur, C. Badulescu, J.-D. Mathias, "Using deconvolution to improve the metrological performance of the grid method", *Research Report number RR-8127*, INRIA, November 2012, https://hal.inria.fr/hal-00749812.

[370] A. Rousseau, A. Darnaud, B. Goglin, C. Acharian, C. Leininger, C. Godin, C. Holik, C. Kirchner, D. Rives, E. Darquie, E. Kerrien, F. Neyret, F. Masseglia, F. Dufour, G. Berry, G. Dowek, H. Robak, H. Xypas, I. Illina, I. Gnaedig, J. Jongwane, J. Ehrel, L. Viennot, L. Guion, L. Calderan, L. Kovacic, M. Collin, M.-A. Enard, M.-H. Comte, M. Quinson, M. Olivi, M. Giraud, M. Dorémus, M. Ogouchi, M. Droin, N. Lacaux, N. P. Rougier, N. Roussel, P. Guitton, P. Peterlongo, R.-M. Cornus, S. Vandermeersch, S. Maheo, S. Lefebvre, S. Boldo, T. Viéville, V. Poirel, A. Chabreuil, A. Fischer, C. Farge, C. Vadel, I. Astic, J.-P. Dumont, L. Féjoz, P. Rambert, P. Paradinas, S. De Quatrebarbes, S. Laurent, "Médiation Scientifique : une facette de nos métiers de la recherche", *Interne*, none, March 2013, https://hal.inria.fr/hal-00804915.

[371] G. Simon, "La Réalité Augmentée", May 2013, Article publié dans le magazine de l'Académie Lorraine des Sciences, https://hal.inria.fr/hal-00906963.

[372] F. Sur, M. Grediac, "Towards deconvolution to enhance the grid method for in-plane strain measurement", *Research Report number RR-8126*, INRIA, November 2012, https://hal.inria.fr/hal-00749804.

[373] F. Sur, M. Grediac, "An automated approach to quasi-periodic noise removal in natural images", *Research Report number RR-8660*, INRIA Nancy, équipe Magrit ; Institut Pascal, Université Blaise Pascal ; INRIA, January 2015, https://hal.inria.fr/hal-01099795.

[374] F. Sur, M. Grediac, "Measuring the noise of imaging sensors in the presence of vibrations and illumination flickering: modeling, algorithm, and experiments", *Research Report number RR-8672*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; Université Blaise Pascal ; INRIA, January 2015, https://hal.inria.fr/hal-01104124.

[375] F. Sur, N. Noury, M.-O. Berger, "Image point correspondences and repeated patterns", *Research Report number RR-7693*, INRIA, July 2011, https://hal.inria.fr/inria-00609998.

6 References for Vegas

Doctoral Dissertations

[376] G. Batog, *Classical problems in computer vision and computational geometry revisited with line geometry*, Theses, Université Nancy II, December 2011, https://tel.archives-ouvertes.fr/tel-00653043.

[377] Y. Bouzidi, *Solving bivariate algebraic systems and topology of plane curves*, Theses, Université de Lorraine, March 2014, https://tel.archives-ouvertes.fr/tel-00979707.

[378] X. Goaoc, *Transversal Helly numbers, pinning theorems and projection of simplicial complexes*, Habilitation à diriger des recherches, Université Henri Poincaré - Nancy I, December 2011, https://tel.archives-ouvertes.fr/tel-00650204.

[379] R. Thomasse, *Complexity analysis of random convex hulls*, Theses, Univeristé Nice Sophia Antipolis, December 2015, https://hal.inria.fr/tel-01252937.

Articles in International Peer-Reviewed Journal

[380] P. Angelini, D. Eppstein, F. Frati, M. Kaufmann, S. Lazard, T. Mchedlidze, M. Teillaud, A. Wolff, "Universal Point Sets for Planar Graph Drawing with Circular Arcs", *Journal of Graph Algorithms and Applications 18*, 3, May 2014, p. 313–324, https://hal.inria.fr/hal-00997207.

[381] B. Aronov, O. Cheong, X. Goaoc, R. Günter, "Lines Pinning Lines", *Discrete and Computational Geometry 44*, 2, 2011, p. 230–260, https://hal.inria.fr/inria-00518028.

[382] Y. Bouzidi, S. Lazard, M. Pouget, F. Rouillier, "Separating linear forms and Rational Univariate Representations of bivariate systems", *Journal of Symbolic Computation 68*, May 2015, p. 84–119, https://hal.inria.fr/hal-00977671.

[383] M. Caroli, M. Teillaud, "Delaunay triangulations of closed Euclidean d-orbifolds", *Discrete and Computational Geometry*, 2016, https://hal.inria.fr/hal-01294409.

[384] C. Chen, T. Gayral, S. Caro, D. Chablat, G. Moroz, S. Abeywardena, "A Six-Dof Epicyclic-Parallel Manipulator", *ASME Journal of Mechanisms and Robotics 4*, 4, April 2012, p. 1–8, https://hal.archives-ouvertes.fr/hal-00684803.

[385] O. Cheong, H. Everett, M. Glisse, J. Gudmundsson, S. Hornus, S. Lazard, M. Lee, H.-S. Na, "Farthest-Polygon Voronoi Diagrams", *Computational Geometry 44*, 4, 2011, p. 14 pages, https://hal.inria.fr/inria-00442816.

[386] O. Cheong, X. Goaoc, A. Holmsen, "Lower Bounds to Helly Numbers of Line Transversals to Disjoint Congruent Balls", *Israël Journal of Mathematics 190*, 2012, p. 213–228.

[387] O. Cheong, X. Goaoc, C. Nicaud, "Set Systems and Families of Permutations with Small Traces", *European Journal of Combinatorics 34*, 2013, p. 229–239, https://hal.inria.fr/hal-00752064.

[388] É. C. De Verdière, G. Ginot, X. Goaoc, "Helly numbers of acyclic families", *Advances in Mathematics 253*, 2014, p. 163–193, https://hal.inria.fr/hal-00646166.

[389] O. Devillers, M. Glisse, X. Goaoc, G. Moroz, M. Reitzner, "The monotonicity of f-vectors of random polytopes", *Electronic Communications in Probability 18*, 23, 2013, p. 1–8, https://hal.inria.fr/hal-00805690.

[390] O. Devillers, M. Glisse, X. Goaoc, R. Thomasse, "Smoothed complexity of convex hulls by witnesses and collectors", *Journal of Computational Geometry 7*, 2, 2016, p. 101–144, https://hal.inria.fr/hal-01285120.

