2012 Project Proposal (Research – Innovation)

Basic Form

This form, and the associated CVs, must be filled in English. Before filling the form, please read carefully the bases published in the STIC-AmSud site (www.sticamsud.org).

This form must be sent by email to the STIC-AmSud Secretariat (sticamsud@conicyt.cl) by the project's International Coordinator.

A. General Information

A1. Project Title

Advances in Analytic Combinatorics: dynamical combinatorics, and applications to number theory, information theory and cryptography.

A2. Acronym DYNALCO

A3. Research Domain:

Mathematical Informatics – Probabilistic analysis of algorithms – Analytic Combinatorics – Dynamical Systems – Computational Number theory – Information Theory – Cryptography

A4. Project goals.

This project is jointly conducted by two teams based in South America (Montevideo and Buenos-Aires) and one team based in France (inside the GREYC Laboratory at the University of Caen). This bi-disciplinary project gathers mathematicians and computer scientists. There are already strong connections between some members of the project, and one of our main motivations to propose this project is to strength and develop these relations,

We also wish to establish this subject in a stronger way in South America, and in good relation with already existing structures (the French-Argentinean LIA Laboratory INFINIS in Buenos-Aires and the French-Uruguayan IFUM Laboratory). This project lies inside the domain of «Mathematical Informatics» and can be a step forward in the development of this theme in South America. It can inherit from the French experience on the subject, since the French team plays an important rôle in the Groupe de Recherches en Informatique Mathématique

There is also an important number of students in the project (an initial number equal to six, two in each team). As a consequence, we also propose to organize a mini-school, mostly oriented to graduate students in the South American region.

A5. Abstract

Probabilistic analysis of algorithms aims at describing the behavior of an algorithm (or its

underlying data structure) on a generic input. Analytic combinatorics is one the main methods which makes possible such an analysis. A unified treatment of this theory, as well as most of its methodological foundations has been proposed by Flajolet. The present project aims at achieving four main goals that may provide meaningful advances in the important domain of Analytic Combinatorics and its applications.

We wish to continue the development of a new methodology Dynamical Combinatorics, which mixes the general methods of Analytic Combinatorics with other methods that come from Dynamical Systems Theory

We aim at studying important problems in three main domains of computational mathematics and theoretical computer science, Algorithmic number theory, information theory and cryptography. We will mainly use Analytic Combinatorics methodology, and very often specific methods of Dynamical Combinatorics.

A.6. Scientific coordinators at each institution

South America A

Institution:	National University of General Sarmiento.
Project Coordinator:	Eda Cesaratto
Adress	National University of General Sarmiento.
	Instituto del Desarrollo Humano– J. M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Bs. As, Arg.
Phone/Fax	+54 11 44 69 77 24
Email	ecesarat@ungs.edu.ar

South America B

Institution:	Universidad de la República
Project Coordinator:	Alfredo Viola
Adress	Julio Herrera y Reissig 565 Montevideo
	URUGUAY CP 11300
Phone/Fax	+ (598) 27114244 X127
Email	viola@fing.edu.uy

France A

Institution:	Centre National de la Recherche Scientifique
	Université de Caen Basse Normandie
Project Coordinator:	Brigitte Vallée
Adress	Laboratoire GREYC (UMR 6072), Campus Côte de Nacre, Boulevard du Maréchal Juin, BP 5186 - 14032 Caen CEDEX
Phone/Fax	FAX: +33 (0)2 31 56 73 30 - Telephone: +33 (0)2 31 56 74 81
Email	brigitte.vallee@info.unicaen.fr

A.7. French Associate laboratories: LIAFA (Paris) and LMNO (Caen)

A.8. List of expected participants (name and affiliation)

UdelaR team:

Coordinator: Alfredo Viola

PhD Students: Nicolás Carrasco – Fernando Fernández

UNGS team:

Coordinator: Eda Cesaratto

Members: Antonio Cafure – Guillermo Matera

Phd Students: Melina Privitelli, Mariana Pérez.

GREYC team:

Coordinator: Brigitte Vallée

Members: Julien Clément – Jean-Marie Le Bars – Loïck Lhote

Associate members: Valérie Berthé (LIAFA, Paris) – Valérie Girardin (LMNO, Caen)

PhD Students: Hun Kanal – Thu Hien Nguyen Thi

A.9. International Project Coordinator

(to be chosen among the Scientific Coordinators mentioned in A6):

Eda Cesaratto (UNGS)

B. Project Details

Introduction: Project guidelines

The domain which is called probabilistic analysis of algorithms was created by Knuth (see [Knuth97]) during the seventies. It aims at describing the behavior of an algorithm (or its underlying data structure) on a generic input. One first defines a probability measure on the set of inputs, and considers the cost function of interest as a random variable (the number of steps of the algorithm, the shape of the output configuration, the path length of an underlying tree that models the studied algorithm, etc.). The final goal aims to estimate its mean value, its variance and, more generally its distribution (if possible), when the input data become large enough.

Analytic combinatorics is one the main methods which makes possible such an analysis. A unified treatment of this theory, as well as most of its methodological foundations has been proposed by Flajolet, and is well described in the book of Flajolet and Sedgewick in [FlaSed09].

In this setting, the present project aims at achieving four main goals that may provide meaningful advances in the important domain of Analytic Combinatorics and its applications:

(A) We wish to continue the development of a new methodology

Dynamical Combinatorics,

also often called Dynamical Analysis of Algorithms, which mixes the general methods of Analytic Combinatorics with other methods that come from Dynamical Systems Theory.

(B) We aim at studying important problems in three main domains of computational mathematics and theoretical computer science,

Computational number theory, information theory and cryptography.

We will mainly use Analytic Combinatorics methodology, and very often specific methods of Dynamical Combinatorics.

(C) This project is jointly conducted by two teams based in South America (Montevideo and Buenos-Aires) and one team based in France (inside the GREYC Laboratory at the University of Caen). This is also a bi-disciplinary project, since these teams gather mathematicians and computer scientists. There are already strong connections between some members of the project, and the graph of shared subjects has already many edges. One of our main motivations to propose this project is to strengthen and develop these relations, in order to obtain an almost complete graph of sharing collaborations.

(D) We also wish to establish this subject in a stronger way in South America, and this project may be a first step towards the development of a systematic regional collaboration in the area of Analytic Combinatorics. This project also gathers teams in Mathematics and Computer Science and lies inside the broader domain of «Mathematical Informatics». This may take a step forward in the development of a regional network in "Mathematical Informatics", in good relation with already existing structures (the French-Argentinean LIA Laboratory INFINIS in Buenos-Aires and the French-Uruguayan IFUM Laboratory). In this sense, we may inherit from the French experience on the subject, since the French team plays an important rôle in the Groupe de Recherches en Informatique Mathématique (GdR IM).

(E) There is also an important number of students in the project (an initial number equal to six, two in each team). As a consequence, we also propose to organize a mini-school, mostly oriented to graduate students in the South American Region.

General project description

6.5. General organisation of the project.

6.6. Intensive school on the scientific themes of the project.

6.7. Towards a South-American network in Mathematical Informatics?

6.8. Curriculum Vitae of participants

0- Context of the Project: Analytic Combinatorics.

We describe here the context of the project, which lies inside the general domain of Analytic Combinatorics. We then explain the main original features of our scientific project, with its main four themes.

The domain of **Analytic Combinatorics** can be described as follows (see [Obi]) «Analytic combinatorics is a modern basis for the quantitative study of combinatorial structures (such as words, trees, mappings, and graphs), with applications to probabilistic study of algorithms that are based on these structures. It also strongly influences other scientific domains, such as statistical physics, computational biology, and information theory. With deep historic roots in classical analysis, the basis of the field lies in the work of Knuth, who put the study of algorithms on a firm scientific basis starting in the late 1960s with his classic series of books. Flajolet's work takes the field forward by introducing original approaches in combinatorics based on two types of methods: symbolic and analytic.

The symbolic side is based on the automation of decision procedures in combinatorial enumeration to derive characterizations of generating functions. The analytic side treats those functions as functions in the complex plane and leads to precise characterization of limit distributions. In the last few years, Flajolet was further extending and generalizing this theory into a meeting point between information theory, probability theory and dynamical systems. »

In this general setting, the present project aims at achieving four main goals that may provide meaningful advances in the important domain of Analytic Combinatorics and its applications. These goals are described in the following Sections.

Theme 1. Dynamical Combinatorics (see Section 1) We wish to continue the development of a new methodology: "Dynamical Combinatorics", also often called "Dynamical Analysis of Algorithms", which mixes the general methods of Analytic Combinatorics with other methods that come from Dynamical Systems Theory.

We then aim at studying important problems in three main domains of computational mathematics and theoretical computer science, Computational number theory, information theory and cryptography. We will mainly use Analytic Combinatorics methodology, and very often specific methods of Dynamical Combinatorics.

Theme 2. Analytic Combinatorics and Computational Number Theory. (see Section 2) There are two basic objects in number theory: (integer) numbers and (univariate) polynomials over finite fields, with a strong parallelism between the two. However, the methods and the general culture of the two related domains may be very different. These two sides are represented in the project (in fact, already inside the GIGA team, which constitute a main strength. The subjects described in 2.1, 2.2, 2.3 belong to the first side, the subjects of 2.4 and 2.5 to the second side. Even if the analysis point of view is shared by all the members of the project, the methods can vary a lot from one side to the other. The polynomial case can often be dealt with Analytical Combinatorics or direct counting methods in Algebraic geometry, while the number case analyses are often performed by the members with Dynamical Combinatorics methods.

With respect to the domain of Analytical or Dynamical Combinatorics, there are two general "opening" domains: Is is possible to design specific methods (of AC type) to deal with analyses in algebraic geometry (see 2.4 and 2.5)? How to mix methods of DC with methods brought by symbolic dynamics (see 2.3) ?

Theme 3. Analytic Combinatorics and Information Theory. (see Section 3) This theme studies the concept of a general source (with various points of view, both probabilistic and dynamical, see 3.4), and uses this modelisation in the analyses of two data structures (trie in 3.1, digital search tree in 3.2) built on words emitted by such sources, or realistic analyses of searching and sorting algorithms (see 3.3), when they are viewed as text algorithms.

T**heme 4. Analytic combinatorics and Cryptography.** (See Section 4) Except in the domain of boolean functions, the members of our team are not specialists in any precise area of cryptography or error-correcting codes. Nevertheless, they are interested to domains (number theory, and information theory) that provide meaningful tools to cryptography (see 4.1). Using methods from AC in the combinatorial study of boolean functions is one of the expertise domain of the project.

1 - Dynamical Combinatorics (also called Dynamical Analysis)

Scientific coordinator: Brigitte Vallée (GREYC)

Participants: Eda Cesaratto (UNGS), Loïck Lhote, Brigitte Vallée (GREYC)

Abstract. This is a new methodology which lies inside the general methodology of Analytic Combinatorics. Dynamical Combinatorics (or DC) is an extension of Analytic Combinatorics (AC) which extends the main principles of AC when the process (the algorithm or the source of input data, for instance) can be viewed as a dynamical system.

1.1. Informal description of Dynamical Combinatorics.

Analytic Combinatorics is a set of deep and strong methods (both combinatorial and analytic) which are not adapted when the algorithm or the source (in the sense of information theory) are too « correlated » ; this happens when the process (for instance, the behaviour of the algorithm or the source) at one step depends on the whole previous history. In this case, the process is no longer decomposable, and it is no longer possible to use the « combinatorial dictionary » to obtain an alternative expression of generating functions from which the nature and the position of their singularities can be derived. Dynamical Combinatorics (or DC) is an extension of Analytic Combinatorics which extends the main principles of AC when the process (the algorithm or the source, for instance) can be viewed as a dynamical system.

DC was introduced at the end of the nineties by Brigitte Vallée (see for instance [Val06,Val01]). She aimed at extending ideas which appeared in almost all of her previous joint works with Philippe Flajolet [DauFlaVal97, FlaVal98, FlaVal00]. They mainly dealt with continued fraction algorithms, but she remarked that most of the main principles they used could be extended to a complete class of Euclidean algorithms, and an important class of sources of information theory. When these processes are viewed as dynamical systems, it is then possible to use all the tools of the dynamical systems theory, and, amongst them, a central object : the transfer operator. In DC, the transfer operator plays the rôle of a generating operator, since it generates itself generating functions, that are here of Dirichlet type. In this context, the asymptotic analysis would be closely related to the dominant eigenvalue of the transfer operator.