[391] V. Dujmović, W. Evans, S. Lazard, W. Lenhart, G. Liotta, D. Rappaport, S. Wismath, "On Point-sets that Support Planar Graphs", *Computational Geometry 43*, 1, 2013, p. 29–50, https://hal.inria.fr/hal-00684510.

[392] M. Glisse, S. Lazard, J. Michel, M. Pouget, "Silhouette of a random polytope", *Journal of Computational Geometry 7*, 1, 2016, p. 14, https://hal.inria.fr/hal-01289699.

[393] M. Glisse, S. Lazard, "On the Complexity of Sets of Free Lines and Line Segments Among Balls in Three Dimensions", *Discrete and Computational Geometry 47*, 4, 2012, p. 756–772, https://hal.inria.fr/hal-00643880.

[394] X. Goaoc, H.-S. Kim, S. Lazard, "Bounded-Curvature Shortest Paths through a Sequence of Points using Convex Optimization", *SIAM Journal on Computing 42*, 2, 2013, p. 662–684, https://hal.inria.fr/hal-00927100.

[395] X. Goaoc, S. Koenig, S. Petitjean, "Pinning a Line by Balls or Ovaloids in R^3", *Discrete and Computational Geometry 45*, 2, 2011, p. 303–320, https://hal.inria.fr/inria-00518033.

[396] X. Goaoc, J. Matoušek, P. Paták, Z. Safernová, M. Tancer, "Simplifying inclusion-exclusion formulas", *Combinatorics, Probability and Computing 24*, 2, 2015, p. 438–456, http://arxiv.org/abs/1207.2591.

[397] M. Hemmer, L. Dupont, S. Petitjean, E. Schömer, "A Complete, Exact and Efficient Implementation for Computing the Edge-Adjacency Graph of an Arrangement of Quadrics", *Journal of Symbolic Computation 46*, 4, 2011, p. 467–494, https://hal.inria.fr/inria-00537592.

[398] P. Kamousi, S. Lazard, A. Maheshwari, S. Wuhrer, "Analysis of Farthest Point Sampling for Approximating Geodesics in a Graph", *Computational Geometry 57*, 2016, p. 1–7, https://hal.inria.fr/hal-01297624.

[399] M. Manubens, G. Moroz, D. Chablat, P. Wenger, F. Rouillier, "Cusp Points in the Parameter Space of Degenerate 3-RPR Planar Parallel Manipulators", *ASME Journal of Mechanisms and Robotics*, 2012, p. 1–10, https://hal.archives-ouvertes.fr/hal-00690975.

[400] G. Moroz, B. Aronov, "Computing the Distance between Piecewise-Linear Bivariate Functions", *ACM Transactions on Algorithms 12*, 1, February 2016, p. 3:1–3:13, https://hal.archives-ouvertes.fr/hal-01112394.

Major International Conferences

[401] D. Attali, O. Devillers, M. Glisse, S. Lazard, "Recognizing shrinkable complexes is NP-complete", *in : 22nd European Symposium on Algorithms – ESA*, A. Schulz, D. Wagner (editors), *8737*, Springer, p. 74–86, Wroclaw, Poland, 2014, https://hal.inria.fr/hal-01015747.

[402] M. Bogdanov, M. Teillaud, G. Vegter, "Delaunay triangulations on orientable surfaces of low genus", *in : International Symposium on Computational Geometry*, p. 20:1–20:15, Boston, United States, June 2016, https://hal.inria.fr/hal-01276386.

[403] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget, F. Rouillier, "Improved algorithm for computing separating linear forms for bivariate systems", *in : ISSAC - 39th International Symposium on Symbolic and Algebraic Computation*, Kobe, Japan, July 2014, https://hal.inria.fr/hal-00992634.

[404] Y. Bouzidi, S. Lazard, M. Pouget, F. Rouillier, "Rational Univariate Representations of Bivariate Systems and Applications", *in : ISSAC - 38th International Symposium on Symbolic and Algebraic Computation*, p. 109–116, Boston, United States, June 2013, https://hal.inria.fr/hal-00809430.

[405] Y. Bouzidi, S. Lazard, M. Pouget, F. Rouillier, "Separating Linear Forms for Bivariate Systems", *in : ISSAC - 38th International Symposium on Symbolic and Algebraic Computation*, p. 117–124, Boston, United States, June 2013, https://hal.inria.fr/hal-00809425.

[406] D. Chablat, R. Jha, F. Rouillier, G. Moroz, "Non-singular assembly mode changing trajectories in the workspace for the 3-RPS parallel robot", *in : 14th International Symposium on Advances in Robot Kinematics*, p. 149 – 159, Ljubljana, Slovenia, June 2014, https://hal.archives-ouvertes.fr/hal-00956325.

[407] D. Chablat, R. Jha, F. Rouillier, G. Moroz, "Workspace and joint space analysis of the 3-RPS parallel robot", *in : ASME 2013 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference, Volume 5A*, p. 1–10, Buffalo, United States, August 2014, https://hal.archives-ouvertes.fr/hal-01006614.

[408] D. Chablat, G. Moroz, V. Arakelian, S. Briot, P. Wenger, "Solution regions in the parameter space of a 3-RRR decoupled robot for a prescribed workspace", *in : Advances in Robot Kinematics*, Kluwer Academic Publishers, p. 1–8, Innsbruck, Austria, June 2012, https://hal.archives-ouvertes.fr/hal-00687005.

[409] D. Chablat, E. Ottaviano, G. Moroz, "A comparative study of 4-cable planar manipulators based on cylindrical algebraic decomposition", *in : Proceedings of the ASME 2011 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference*, p. 1–10, Washington, United States, August 2011, https://hal.archives-ouvertes.fr/hal-00597924.

[410] É. C. De Verdière, G. Ginot, X. Goaoc, "Multinerves and Helly Numbers of Acyclic Families", *in : 27th Symposium on Computational Geometry – SoCG'12*, ACM, p. 209–218, Chapel Hill, United States, June 2012. Received one of the two Best paper awards., https://hal.inria.fr/hal-00752073.

[411] O. Devillers, M. Glisse, X. Goaoc, R. Thomasse, "On the smoothed complexity of convex hulls", *in : 31st Symposium on Computational Geometry – SoCG'15*, Lipics, Eindhoven, Netherlands, June 2015, https://hal.inria.fr/hal-01144473.

[412] O. Devillers, M. Glisse, X. Goaoc, "Complexity Analysis of Random Geometric Structures Made Simpler", *in : 29th Symposium on Computational Geometry – SoCG'13*, p. 167–175, Rio, Brazil, June 2013, https://hal.inria.fr/hal-00833774.