In DC as well in Analytic combinatorics (AC), there are two main steps: The combinatorial step deals with the transfer operator, and views it as a generating operator,

which generates itself the generating functions of interest (that are of Dirichlet type, and depend on a complex parameter, say s). The analytic step deals with the geometry of the dynamical system, translates it into spectral properties of the transfer operator, then into analytical properties for the generating functions. The dominant eigenvalue of the operator plays there the same rôle as the dominant singularity in « classical » analytic combinatorics. (see [Val06,Val01] for a general survey of the methodology).

1.2. From average-case analysis towards distributional analysis.

When first proposed, DC dealt with average-case analysis of algorithms [Val98b,Val03]. In this case, it is sufficient to study the generating functions, and then the transfer operator when their main parameter s has its real part larger than 1; the method succeeds as soon as the dynamical system is Markov and expanding, since it is possible to prove in this case good spectral properties of the transfer operator (a dominant eigenvalue and a spectral gap).

However, for distributional results, one needs to study the generating functions and the transfer operator on larger domains, when the real part of the parameter s may be smaller than 1. Then, Baladi and Vallée introduced Dolgopyat's work [Dol98, Dol00] into the DC domain and adapted it in [BaVal05a] and [BaVal05b]. Dolgopyat provides sufficient conditions (the UNI conditions) on the dynamical system that entail a good behaviour of the transfer operator for Re(s) smaller than 1. Then, Baladi and Vallée in [BaVal05a] exhibited various asymptotic gaussian laws in the context of DC. Later, the tools and techniques introduced in those works gave the machinery for obtaining other distributional results or to refining error terms. This has been done for instance by Lhote and Vallée [LhoVal], Cesaratto and Vallée in [CesVal11] or by Roux and Vallée [RoVal11].

1.3. Main domains of application.

As was previously said, Dynamical Combinatorics was first introduced and used in the context of continued fraction expansion and gcd algorithms in various joint works of Flajolet and Vallée [DauFlaVal97, FlaVal, FlaVal]. Then, the method was fully extended in two domains. In Computational Number Theory, it was applied to any dynamical system of Euclidean type. In Information Theory, it led to the concept of dynamical sources [Val01], where encoded trajectories of the dynamical system are viewed as words, and define the source. In the last context, the Dirichlet generating function Lambda(s) of the source plays a fundamental role, and can be expressed with an extension of the transfer operator of the underlying dynamical system. Dynamical sources provide a nice extension of classical sources (memoryless sources or Markov chains); the class is large enough to model sources with a high degree of correlation, but also precise enough to be analyzed using analytic tools.

Finally, Dynamical Combinatorics is quite powerful in some specific areas of Computational Number Theory and Information Theory. More specifically, it has contributed to solve the following problems:

In Computational Number Theory
-- Analysis of the Gauss algorithm for lattice reduction [DauFlaVal97]
-- Precise analysis of the continued fraction expansion [FlaVal9!, FlaVal00]
– Precise analysis of an efficient GCD based on a Divide and Conquer Principle [CesCleDaiLhoMauVal09]
-- Study of « constrained » numbers (a constrained number obeys some constraints on the digits of its continued fraction expansion)
-- counting « constrained » rational numbers [CesVal11]
-- Estimates of the Hausdorff dimension of « constrained » real numbers [Val98, CesVal06]
--Analysis of the randomness of Kronecker sequences [CesPlagVal06, CesVal12]

In Information Theory

-- Analysis of parameters of trie structure [CleFlajVal01], [CesVal11b]
-- Analysis of sorting algorithms [ValCleFlajFill09]

1.4. Specific projects of the team : Distributional analyses of periodic trajectories.

Previous distributional results deal with particular trajectories of the Euclid dynamical system, namely rational trajectories which attain 0 in a finite number of steps. The interest in these particular trajectories arises in a natural way since they are related to executions of the Euclid Algorithm. The previous results [BaVa05a] can be described in an informal way by the following (informal) sentence : « these particular rational trajectories behave as generic real trajectories ».

In dynamical systems theory, there exist other particular trajectories, which are well studied by the researchers of the domain : the periodic trajectories. In the continued fraction case, they are related to irrational quadratic numbers. This class of trajectories was already studied in the average case in [Val98]. On the other hand, important results exist about the distributional analysis of periodic trajectories of a general dynamical system [PolSharp98], at least when it has a finite number of branches, since it is possible to use in this case the already mentioned results of Dolgopyat [Dol98], [Dol00]

For an infinite number of branches, the analysis is much more difficult : even if the results of Dolgopyat are now extended to this case in [BaVal05a] and [BaVal05b], a further extension is needed, and a recent (yet unpublished) work of Vallée [Val12b] explains the main principles to get this extension. Cesaratto and Vallée wish to obtain a complete distributional analysis of « weighted » periodic trajectories. In particular, Gaussian laws can be expected, for a class of moderate weights. Cesaratto and Vallée are also interested in obtaining local limit laws in the same spirit as those obtained by Vallée for rational trajectories [Val12a]. This also could be applied in a specific way to irrational quadratic numbers (see 2.2)

2 - Analytic Combinatorics and Computational Number Theory

Scientific coordinator: Eda Cesaratto (UNGS)

Participants. Antonio Cafure, Eda Cesaratto, Guillermo Matera, Mariana Pérez, Melina Privitelli (UNGS), Alfredo Viola (UdelaR), Loïck Lhote, Brigitte Vallée (GREYC), Valérie Berthé (LIAFA, Paris)

Abstract. There are two basic objects in number theory: (integer) numbers and (univariate) polynomials over finite fields, with a strong parallelism between the two. However, the methods and the general culture of the two related domains may be very different. These two sides are represented in the project (in fact, already inside the GIGA team), and this is a great strength. The subjects described in 2.1, 2.2, 2.3 belong to the first side, the subjects of 2.4 and 2.5 to the second side. Even if the analysis point of view is shared by all the members of the project, the methods can vary a lot from one side to the other. The polynomial case can be often dealt with Analytical Combinatorics or direct counting methods in Algebraic geometry, while the number case analyses are often performed by the members with Dynamical Combinatorics methods.
With respect to the domain of Analytical or Dynamical Combinatorics, there are two general "opening" domains: Is is possible to design specific methods (of AC type) to deal with analyses in algebraic geometry (see 2.4 and 2.5)? How to mix methods of DC with methods brought by symbolic dynamics (see 2.3) ?

2.1. Randomness of Kronecker sequences

State of the art. According to Franklin and Knuth [Knuth65] « a sequence is random if it has every property that is shared by all infinite sequences of independent samples of random variable from the uniform distribution ». Cryptographic applications require the generation of random sequences, but they are « difficult » to produce.

Pseudo-random generators are efficient deterministic processes that generate sequences that appear to be random with respect to one or several measures of randomness. These kinds of measures give quantitative information about the difference between a random sequence and a non-random one. The discrepancy is a very popular measure of randomness, widely studied; but there is of course many other ones, and very recently, Arnold introduces another measure, much less studied, which will be called in the following the Arnold Constant.

The Kronecker sequence S(a) is associated to a real a and gathers the fractional parts of the multiples of a. When a is a rational u/v, such a sequence is closely related to the modular arithmetic progression of the form $x(i)=x(i-1)+u \pmod{v}$ which is the simplest case of the widely used Linear Congruential Generator.

Previous results obtained by the team. Cesaratto and Vallée adopted in [CesPlagVal06] and [CesVal12] original points of views in the domain, and they performed a probabilistic study of the pseudo-randomness of the Kronecker sequences : they precisely estimated « on the average » the discrepancy and the Arnold constant of a random Kronecker sequence S(a), in two cases : the number a is a random real or the number a is a random rational among those rationals with denominator less than a fixed number N.

Specific project of the team. Works due to Schoissengeier or Behnke [Beh1, Beh2, Scho1, Scho2] show that the behavior of the discrepancy of S(a) strongly depends on the average of the digits which appear in the continued fraction expansion of a. It is then interesting to perform the same study as previously (mean values of the discrepancy and Arnold constants) but restricted to inputs a (rational or real) for which the sequence of digits admits bounded averages. Cesaratto and Vallée previously dealt with these constrained probabilistic models,

both in the real and rational case [Val98, CesVal06, CesVal11], and use dynamical combinatorics methodology. The team wishes to use these previous studies to describe the randomness of random Kronecker sequences S(a) in this « constrained » framework. In fact, inside this constrained framework, there is a super-constrained case, when all the digits in its continued fraction expansion are bounded by the same bound M. In this case, Cesaratto and Vallée have already obtained precise results which provide a probabilistic version of results by Schoissengeier or Behnke.

2.2. Quadratic numbers.

State of the art. Irrational quadratic numbers have always attracted mathematicians and theoretical computer scientists. In an informal way, these are the irrational numbers that are the most different from rational numbers, in the sense that they are very badly approximated by rationals. In particular, previous works showed that the Kronecker sequences associated to quadratic irrationals possess, in some precise sense, the largest quantity of randomness (see [Beck09] for a summary of results).

Specific project of the team. In Section 1.4, we have described our general interest in distributional results about periodic trajectories of a general dynamical system. In the particular case of the continued fraction source, periodic trajectories are those of quadratic irrational numbers. Then, it will be possible to consider the present study as a particular case of the study performed in Section 1. But we are also interested here in this specific case, and to its consequences on the probabilistic behaviour of Kronecker sequences S(a) associated a random quadratic irrational. And, as we explained in Section 2.1, it would be interesting to also study the restricted case of a random quadratic irrational whose all digits in its continued fraction expansion are bounded by a fixed integer M.

2.3. Continued Fraction Algorithms in higher dimensions.

There does not exist a unique "natural" generalization of continued fraction expansion in higher dimensions. But there are various possible approaches that encompass both traditional algorithms for multidimensional continued fraction expansion (e.g., Jacobi-Perron, Brun, Ostrowski...), classical algorithms for calculating the gcd of several integers and lattice reduction algorithms (such as the celebrated LLL algorithm), or stronger algorithms (such as the algorithm called BKZ); see [HS99], [Sch00] and the references in [NgVa10]. These algorithms play an important rôle in discrete geometry, or in cryptography, for instance (See Section 4).

Dynamical Combinatorics has proved its efficiency in the analyses of continued fraction expansion algorithms in small dimensions. However, the analysis of multidimensional continued fractions appears to be much more intricate.

Specific projects of the team. They are of three types:

a) We first wish to extend the main general principles of Dynamical Combinatorics to the analysis of dynamical systems in higher dimensions. Previously, the underlying dynamical systems of interest were always one-dimensional. The evolution of a dynamical system is of course much more complex in higher dimensions. We restrict ourselves to simple geometries (of Markovian type) and wish to describe sufficient conditions on the branches of the system under which the DC methods can be applied. In particular, it would be interesting and useful to obtain an analog of the UNI Condition which is crucial in previous analyses.

b) There exist various strategies for computing the gcd of d (d>2) positive integers (Brun, Jacobi-Perron or Knuth). They give rise to various strategies for computing a multidimensional continued fraction expansion of d-1 rationals. It is then important to analyze these various strategies and compare their efficiency. In a work in progress, the team

deals with the algorithm of Brun and already obtained first results in its analysis (yet unpublished, see [BerLhoVal12]). We wish to extend our analysis to other strategies.

c) The probabilistic behavior of lattice reduction algorithms is not well understood, and their dynamics in high dimensions appears to be very intricate. It is then not realistic to hope using directly the Dynamical Combinatorics method. This is why Madritsch and Vallée in [MaVa10] have designed and analyzed a simplified model for the LLL algorithm using sandpiles (a class of simple discrete dynamical systems, very well studied). Recently, the authors of [HPS11] have analyzed a simplified model of the BKZ lattice reduction algorithm, also related to sandpiles. In her thesis [Geor12], prepared in the GREYC laboratory (Caen), Mariya Georgieva proposed a more realistic model (less simplified, but probably yet manageable) which leads to a general dynamical system (no longer a sandpile). We begin to study the case of three dimensions, which gives rise to a two-dimensional dynamical system, and we have obtained preliminary results on the subject [Geor12]. We wish to extend this approach to general dimensions.