[413] O. Devillers, M. Karavelas, M. Teillaud, "Qualitative Symbolic Perturbation", *in : SoCG 2016 - International Symposium on Computational Geometry*, p. 33:1–33:15, Boston, United States, June 2016, https://hal.inria.fr/hal-01276444.

[414] V. Dujmović, W. Evans, S. Lazard, W. Lenhart, G. Liotta, D. Rappaport, S. Wismath, "On Point-sets that Support Planar Graphs", *in : 19th International Symposium on Graph Drawing – GD'11*, Eindhoven, Netherlands, September 2011, https://hal.inria.fr/hal-00643824.

[415] I. Z. Emiris, G. Moroz, "The assembly modes of rigid 11-bar linkages", *in : IFToMM 2011 World Congress*, IFToMM - Mexico, Universidad de Guanajuato, Guanajuato, Mexico, June 2011, https://hal.inria.fr/inria-00530327.

[416] R. Imbach, G. Moroz, M. Pouget, "Numeric and Certified Isolation of the Singularities of the Projection of a Smooth Space Curve", *in : Proceedings of the 6th International Conferences on Mathematical Aspects of Computer and Information Sciences – MASIS*, Springer LNCS, Berlin, Germany, October 2015, https://hal.inria.fr/hal-01239447.

[417] R. Jha, D. Chablat, F. Rouillier, G. Moroz, "An algebraic method to check the singularity-free paths for parallel robots", *in : International Design Engineering Technical Conferences & Computers and Information in Engineering Conference*, ASME, Boston, United States, August 2015, https://hal.archives-ouvertes.fr/hal-01142989.

[418] R. Jha, D. Chablat, F. Rouillier, G. Moroz, "Workspace and Singularity analysis of a Delta like family robot", *in : 4th IFTOMM International Symposium on Robotics and Mechatronics*, Poitiers, France, June 2015, https://hal.archives-ouvertes.fr/hal-01142465.

[419] G. Moroz, B. Aronov, "Computing the Distance between Piecewise-Linear Bivariate Functions", *in : SODA - Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms - 2012*, SIAM, Kyoto, Japan, January 2012, https://hal.inria.fr/inria-00608255.

Secondary International Conferences

[420] P. Angelini, D. Eppstein, F. Frati, M. Kaufmann, S. Lazard, T. Mchedlidze, M. Teillaud, A. Wolff, "Universal Point Sets for Planar Graph Drawings with Circular Arcs", *in : Canadian Conference on Computational Geometry – CCCG*, p. 117–122, Waterloo, Canada, August 2013, https://hal.inria.fr/hal-00846953.

[421] O. Bodini, G. Moroz, H. Tafat-Bouzid, "Infinite Boltzmann Samplers and Applications to Branching Processes", *in : GASCom - 8th edition of the conference GASCom on random generation*

of combinatorial structures - 2012, Bordeaux, France, June 2012, https://hal.inria.fr/hal-00763301.

[422] M. Bogdanov, M. Caroli, M. Teillaud, "Computing Periodic Triangulations", *in : Shape up - Exercises in Materials Geometry and Topology*, p. 60–61, Berlin, Germany, September 2015, https://hal.inria.fr/hal-01224549.

[423] Y. Bouzidi, S. Lazard, M. Pouget, F. Rouillier, "New bivariate system solver and topology of algebraic curves", *in : 27th European Workshop on Computational Geometry - EuroCG 2011*, Morschach, Switzerland, March 2011, https://hal.inria.fr/inria-00580431.

[424] X. Goaoc, J. Matoušek, P. Paták, Z. Safernová, M. Tancer, "Simplifying inclusion-exclusion formulas", *in : European Conference on Combinatorics, Graph Theory and Applications – EuroCOMB*, Pisa, Italy, September 2013. 14 pages, 1 figure, https://hal.inria.fr/hal-00764182.

[425] G. Tzoumas, "Exact medial axis of quadratic NURBS curves", *in : 27th European Workshop on Computational Geometry – EuroCG'11*, Morschach, Switzerland, March 2011, https://hal.inria.fr/inria-00581588.

Books or Proceedings Editing

[426] S.-W. Cheng, O. Devillers (editors), *Discrete and Computational Geometry; Special Issue: 30th Symposium on Computational Geometry*, *53*, 3, springer, 2015, https://hal.inria.fr/hal-01154063.

[427] S.-W. Cheng, O. Devillers (editors), *Journal of Computational Geometry; Special issue of Selected Papers from SoCG 2014*, *6*, 2, Computational Geometry Lab, Carleton University, 2015, https://hal.inria.fr/hal-01154065.

[428] O. Cheong, J. Erickson, M. Teillaud (editors), *Proceedings of Computational Geometry (Dagstuhl Seminar 15111)*, France, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015, https://hal.inria.fr/hal-01177029.

Book chapters

[429] L. Castelli Aleardi, O. Devillers, J. Rossignac, "Compact data structures for triangulations Name: Compact data structures for triangulations", *in : Encyclopedia of Algorithms*, Springer, 2015, https://hal.inria.fr/hal-01168565.

[430] O. Devillers, "Delaunay triangulation and randomized constructions", *in : Encyclopedia of Algorithms*, Springer, 2014, https://hal.inria.fr/hal-01168575.

Other Publications

[431] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget, F. Rouillier, M. Sagraloff, "Improved algorithms for solving bivariate systems via Rational Univariate Representations", *Research report*, Inria, June 2015, https://hal.inria.fr/hal-01114767.

[432] Y. Bouzidi, S. Lazard, M. Pouget, F. Rouillier, "Rational Univariate Representations of Bivariate Systems and Applications", *Research Report number RR-8262*, INRIA, March 2013, https://hal.inria.fr/hal-00802698.

[433] Y. Bouzidi, S. Lazard, M. Pouget, F. Rouillier, "Separating linear forms for bivariate systems", *Research Report number RR-8261*, INRIA, March 2013, https://hal.inria.fr/hal-00802693.

[434] O. Devillers, M. Glisse, X. Goaoc, G. Moroz, M. Reitzner, "The monotonicity of f-vectors of random polytopes", *Research Report number RR-8154*, INRIA, 2012, https://hal.inria.fr/hal-00758686.

[435] O. Devillers, M. Glisse, X. Goaoc, R. Thomasse, "Smoothed complexity of convex hulls by witnesses and collectors", *Research Report number 8787*, INRIA, October 2015, https://hal.inria.fr/hal-01214021.