2.4. Computing rationals points of algebraic varieties defined over finite fields.

Presentation of the domain. It is very important, in particular for potential cryptographic applications, to find in an efficient way rational points in algebraic varieties over finite fields. This problem is equivalent to solving polynomial systems over the finite field F_q. The GIGA group in Buenos Aires aims at developing efficient (symbolic or numeric) algorithms for solving polynomial systems. One of the main interests of the group is the analysis of these algorithms from a probabilistic point of view. Then, the group was led to solve related combinatorial problems. In [CaMa06a], the group provides estimates for the number of rational points in a generic irreducible variety, and, in [CesMaGat11], it evaluates the number of irreducible algebraic curves and the mean number of points of an algebraic curve in the projective space F_q .(see also 2.5)

Most of the algorithms which solve polynomial systems are typically designed to compute all the solutions of the system, whereas only some selected solutions are often needed. Consequently, GIGA concentrates on algorithms for computing only selected solutions, which are often more efficient. In the papers [CaMa06b] and [Mat10], Cafure and Matera proposed algorithms which can be applied to varieties that possess certain particular geometric properties. They also designed new versions of algorithms based on the strategy called « Search on Vertical Strips » (SVS). This type of strategy was introduced in [GaShpSin03] into the domain of curves and the group has adapted it to the case of hypersurfaces.

In the particular case of algorithms designed to find rational points on hypersurfaces with this strategy, the problem is: Given a polynomial $R(X_1, X_2, .. X_r)$ with r variables and coefficients in the finite field F_q of q elements, find a vector $x =(x_1, x_2, \ldots, x_r)$ in F_q^r such that $R(x_1, x_2, \ldots, x_r)= 0$. The algorithm enumerates all the points a with $r-1$ coordinates in F_q, and, for each point a, it evaluates the polynomial R at each point a and tries to find a root in F_q of the univariate polynomial $R(a,X_r)$. The main question is of probabilistic type : How many evaluations are needed to find a root of the polynomial $R(X_1, X_2, .. X_r) = 0$? The main parameters are the degree d, the number r of variables, and the number s of points.

A (yet unpublished) work of the GIGA team [Cafure et al.12] already performed a probabilistic study of the previous algorithm and proved the following : Consider a random polynomial $R(X)$ of degree at most d in r variables. Then, the probability that the algorithm finds a root of $R(X)$ in the first evaluation equals the probability that a random univariate polynomial of degree at most d has a root. The latter probability is (asymptotically in d), equal to $1-(1/e)$ (where e is the standard basis for the logarithm). This result shows that the algorithm stops at the first step with high probability.

Specific projects of the team. Our objective is to completely understand the behavior of this type of algorithms, and we wish to estimate the probability that the algorithm performs s steps (when the cardinality q becomes large). This leads to the following combinatorial problem, depending in the triple *(d, s, q)*: Given s elements of F_q, determine the number of univariate polynomials of degree $d < q$ with s coefficients fixed which have a root in F_q.

Even if this combinatorial problem remains open in its whole generality, there already exist two cases where the problem is solved. A paper due to Knopmacher and Knopmacher [KnopKnop90] solves the problem when d greater or equal to q and uses tools from Analytic Combinatorics. Another paper, due to Uchiyama [Uchi55], deals with exponential sums and provides such a result when q is prime, with an error term which is reasonably small when s is less than the square root of d.

Our team wishes to adapt methods from Algebraic Geometry that it has already used in the paper [CaMaPri12] to obtain results when s is less than $d/3$. It is our hope that the collaboration between all the partners helps to solve this combinatorial problem for all cases under analysis.

2.5. Polynomials over F_q.

In a work in progress [BerNakNatVal12], Berthé and Vallée returned to the precise analysis of the Euclid Algorithm, when it deals with polynomials of *F_q[X].* The polynomial case (*F_q[X])* is always easier than the integer case (Z), and the complete analysis of the polynomial Euclid algorithm can be completely performed inside the framework of Analytic Combinatorics: with the AC methods, Lhote and Vallée in [LhoVa08l obtained an asymptotic Gaussian law for the bit complexity of the polynomial gcd algorithm. The paper (in progress, yet unpublished) performs a more precise analysis of the bit complexity, since it is not based on the degree of polynomials, but on the number of monomials which actually appear. Some other refinements on the distributional analysis of the polynomial Euclid algorithm can be dealt with, and this would be important inside the present project, since this subject mixes an object of interest for the GIGA group and methods of Analytic Combinatorics.

A well-known result of Gauss describes the density of irreducible univariate polynomials over *F_q*, and "most" polynomials are reducible. The latter changes drastically for two and more variables, where "most" polynomials are irreducible. The paper [CesMaGat11] provides estimates for the number of reducible curves over a finite field, for dimension *r>2.* It shows that for curves of degree *d* in the projective space *P^r,* there is a threshold *d_0(r)=4r-8*: For *d > d_0(r)*, most curves are irreducible, and for *d < d_0(r),* most are reducible. All the estimates are explicit, without unspecified constants.

3 - Analytic Combinatorics and Information Theory

Scientific coordinator: Julien Clément (GREYC)

Participants : Eda Cesaratto (UNGS), Alfredo Viola (UdelaR), Julien Clément, Loick Lhote, Brigitte Vallée, Thu Hien Nguyen Thi, Kanal Hun (GREYC), Valérie Girardin (LMNO, Caen)

Abstract. This theme studies the concept of a general source (with various points of view, both probabilistic and dynamical, see 3.4), and uses this modelisation in the analyses of two data structures (trie in 3.1, digital search tree in 3.2) built on words emitted by such sources, or realistic analyses of searching and sorting algorithms (see 3.3), when they are viewed as text algorithms.

3.1. The trie structure. There is a tree structure which implements dictionaries in a very efficient way. In [CleFlajVal01], Clément and Vallée have analysed, together with Philippe Flajolet, the main parameters of a trie when it is built on words produced by a general

(dynamical) source. The main results of the paper refer to the typical depth and the height of a trie built on *n* words of the source; The authors mainly deal with the transfer operator of the source, the generating function of the source and obtain asymptotic estimates for the mean values of the typical depth and the height, which respectively involve the entropy and the coincidence of the source.
Then, ten years later, in [CesVal11b] (a paper under submission), Cesaratto and Vallée returned to this study, and exhibited an asymptotic gaussian law for the typical depth of the trie built on a general source, as soon as the generating function Lambda(s) is "tame" on the left of the vertical line *Re(s)* = 1. This is the case when the source is a dynamical source which satisfies the UNI Conditions. It may be important to obtain an extension of the result in the case when the source satisfies other conditions, the so-called DIOP Conditions (see [RoVa11]).

3.2. Digital Search Tree. In March 2010, Flajolet and Vallée decided to study another important data structure, the digital search tree (intermediary between the Trie and the BST, when it is built on words emitted by a general source. This data structure is central in compression algorithms, and had already given rise to many analyses for « classical » sources (See the book [Szp] for instance). Kanal Hun has begun to work on this subject for his PhD thesis, in January 2012.

3.3. Towards a realistic analysis of sorting and searching algorithms. Robert Sedgewick had already remarked (around 1990) that classical sorting and searching algorithms (as QuickSort and QuickSelect) were not analyzed in a realistic way, since the cost of a comparison between two keys is always assumed to be equal to 1, even in contexts where the keys may have a complex structure. He proposed to take into account the structure of keys, and to consider the total number of bits to be compared. This would provide a unified framework which gathers all the sorting algorithms, and makes possible the comparison between the Trie structure and the BST (Binary Search Tree) structure, for instance. Around 2005 in [FJ], Fill and Janson analysed QuickSort in the case when the keys are uniform real numbers of the unit interval written in binary.

First analyses. In the paper [ValCleFlajFill09] (a joint work of Clément and Vallée with Flajolet and Fill), the authors have further revisited classical sorting and searching algorithms when the keys are viewed as words, emitted by a general source, which are compared via their symbols in a lexicographical way. The cost of interest is now the total number of symbol comparisons which are needed to sort a set of n words, and the authors studied the algorithms QuickSort and QuickSelect, under a double realistic point of view (a realistic comparison between words produced by a realistic general source). In fact, they design a general framework for the analysis of any sorting or searching algorithm (performing only comparisons and exchanges), and they prove that the (realistic) efficiency of such an algorithm is based on two independent characteristics: The coincidence gamma only depends on the source and measures the similarity of the words produced and then the difficulty of their comparisons, whereas the density phi only depends on the algorithm and measures the "intelligence'' of its strategy. And, they exhibit a mixed Dirichlet series which mainly involves the product (gamma . phi), from which the mean number of symbol comparisons can be easily evaluated.

Specific project of the team. Clément and Vallée are convinced that this double realistic point of view (a realistic comparison between words produced by a completely general source) may be very fruitful, and they plan to revisit most of classical algorithms (sorting and searching) with this point of view. They supervise together the PhD thesis of Thu Hien Nguyen Thi, devoted to this subject, which began in September 2010.

3.4. General Sources.

A dynamical point of view on general sources. During the previous work [ValCleFlajFill09],

the present team (Clément, Vallée), together with Flajolet adopted a « dynamical point of view » on a general source, and proved that any general source admits a « good » parametrization by the unit interval, i.e., there exists a mapping M such that any word of the source can be written as $M(x)$ for some x in [0, 1]. This parametrization extends the natural parametrization that holds for a general dynamical source. The team wishes to understand in a deeper way this point of view, which appears to be very fruitful for a better understanding both in information theory and analysis of text algorithms.

Various notions of entropy. There exist various entropy rates; the most classical ones are due to Shannon or Rényi, but there are also various alternative notions due to Tsallis, Sharma-Mittal and many others. In [CiuGirLho11], the authors have computed and estimated generalized entropy rates for general sources (including regular countable Markov chains). They prove that generalized entropy rates are either zero or infinite out of a threshold at which they are equal to the Rényi or Shannon entropy rates. This situation is due to an inadequate normalization in the definition of the entropy rates and can be corrected through a convenient rescaling. It will be of interest, first to study the rescaled generalized entropy rates for general sources; then to extend the results to the relative entropy rates.

Approximation of general sources. The approximation of general sources by simple ones -- such as Markov chains -- is an important issue in algorithmics in general and in particular in analysis of text algorithms. Various notions of convergence of random processes exist in probability theory. They may be used for defining fruitful notions of approximation of sources. Once these notions will be properly defined, the group aims at studying the links between the fundamental parameters (entropy, invariant measures, generating function Lambda(s)...) of the simple sources and the fundamental parameters of the general ones.

4 - Analytic Combinatorics and cryptography

Scientific coordinator: Alfredo Viola (UdelaR)

Participants : Alfredo Viola, Nicolás Carrasco, Fernando Fernández (UdelaR), Team of UNGS, Julien Clément, Jean-Marie Le Bars, Loïck Lhote, Brigitte Vallée (GREYC).

Abstract. Except in the domain of boolean functions, the members of our team are not specialists in any precise area of cryptography or error-correcting codes. But they are interested to domains (number theory, and information theory) that provide meaningful tools to cryptography (see 4.1). Using methods from AC in the combinatorial study of Boolean functions is one of the expertise domain of the project.

4.1. Various applications of Number Theory and Information Theory. All the subjects described in Sections 2 have both motivations and consequences in cryptography. Pseudo-random generators, rational points on algebraic curves, lattice reduction algorithms or polynomials over finite fields are central objects in cryptography and error correcting-codes, while information theory and the notion of source are basic concepts for the domain. Presently, most of our team members know well cryptography, (they often teach it), they are aware of the deep connections their scientific results may have in cryptography. At the occasion of schools or plenary meetings, the members of the project wish to better understand these close links.

4.2. Boolean Functions.

Description of the domain. Symmetric cryptosystems like DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are widely used in cryptography because of their

efficiency. Compared to public-key cryptography, they lead to faster implementation both in hardware and software, and their key size is shorter for the same level of security. The Vernam cryptosystem is the only one cryptosystem that has been proved to achieve unconditional security [Shannon49], but it could not be used due two main drawbacks: the size of the private key must be the same as the size of the plain text to encrypt), and it needs a source of "true random" bits. Since the generation of random numbers by physical processes or coin tosses is time consuming, one replaces true randomness by pseudo-randomness, and uses Linear Feedback Shift Registers (LFSR) as a basis of this pseudo-randomness.