[436] O. Devillers, M. Glisse, X. Goaoc, "Complexity analysis of random geometric structures made simpler", *Research Report number RR-8168*, INRIA, 2012, https://hal.inria.fr/hal-00761171.

[437] O. Devillers, R. Hemsley, "The worst visibility walk in a random Delaunay triangulation is $O(\sqrt{n})$", *Research Report number RR-8792*, INRIA, October 2015, https://hal.inria.fr/hal-01216212.

[438] O. Devillers, M. Karavelas, M. Teillaud, "Qualitative Symbolic Perturbation: a new geometry-based perturbation framework", *Research Report number RR-8153*, INRIA, 2015, https://hal.inria.fr/hal-00758631.

[439] M. Glisse, S. Lazard, J. Michel, M. Pouget, "Silhouette of a random polytope", *Research Report number RR-8327*, INRIA, July 2013, https://hal.inria.fr/hal-00841374.

[440] R. Imbach, P. Mathis, P. Schreck, "A Robust and Efficient Method for Solving Point Distance Problems by Homotopy", *Research Report number RR-8705*, INRIA, January 2016, https://hal.inria.fr/hal-01135230.

[441] R. Imbach, G. Moroz, M. Pouget, "Numeric certified algorithm for the topology of resultant and discriminant curves", *Research Report number RR-8653*, Inria, April 2015, https://hal.inria.fr/hal-01093040.

[442] R. Imbach, "A Subdivision Solver for Systems of Large Dense Polynomials", *Technical Report number RT-0476*, INRIA Nancy, March 2016, https://hal.inria.fr/hal-01293526.

[443] P. Kamousi, S. Lazard, A. Maheshwari, S. Wuhrer, "Analysis of Farthest Point Sampling for Approximating Geodesics in a Graph", *Research report*, INRIA, November 2013, https://hal.inria.fr/hal-00927643.

[444] S. Lazard, M. Pouget, F. Rouillier, "Bivariate Triangular Decompositions in the Presence of Asymptotes", *Research report*, INRIA, September 2015, https://hal.inria.fr/hal-01200802.

[445] G. Moroz, "Fast polynomial evaluation and composition", *Technical Report number RT-0453*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; INRIA, July 2013, https://hal.archives-ouvertes.fr/hal-00846961.

[446] J. Recknagel, *Topology of planar singular curves resultant of two trivariate polynomials*, Mémoire, Institute for Computer Science, Martin-Luther-University, Halle-Wittenberg, August 2013, https://hal.inria.fr/hal-00927768.

7 Other References of Department 1

Articles in International Peer-Reviewed Journal

[447] A. E. Frid, D. Jamet, "The number of binary rotation words", *RAIRO - Theoretical Informatics and Applications (RAIRO: ITA) 48*, 4, October 2014, p. 453 – 465, The original publication is available at www.rairo-ita.org., https://hal.archives-ouvertes.fr/hal-01089726.

[448] Jamet, Damien, "Foreword - Special issue dedicated to the fifteenth "Journées Montoises d'Informatique Théorique"", *RAIRO-Theor. Inf. Appl. 50*, 1, 2016, p. 1, http://dx.doi.org/10.1051/ita/2016012.

Major International Conferences

[449] V. Berthé, D. Jamet, T. Jolivet, X. Provençal, "Critical Connectedness of Thin Arithmetical Discrete Planes", *in : International Conference Discrete Geometry for Computer Imagery*, *7749*, p. 107–118, Sevilla, Spain, March 2013, https://hal.archives-ouvertes.fr/hal-00943827.

[450] D. Jamet, X. Provençal, L. Nadia, "Generation of Digital Planes Using Generalized Continued-Fractions Algorithms", *in : 19th IAPR International Conference on Discrete Geometry for Computer Imagery*, Springer (editor), *Discrete Geometry for Computer Imagery 19th IAPR International Conference, DGCI 2016, Nantes, France, April 18-20, 2016. Proceedings*, *9647*, p. 45–56, Nantes, France, April 2016, https://hal.archives-ouvertes.fr/hal-01364622.

02

Project

Loria

Department 1

Algorithms, Computation, Geometry and Image

Department Head: Sylvain Lazard

Department project

As already mentioned in the section concerning the evaluation period, *algorithms* is a common center of interest to all these teams (and of course to some teams of other departments as well). Beside this common ground, there are various centers of interest common to several teams. *Geometry* plays an important role in most teams, i.e., ADAGIO, ALICE, CARAMBA, MAGRIT, and VEGAS. *Symbolic and algebraic computing* is of common interest of CARAMBA and VEGAS, *image* is of interest to ADAGIO, ALICE and MAGRIT, *combinatorics and complexity* also concerns several groups as ADAGIO, CARAMBA, and VEGAS, *certified computing* (in a sense that sometimes requires computing with arbitrary precision numbers) is also of common interest to CARAMBA, VEGAS, ADAGIO, and ALICE. The main common interest of ABC with the other groups is the algorithmic culture they share.

Although not all, most research topics in our department have a strong mathetical and theoretical flavor. As a result, our high-level research topics are quite stable and we do not envision drastic thematic changes from the past evaluation period to the next. We thus refer to the section concerning the evaluation period for a description of our research topics.

1 Life and governance of the department

In terms of governance, we run our department with a council that consists of the head of the department and the heads of the teams. This council handles typical matters at the level of the department such as the scientfic animation, the evaluation and ranking of PhD candidates for UL contracts, the department bugdet, the needs for new faculty positions (*profils de postes*), etc.

The head of the departement (unless conflicts of interest) also oversees for CNRS and UL the creation of new teams. This process is recurrent for Inria-CNRS-UL teams becauce Inria teams last at most 12 years by rule. The evaluation period has seen the creation of Caramba (from Caramel) and we are in the process of creating Gamble (from Vegas). However, these two team creations did/do not involve any restructuring of the teams but only require(d) redefining their scientific projects. Teams are quite stable in our departement and there haven't been any fundamental restructuring.

The next evaluation period may see more changes though. The Alice team is quite large and growing from 7 to 9 faculty members in Sept. 2016. They will thus likely split in two new teams: one centered on geometry processing for scientific computing and the other on computer-aided fabrication (3d printing). Also, the fusion of LITA (Metz) with LORIA may have an impact on the department. Team ABC may

grow substentially as they already have some strong connexions with some LITA members (e.g., An Le Thi already joined ABC for one year on a “sabbatical”). This could also be an opportunity to create a team on graph theory since both labs have isolated researchers on the subject (such as Dieter Kratsch at LITA and Jean-Sebastien Sereni at LORIA). However, all these plans, in particular those involving LITA, are very speculative and the team projects (Section 2) do not enter into these considerations.