However, LFSR's present strong cryptographic weaknesses, due to their linear properties. Then, Boolean functions are often used to eliminate this linearity and increase the cryptographic security. Boolean functions and vectorial Boolean functions are extensively used in cryptographic applications and there is a rich literature on this issue. Carlet in [Carlet12a] and [Carlet12b] presents extensive surveys on the area, with a very long set of references. In the generic example, Boolean functions are used to combine several LFSR's, but there may be also a single register filtered by a Boolean function [Siege85]. These Boolean functions need to fulfill important properties to resist several types of attacks. For example, to avoid attacks using Berlekamp Massey algorithm [Massey69], they must have high algebraic degree and to avoid Siegenthaler's correlation attack [Siege84] they must be correlation-immune, with a high order.

State of the art. There exists several classes of "useful" Boolean functions (resilient functions, correlation-immune, bent functions…) depending on criteria which should be satisfied for cryptographic applications. These properties are important to resist known cryptographic attacks to exploit weakness or hidden correlations in Boolean functions. As a consequence, an "ideal" Boolean function should have high algebraic degree, high algebraic immunity, high nonlinearity (eg bent functions), be resilient of high order, etc. Nevertheless, these restrictions cannot be optimally achieved all together. For example, if a function is k-resilient, the algebraic degree can be at most $n-k-1$, while the highest algebraic degree is n.

There are very numerous results which generate specific subclasses of Boolean functions that optimally satisfy one or several good cryptographic properties. In several cases, these constructions generate functions that could be used in practice, but usually they do not generate all of them in a systematic manner. For instance, several constructions of correlation-immune and resilient functions are presented by Carlet in [Carlet12] or by Schneider in [Sch97], but these constructions do not give any insight about the combinatorial structure of these classes.
From a cryptographic point of view, one could be satisfied to consider and build a large set of Boolean functions that satisfy in a very good way, most of the cryptographic criteria. On the other side, we strongly believe that a complete characterization of these functions could lead to more efficient constructions, more efficient random generation algorithms, and better understanding of their properties.

However, these subclasses are not well known: they are not completely characterized, their combinatorial structure remains mysterious, and of course they contain a large number of elements, even if it is very often very small with respect to the total number of Boolean functions. (We have to keep in mind that the total number of Boolean functions with 8 variables is approximately 1.15 X 10^77, larger than the estimated number of atoms in the universe!). It is thus usually not possible to find Boolean functions with given properties with the help of an efficient random drawing based on a trial and error method.

Previous results obtained by the team. The main methodological and innovative contribution in [LBV10] is the division of the complete set of Boolean functions intp equivalence classes with respect to the correlation-immunity property. In this sense, an equivalence relation of functions is proposed, that provides a partition of the set of functions in n variables into classes. The fundamental aspect on this approach is to give a clear recursive construction of "classes", instead of the functions themselves. In this setting, given a

specific class of equivalence of functions on n variables, we described in a constructive way, all the possible combinations of classes in *n-1* variables that generate it. This approach leads naturally to counting algorithms, enumeration algorithms and random generation algorithms. For instance, this makes possible the counting and enumerating all the correlation classes, not only those of the correlation-immune functions.

As the matter of fact, [LBV10] is the first paper to completely characterize, in a constructive way, the set of Boolean function on *n* variables that optimally satisfy some cryptographic property. Moreover, this characterization leads to a generating function approach, and then to extremely tight asymptotic estimators of the total number of correlation immune functions on *n* variables ([Bach09], [CGGMR09]). With an efficient implementation of this approach, Le Bars and Viola obtain the exact number of 1-resilient functions with 7 and 8 variables [LBV10, Carrasco10], the latter being done by Nicolás Carrasco (a Master student at the PEDECIBA Program in Uruguay, and participant of this proposal). In [CLBV11] Carrasco, Le Bars and Viola present an enumerative encoding of 1-correlation-immune and, more specifically, of 1-resilient Boolean functions.

Specific project of the team. Our main goal is to find an alternative "constructive" or "algorithmic" characterization of Boolean functions that optimally satisfy some cryptographic criteria. We believe that a better understanding of the combinatorial properties of these functions, can lead to more efficient constructions, and to better understanding of their behavior against attacks. This understanding would also be a key to a generating function approach, from which we could apply analytic combinatorics in order to get tight asymptotic bounds for the number of Boolean functions we are interested in.

Can the idea of decomposing recursively in classes successfully applied to 1-resilient functions be generalized for other problems? The problem is far from trivial, and this is an extremely difficult question to answer. The main problem consists on how to define these equivalence classes, for the problem at hand (for example, bent functions), and how to give a construction based solely on the classes. It is far from clear, that such partition exist or can be defined in a "simple" way. Moreover, once this partition is defined, then constructions based on classes have to be found.

In any case, we consider important to give some initial steps in this direction, at least to understand the behavior of Boolean functions with small number of variables (like bent functions on 8 variables). It is important to notice, that even though the universe of optimal functions with respect to some cryptographic property is negligible with respect to the total number of Boolean functions in n variables, these numbers are really huge!

There are two main lines of research we are interested in.

We first wish to extend the enumerative encoding performed in [CLBV11] to *k*-order correlation immune functions (for $k>1$).

For our second line of action, we wish to obtain a combinatorial characterization of Bent functions. There are several constructions of specific subclasses as presented in [Carlet12a], but there does not exist any known characterization of all Bent functions for general values of the number n of variables. The idea is to extend the work presented in [LBV10] and, as an initial step, we wish to understand and use the main ideas presented in [LL11]. Among other things, this paper relates Bent functions and Reed-Muller codes, and performs an "intelligent" brute-force complete counting of all Bent functions in 8 variables. The first step consists in understanding the methdology used to count this set of functions. Moreover, based on this understanding, the next step is to try to see the possibility of rederive these results using the "method of classes approach" presented in [LBV10]. This step would be key to understand and try to provide a general methodology to be used to characterize in a constructive way all set of Bent functions in *n* variables, for general *n*. This particular case ($n = 8$) is the central subject of Master's thesis of Nicolás Carrasco.