Scientific animation. The departement seminar is distributed in the sense that it is the teams' seminars that we share within the departement. This seminar organisation is not very formal but we are happy with it. These seminars are by nature specialized and thus concern subsets of the departement teams. For instance, seminars of algorithmic or geometric flavor potentially concern almost all teams. Those of algebraic nature gather Caramba and Vegas/Gamble and those on images involve Adagio, Alice and Magrit. We also have inter-departements seminars on computer security organized by Caramba and Pesto (D2, ex-Cassis), which also involves Madynes (D3) and Carte (D2). Furthermore, we recently started regular seminars and working groups involving Vegas/Gamble and teams from the IECL math lab (Tosca and Bigs teams).

We also organize once a year a day of the departement in which every PhD student presents their work. This is both a way to interact scientifically within the departement and also to help detect possible difficulties that PhD students may have. We also take advantage of lab evaluations to organize departement days in which teams present surveys of their realizations.

Master programs. We also discuss and coordinate within the departement for promoting coherent courses proposal in the UL computer science Master program. These involve in particular teams Alice, Adagio, Magrit and Vegas/Gamble. We are in particular in this process for the future Master program.

2 SWOT

	Positive	Negative
Intern	Strengths: - Good theoretical and practical expertise that covers a wide and coherent set of scientific domains - Teams stability - ERC & awards track record - Friendly relations beetween teams which yields an healthy dpt governance - INRIA scientific environment - Augmented funding opportunities (e.g. PhD grants) thanks to the combination of INRIA, UL, and CNRS environments	Weaknesses: - No local Master program in theoretical computer science
Extern	Opportunities: - Closeness of other labs in particular in Maths and Control (IECL and CRAN) and effective collaborations	Threats: - Difficulty to attract Maths PhD students despite the closness with IECL lab - Inadequation of European programs (except ERC) for most teams - Randomness of ANR programs - Duplication of administrative work (e.g. evalutations) due to INRIA and university/CNRS environment

3 ABC

Team composition

Yann Guermeur (DR CNRS, team leader), Fabien Lauer (MCF UL).

Project

The statistical learning theory is made up of three subfields: pattern classification (discrimination), regression and density estimation. For the evaluation period to come, we will concentrate on the two first ones.

Regarding pattern classification, we are primarily interested in margin multi-category models. For these models, our main goal consists in establishing guaranteed risks. More precisely, we want to study the dependency of the control term of such risks on the three basic parameters: the sample size m (convergence rate), the number C of categories, and the margin parameter γ. The results of this kind already available make use of different empirical pseudo-metrics on the functional classes of interest. We intend to establish a result holding for the pseudo-metrics associated with the L_p-norm, for p ranging from 1 to ∞. This result will provide us with a criterion to set the value of the hyperparameters of multi-category kernel machines. The corresponding non-convex programming problems will be solved by means of optimization methods developed in the framework of a collaboration with An Le Thi's research team.

We will continue our investigations on switching regression (i.e., learning piecewise affine/smooth target functions or a model arbitrarily switching between multiple submodels) with a focus on global optimality, theoretical guarantees and algorithmic complexity issues. The relationship between switching regression and robust regression will also lead us to tackle these issues in the more general framework of learning a single model in the presence of outliers. Works initiated in this direction have shown the importance of looking at these problems from a classification perspective. Therefore, the results to be obtained will also provide the basic tools to propose, for instance, exacts algorithms for empirical risk minimization in a classification context, with a broader impact.

4 ADAGIo

Team composition

Isabelle Debled-Rennesson (PR UL, team leader), Eric Domenjoud (CR CNRS), Philippe Even (PR UL), Bertrand Kerautret (MCF UL), Phuc Ngo (MCF UL).

Project

During the next years, we intend to carry on the work we took up in Discrete Geometry in the two following domains.

Study of discrete primitives. Among the basic primitives available in geometry, we focus on the arithmetical viewpoint, introduced by Jean-Pierre Reveillès [Rev91]. In this framework, analytical definitions

[Rev91] J-P. Reveillès. *Géométrie discrète, calculs en nombre entiers et algorithmique*. Thèse d'état, Université Louis Pasteur, Strasbourg, 1991.

of discrete primitives such as *digital straight line*, *digital plane* have been proposed. We study the arithmetical, geometrical, topological and combinatorial properties of these objects and we also are interested in introducing new definitions for non-linear discrete objects or for noisy objects.
Topological properties of arithmetical discrete primitives. We almost completely solved the problem of the $(d-1)$-connectedness of discrete hyperplanes in $\mathbb{R}^d$ [DPV16,BDJP14]. We want to complete these results in the case of hyperplanes with non-zero-shift and extend them to other connectedness and to linear objects of lower dimensions, i.e. to intersections of hyperplanes. To this aim, we will study the links which arose between this problem and numeration systems. We will also continue our study of these objects from a word combinatorics point of view.
Arithmetical study of discrete plane pieces. A first work [DRDR06]has been done about the arithmetic properties of the convex hull of a discrete straight line segment. It permits to obtain very efficient algorithms to decompose a curve into such primitives taking into account the convexity of the discrete curve. We want to obtain the same kind of results about the convex hull of discrete plane pieces. It could be used to obtain a guided decomposition of the discrete object borders.
Discrete primitives for 3D reconstruction from images. We plan to investigate the use of discrete blurred primitives within autonomous or supervised vision techniques. The blurred segment detection method [KE] we already developed to process gray-level images can be applied to provide fast edge tracking tools. We also intend to extend this method in order to process 3d data, such as LIDAR data. Furthermore these blurred primitives may be used to set up new 3d structure reconstruction algorithms able to get a better handling of uncertainty. Such primitive could be also exploited in the context of an industrial collaboration (NumAlliance company) where the 3d extension of defect measure is an important stage.

Analysis and modelling of discrete curves and surfaces. We develop new tools to analyse discrete objects and to reconstruct some continuous representations of them. Two main axes can be distinguished. On the one hand, the *multi-resolution analysis* of discrete curves and surfaces provides progressive analysis and new information. This analysis is based on the arithmetical, geometrical and combinatorial properties of the discrete primitives that permit to obtain efficient algorithms (recognition, scanning, ...) and to extract geometrical parameters (perimeter, curvature, normal vector, area, ...) on the discrete curves and surfaces. It is useful for the comparison, the classification or the simplification. On the other hand, the *reconstruction of geometrical models* with a controlled precision with respect to the original discrete curves or surfaces open perspectives for the use of a post-processing task based on Euclidean geometry.
Meaningful scale for 3D discrete curves and surfaces. The concept of meaningful scale [KL14,KL12] can also be extended for surfaces and 3D curves. A first step is to consider or introduce new definitions of maximal plane (resp. 3D segment) recognition and deduce asymptotic properties on area (resp. length).
Study of noisy discrete curves and surfaces. The notion of *Adaptive Tangential Cover (ATC)* [NNDRK16]

[DPV16] Eric Domenjoud, Xavier Provençal, and Laurent Vuillon. Palindromic language of thin discrete planes. *Theoretical Computer Science*, 2016.

[BDJP14] Valérie Berthé, Eric Domenjoud, Damien Jamet, and Xavier Provençal. Fully Subtractive Algorithm, Tribonacci numeration and connectedness of discrete planes. *RIMS Kôkyûroku Bessatsu*, (B46):159–174, 2014.

[DRDR06] H. Dörksen-Reiter and I. Debled-Rennesson. A linear algorithm for polygonal representations of digital sets. In *IWCIA*, volume 4040 of *LNCS*, pages 307–319. Springer, 2006.

[KE] B. Kerautret and Ph. Even. Blurred Segments in Gray Level Images for Interactive Line Extraction. In *Proc. of IWCIA 2009*, volume 5852 of *LNCS*, pages 176–186.

[KL14] Bertrand Kerautret and Jacques-Olivier Lachaud. Meaningful Scales Detection: an Unsupervised Noise Detection Algorithm for Digital Contours. *Image Processing On Line*, 4:18, May 2014.

[KL12] Bertrand Kerautret and Jacques-Olivier Lachaud. Meaningful Scales Detection along Digital Contours for Unsupervised Local Noise Estimation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(12):2379–2392, December 2012.

[NNDRK16] Phuc Ngo, Hayat Nasser, Isabelle Debled-Rennesson, and Bertrand Kerautret. Adaptive Tangential Cover for Noisy Digital Contours. In *DGCI 2016 - 19th international conference on Discrete Geometry for Computer Imagery*, Nantes, France, April 2016.

of a discrete curve is deduced from the *Meaningful thickness* [KLS12]. It permits to obtained curve decomposition into discrete segments transmitting the noise levels and the geometrical structure of the given discrete curve. It opens numerous perspectives for the geometrical estimators on discrete curves (2D and 3D) and on surfaces that we want to explore. For example, in the framework of the polyhedrization of 3D discrete objects, a first step could be to extend the notion of ATC to surfaces and to study the obtained structures.

Geometric properties of rigid transformations on $\mathbb{Z}^2$. Rigid transformation in $\mathbb{R}^n$ is a geometry-preserving operation. Due to digitisation effects, this important property is generally lost when considering digital images defined on $\mathbb{Z}^n$. In this context, we investigate this issue by studying rigid transformations on $\mathbb{Z}^2$. More precisely, the conditions/characterizations of digital images that allow the preservation of their geometric properties under arbitrary rigid transformations. This study adresses numerous image processing tasks such as image registration or shape analysis.

5 Alice

Team composition

Laurent Alonso (CR Inria), Dobrina Boltcheva (MCF UL), Samuel Hornus (CR Inria), Sylvain Lefebvre (DR Inria), Bruno Levy (DR Inria, team leader), Jonas Martinez (CR Inria) Nicolas Ray (CR Inria), Dmitry Sokolov (HdR, MCF UL), Cédric Zanni (MCF).

Project

We plan to continue to shift our Geometry Processing axis more and more towards **scientific computing and applied mathematics**. In particular, we focus on ways of decomposing a volume of interest into elementary cells (different forms of meshing). In a middle term, we plan to develop meshing algorithms that are adapted to existing numerical methods for solving Partial Differential Equations, and in a longer term, to prepare the ground for the upcoming next generation of such methods, developed in cooperation with mathematicians:

- **Hex-dominant and Hexahedral meshing.** (Middle-term objectives.) For some simulation techniques, meshes composed of deformed cube (i.e. hexahedra) are prefered over tetrahedral meshes. This is for several reasons, including the smaller number of elements, the fact that trilinear hexahedral elements can capture some order 3 terms whereas linear elements are… linear, and also because they can avoid some "locking" phenomena when used to model some physics, i.e. deformations of elastic materials. However, such hexahedral meshes are extremely difficult to produce. In 2010 we published the first method to automatically generate an hybrid hexahedral-dominant mesh (composed of hexahedra and tetrahedra). We refined the method in 2016, and we are now able to generate meshes with a very large proportion of hexahedra. We are targeting pure hexahedral meshes as a middle-term objective. In a shorter perspective, we are currently developing finite element techniques with hybrid elements, operating on mixed hexahedra-tetrahedra meshes, together with the evaluation techniques to measure the rate of convergence relative to element size. The first results, with linear elasticity, are very promising.

- **Towards an effective geometric measure theory.** (Longer-term objectives.) Two years ago, a network of mathematicians and computer scientists started to work together, with an ambitious

[KLS12] Bertrand Kerautret, Jacques-Olivier Lachaud, and Mouhammad Said. Meaningful Thickness Detection on Polygonal Curve. In *ICPRAM - International Conference on Pattern Recognition Applications and Methods - 2012*, pages 372–379, Vilamoura, Portugal, February 2012. SciTePress.

long-term vision, to invent new means of discretizing 3D shapes together with the equations that govern them. We started meeting and exchanging ideas on a regular basis (in Banff, Bonn, Paris, Montreal, Mexico …). Our point of view is to use a (measure) theory that describes both the continuous and the discrete settings. As a consequence, the good properties are naturally preserved by the computer implementation, without needing to adapt the theory and without losing properties. The expected long-term impact is a class of numerical solvers for a category of different problems (Optimal Transport, Monge Ampere equation) that can serve as a fundamental component in several domains (computational physics and deep learning).

This objective is very ambitious and difficult. To mitigate the risk, we developped a network which involve excellent mathematicians such as Yann Brenier, one of the inventors of Optimal Transport theory, and which is in the process of being formalized through submitted ANR and INRIA *exploratory* projects. Furthermore, on the path towards this long-term objective, the road is paved with intermediate goals that should have applications in geometric modeling, geometry processing, and Finite Element Analysis.

On the other hand, our past research axis on modeling and rendering also evolved into a research project on **computer aided fabrication and 3d printing**. This requires a full understanding of the creation pipeline, from the modeling of the object to the fabrication on 3D printers. This also means developing innovative CAD software for additive manufacturing, as we started to do with our IceSL software.

Our goal is to start from a description of an object in terms of solid operations (union, difference, intersection, offsetting) and directly generates the instructions driving the printer. We think that this strategy is especially well-suited for combining parts from existing designs, as well as dealing with shapes with complex, intricate geometries. A longer-term goal is to erase the boundaries between modeling and the printing process, and develop novel approaches considering both issues simultaneously.

We hope to bring novel ways to model complex shapes, developing algorithms that handle the difficult task of finding a compromise between the intention of the designer, the technical requirements of the fabrication process, and the function of the final, real object.

It should be stressed that research on 3d printing is fashionable and thus risky because there is an increasing level of competition in the Computer Graphics community. We intend to remain focused on what makes our point of view original, that is modeling from examples of complex geometries and geometry processing for fabrication through image/voxel based representations. This approach resulted in interesting contributions, and we think it will continue in the future. We also plan on working more closely with researchers in the field of additive manufacturing (processes/materials) to further explore the interaction between modeling and fabrication.

6 Caramba

Team composition

J. Detrey (CR INRIA), P. Gaudry (DR CNRS), P.-J. Spaenlehauer (CR INRIA), M. Videau (MCF UL), E. Thomé (DR INRIA, team leader), P. Zimmermann (DR INRIA).

Caramba was created as a team in January 2016, and is a follow-up to Caramel (joint INRIA-LORIA project-team). Caramba is still being reviewed as a proposal for a joint INRIA-LORIA project-team.

Project

Our research addresses the broad application domain of cryptography and cryptanalysis from the algorithmic perspective. We study all the algorithmic aspects, from the top-level mathematical background

down to the optimized high-performance software implementations. Several kinds of mathematical objects are commonly encountered in our research. Some basic ones are truly ubiquitous: integers, finite fields, polynomials, real and complex numbers. We also work with more structured objects such as number fields, algebraic curves, or polynomial systems. In all cases, our work is geared towards making computations with these objects effective and fast.

The mathematical objects we deal with are of utmost importance for the applications to cryptology, as they are the background of the most widely developed cryptographic primitives, such as the RSA cryptosystem or the Diffie–Hellman key exchange. The two facets of cryptology—cryptography and cryptanalysis—are central to our research. The key challenges are the assessment of the security of proposed cryptographic primitives, through the study of the cornerstone problems, which are the integer factorization and discrete logarithm problems, as well as the optimization work in order to enable cryptographic implementations that are both efficient *and* secure.

Among the research themes we set forth in our research proposal, two are guided by the most important mathematical objects used in today's cryptography, and two others are rather guided by the technological background we use to address these problems:

Extended NFS family. A common algorithmic framework, called the Number Field Sieve (NFS), addresses both the integer factorization problem as well as the discrete logarithm problem over finite fields. We have numerous algorithmic contributions in this context, and develop software to illustrate them. We plan to improve on the existing state of the art in this domain by researching new algorithms, by optimizing the software performance, and by demonstrating the reach of our software with highly visible computations.

Algebraic curves and their Jacobians. We develop algorithms and software for computing essential properties of algebraic curves for cryptology, eventually enabling their widespread cryptographic use. One of the challenges we address here is point counting. In a wider perspective, we also study the link between abelian varieties over finite fields and principally polarized abelian varieties over fields of characteristic zero, together with their endomorphism ring. In particular, we work in the direction of making this link an effective one. We are also investigating various approaches for attacking the discrete logarithm problem in Jacobians of algebraic curves.

Arithmetic. Our work relies crucially on efficient arithmetic, be it for small or large sizes. We work on improving algorithms and implementations, for computations that are relevant to our application areas.

Polynomial systems. It is rather natural with algebraic curves, and occurs also in NFS-related contexts, that many important challenges can be represented via polynomial systems, which have structural specificities. We intend to develop algorithms and tools that, when possible, take advantage of these specificities.

The first two challenges above interact with the latter two, which are also research topics in their own right. Both algorithmic and software improvements are the necessary ingredients for success. The different axes of our research form thus a coherent set of research directions, where we apply a common methodology.

We consider that the impact of our research on cryptology in general owes a lot to the publication of concrete practical results. We are strongly committed to making our algorithms available as software implementations. We thus have several long-term software development projects that are, and will remain, parts of our research activity.

7 From Vegas to Gamble

Team composition

O. Devillers (DR INRIA, team leader of Gamble), L. Dupont (MCF UL), S. Lazard (DR INRIAm team leader of Vegas), G. Moroz (CR INRIA), M. Pouget (CR INRIA), M. Teillaud (DR INRIA).

Vegas was an INRIA-LORIA project-team created in January 2005 and Gamble (Geometric Algorithms and Models: Beyond the Linear and Eucldean realm) is its follow up which we are in the process of creating.

Project

Starting in the eighties, the emerging computational geometry community has put a lot of effort to design and analyze algorithms for geometric problems. The most commonly used framework was to study the worst-case theoretical complexity of geometric problems involving linear objects (points, lines, polyhedra…) in Euclidean spaces. This so-called *classical computational geometry* has some known limitations:

- Objects: dealing with objects only defined by linear equations.
- Ambiant space: considering only Euclidean spaces.
- Complexity: worst-case complexities often do not capture realistic behaviour.
- Robustness: ignoring degeneracies and rounding errors.
- Dimension: complexities are often exponential in the dimension.

Even if these limitations have already got some attention from the community [C+99], a quick look at the flagship conference SoCG[1] proceedings shows that these topics still need a big effort.

We plan to address several of these limitations:

Non-linear computational geometry. Curved objects are ubiquitous in the world we live in. However, despite this ubiquity and decades of research in several communities, low-degree surfaces are far from being robustly and efficiently manipulated by geometric algorithms. Our work on, for instance, quadric intersections and certified drawing of planar curves has proved that dramatic improvements can be accomplished when the right mathematics and computer science are put into motion. In this direction, many problems are fundamental and solutions would have very high industrial impacts. Intersecting NURBS and meshing singular surfaces in a certified manner are important examples of such problems.

Non-Euclidean computational geometry. Triangulations are central geometric data structures in many areas of science and engineering. Traditionally, their study has been limited to the Euclidean setting. Needs for triangulations in non-Euclidean settings have emerged in many areas dealing with objects whose sizes range from the nuclear to the astrophysical scale, and both in academia and in industry. It has become timely to extend the traditional focus on $\mathbb{R}^d$ of computational geometry and encompass non-Euclidean spaces.

Probability in computational geometry. The design of efficient algorithms is driven by the analysis of their complexity. Traditionally, worst-case input and sometimes uniform distributions are considered and many results in these settings have had a great influence on the domain. Nowadays, being more subtle, in between these two extreme settings, is necessary to accomplish further progress. For instance, smooth analysis, which was introduced for the simplex algorithm and which we applied successfully to convex hulls, proves that such promising alternatives exist.

[1] Symposium on Computational Geometry. `http://www.computational-geometry.org/`.

[C+99] Bernard Chazelle et al. Application challenges to computational geometry: CG impact task force report. In B. Chazelle, J. E. Goodman, and R. Pollack, editors, *Advances in Discrete and Computational Geometry*, volume 223 of *Contemporary Mathematics*, pages 407–463. American Mathematical Society, Providence, 1999.

These three axes constitute research topics that are innovative in computational geometry. They are rather new and risky and they require various expertises in theoretical computer science and mathematics ranging from computer algebra to probability. Our approach of these problems is to aim at providing solutions that are both elegant in theory and that work in practice. This is never guaranteed but we hope to succeed in following Vegas' trademark, as noticed by the evaluators in their recent INRIA evaluation (March 2015), *"The group has established a reputation of turning problems that can be solved only in principle into problems that can actually be solved in practice."*

8 Magrit

Team composition

M.-O. Berger (DR INRIA, team leader), E. Kerrien (CR INRIA), G. Simon, F. Sur, P.-F. Villard, B. Wrobel-Dautcourt (MCF UL, the four of them).

Project

During the next five years, we will continue to be active both in classical and medical Augmented Reality (AR). Our aim is to develop reliable and effective methods that yield significant progresses in terms of ease of implementation, robustness to external conditions and capacity of handling complex environments. The maturity of tracking technologies differs depending on the need for rigid or deformable registration. In the case of rigid objects, many solutions are now available for tracking even if the robustness still needs to be improved in complex environments. Pending problems are currently more about the automation of the initialization procedure and about matching when the conditions in which the model and the current view were acquired are different. AR for deformable objects offers promising applications, especially in medical applications but tracking procedures are less mature with the additional difficulty to identify outliers in a deformable context. We believe that significant progress will emerge from the conjunction of improvements at various levels: (i) improved low level processing (noise characterization and associated inversion procedures), (ii) design of efficient statistical methods for matching and modeling and (iii) better consideration of the context to guide modeling and matching. Specifically, we plan to focus our research on the three following themes.

Matching and localization. Most existing applications cannot handle large viewpoint changes between the model and current images. Our aim is to develop scalable solutions for pose computation in large environments without constraining the users motion. Our work on the use of simulated viewpoints has proven effective in cases where traditional methods fail, thus opening the way towards challenging applications. One of our mid-term objective is now to investigate the optimal choice of virtual cameras so as to have both a good coverage of the scene and a small-size model, making pose computation amenable to near real time.

In practice, changes in atmospheric or lighting conditions as well as the presence of pedestrians, cars or street furnitures can dramatically increase the ratio of outliers in matching hypothesis, making pose computation inefficient. We believe that further improvements in camera localization will hardly be obtained without considering higher-order understanding of the scenes. Indeed, using recognition procedures to identify potentially perturbing elements in the scene, such as pedestrians and cars, may help to remove matching hypothesis in these areas. On the contrary, the possibility to recognize categories, such as building and doors, will permit to focus model/image matching hypotheses on these areas. Another idea we want to explore is to improve the description of the model in order to facilitate matching and recognition. We thus intend to investigate whether textured models could be automatically defined in terms of high-level primitives and their spatial arrangements. Globally, our goal is to establish a better cooperation between object recognition techniques and matching algorithms in order to obtain larger

inlier ratios in correspondence hypotheses, thus leading to robust and efficient pose algorithms in large scale environements.

Modeling and tracking potentially deformable objects. Mainly motivated by medical AR applications, our aim is to address the problem of 3D tracking and modeling deformable organs in an endoscopic multimodality context from images acquired pre-operatively (CT images) and intra-operatively (video, US images). Noisy intra-operative imagery, such as ultrasound, repetitive textures on the organs and large organ deformations, favor the presence of outliers and may dramatically affect the computed deformation. Designing outlier rejection schemes for deformable registration is currently a subject of high interest [PB11,TCC+12]. In the case of multimodal imagery, we intend to consider a larger combination of visual cues and improved statistical models such as A Contrario models. Another track of research is the investigation of semi-supervised procedures to identify what are important visual cues, what is the scale of the matching errors or what are the appropriate degrees of freedom of the model. We also intend to investigate how knowledge on the organs and specifically on their mechanical properties may help to constrain the matching or the segmentation procedures. In the context of heart valve surgery, we especially want to investigate how to realistically simulate patient-based mitral valve closure. Our strategy is to study segmentation methods that are (i) faithful enough to model real anatomical geometries and that are (ii) based on a biomechanical models that are appropriate enough to accurately simulate the valve behaviour.

Inverse problems and parameter estimation. Mechanical models are now widely used but they require to characterize the properties of specimen under study. Contactless methods are obviously highly desirable and we describe here our objectives in terms of image-based characterization of mechanical properties in the continuity of our collaborations on experimental mechanics and in the medical context.

Concerning experimental solid mechanics, our research prospects are in the field of image restoration. We are interested in displacement and strain field measurements which come with a very low signal-to-noise ratio, these fields being impaired by a signal-dependent spatially correlated noise. We intend to investigate super-resolution and denoising in this context. The challenge consists in quantifying the metrological performances, the resolution being mainly limited by noise, together with the measurements. In this context, it is not possible to use off-the-shelf methods from the image processing literature. Dedicated approaches, supported by a careful modeling of image noise and a thorough analysis of the measurement method, are needed.

In the context of interventional neuradiology, we want to further investigate Image-Driven Simulation. The long-term objective is to offer the physicians a dynamic 3D depiction of the surgical field in real time during the operation. The potential of data fusion methods will be investigated in order to maintain a simulation of the blood vessels and the interventional tools (e.g. micro catheters, micro guides, coils) in accordance with the live fluoroscopy X-ray images taken during the operation.

[PB11] Daniel Pizarro and Adrien Bartoli. Feature-based deformable surface detection with self-occlusion reasoning. *International Journal of Computer Vision*, 97(1):54–70, 2011.

[TCC+12] Quoc-Huy Tran, Tat-Jun Chin, Gustavo Carneiro, Michael S. Brown, and David Suter. In *ECCV 2012*, pages 274–287, 2012.

Report integrators: Éric Domenjoud (Team ADAGIo) and Philippe Dosch (Team QGAR). Report designed under Linux using Emacs, and formated thanks to XeLaTeX.