5- Bibliography

[Beh1] BEHNKE, H., Uber die Verteilung von Irrationalzahlen mod 1, Hamb. abh 1, 252--267 (1022)

[Beh2] BEHNKE, H., Theorie der Diophantischen Approximationen}, Hamb. Abh 3, 261--318 (1924)

[Bach09] BACH, E. Improved Asymptotic Formulas for Counting Correlation- Immune Boolean Functions. SIAM Journal on Discrete Mathematics, 23, 1525-1528, 2009.

[BaVa05a] BALADI, V., and VALLÉE, B., Euclidean Algorithms are Gaussian, Journal of Number Theory, Vol. 110, 2, 2005, pages 331-386.

[BaVa05b] BALADI, V., and VALLÉE, B., Exponential decay of correlations for surface semi-flows without finite Markov partitions, Proc. Amer. Math. Soc. 133, 2005, pages 865-874.

[Beck09] BECK, J., Inevitable Randomness in Discrete Mathematics, University Lecture Series, American Mathematical Society, 2009.

[CaMa06a] CAFURE A., MATERA, G., Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields and their Applications, volume 12(2), (2006) pp. 155-185.

[CaMa06b] CAFURE A., MATERA, G., Fast computation of a rational point of a variety over a finite field, Mathematics of Computation, volume 75(256), 2006, pp. 2049-2085.

[CaMaPri12] CAFURE, A., MATERA, G., and PRIVITELLI, M., Singularities of symmetric hypersurfaces and Reed-Solomon codes, Adv. Math. Commun, 6(1), 2012, pages 69-94.

[CCCS91] CAMION, P., CARLET, C., CHARPIN, C., SENDRIER, N. On correlation-immune functions. Advances in Cryptology: Crypto 91, Proceedings, Lecture Notes in Computer Science, vol. 576, pp. 86-100, 1991.

[CGGMR09] CANFIELD, E. R., GAO, Z., GREENHILL, G., McKAY, B. D., ROBINSON, R. W. Asymptotic enumeration of correlation-immune boolean functions. *Cryptography and Communications*, 2 (1), 111-126, 2010.

[Carrasco10] CARRASCO, N. Generación aleatoria efficiente de funciones Booleanas resilientes. Undergraduate thesis. Universidad de la Republica, Uruguay, 2010.

[Carlet12a] CARLET, C. Boolean Functions for Cryptography and Error Correcting Codes. To appear in ”Boolean Methods and Models”. Cambridge University Press.

[Carlet12b] CARLET, C. Vectorial Boolean Functions for Cryptography. To appear in ”Boolean Methods and Models”. Cambridge University Press.

[CesVal06] CESARATTO, E., VALLÉE, B., Hausdorff dimension of real numbers with bounded digit averages.

[CesPlagVal06] CESARATTO, E., PLAGNE, A., and VALLÉE, B., On the non-randomness of modular arithmetic sequences. Discrete Math. Theor. Comput. Sci. Proc. AG, 2006, pages 271-288.

[CesCleDaiLhoMauVal09] CESARATTO, E., CLEMENT, J., DAIREAUX, B., LHOTE, L., MAUME, V., and VALLÉE, B., Regularity of the Euclid Algorithm. Application to the analysis of fast gcd Algorithms. Journal of Symbolic Computation, vol 44, 2009, pages 726-767.

[CesVal11a] CESARATTO, E., and VALLÉE, B., Small quotients in Euclidean algorithms, Ramanujan Journal, vol 24, 2, 2011, pages 183-218.

[CesVal12] CESARATTO, E., and VALLÉE, B., Pseudorandomness of a random Kronecker sequence, in David Fernández-Baca (Ed.): Latin 2012, Theoretical Informatics, Lecture Notes in Computer Science, 7256, 2012, pages 157-171.

[CiuGirLho11] CIUPERCA, G., GIRARDIN, V., and LHOTE, L., Computation of Generalized Entropy Rates. Application and Estimation for Countable Markov Chains, *IEEE Transactions on Information Theory,* V57, pp. 4026--4034, (2011)

[CleFlajVal01] CLEMENT, J., FLAJOLET, P., and VALLÉE, B., Dynamical Sources in Information Theory: A General Analysis of Trie Structures, Algorithmica 29, 2001, pages 307-369.

[Cover73] COVER, T-M. Enumerative Source Encoding. IEEE Transactions on Information Theory, 19 (1) , 73 - 77, 1973.

[DauFlaVal97] DAUDE, H., FLAJOLET, Ph., and VALLÉE, B., Average-case analysis of the Gaussian algorithm for lattice reduction, Combinatorics, Probability and Computing, vol *6 (4),* 1997, pages 397-433.

[Dol98] DOLGOPYAT, D., On decay of correlations in Anosov flows. Ann. Math. 147, 2, 1998, pages 357-390.

[Dol00] DOLGOPYAT, D., Prevalence of rapid mixing. II. Topological prevalence. Ergodic Theory Dynam. Systems, 20, 4, 2000, pages 1045-1059.

[FlaSed09] FLAJOLET, Ph., and SEDGEWICK, R. Analytic Combinatorics. Cambridge University Press, 2009. xiv+810 pages. Also available electronically from the authors' home pages.

[FlaVal98] FLAJOLET, P. and VALLÉE, B., Continued fraction algorithms, functional operators, and structure constants, Theoretical Computer Science (1998), vol 194, 1--2, pp 1--34.

[FlaVal00] FLAJOLET, P. and VALLÉE, B., Continued Fractions, Comparison Algorithms, and Fine Structure Constants}, in Constructive, Experimental et Non-Linear Analysis, Michel Thera, Editor, Proceedings of Canadian Mathematical Society, Vol 27 (2000), pp 53-82

[GaShpSin03] VON ZUR GATHEN, J., SHPARLINSKI, I., and SINCLAIR, A., Finding points on curves over finite fields, SIAM J. Comput., 6,32, 2003, pages 1436-1448.

[HPS11] HANROT, G., PUJOL, X., and STEHLÉ, D., Analyzing Blockwise Lattice Algorithms using Dynamical Systems, In the proceedings of CRYPTO 2011.

[HS99] HAVAS, G., SEIFERT, J., The Complexity of the Extended GCD Problem, Mathematical Foundations of Computer Science 1999, *LNCS*, Vol.1672, pp.103-113, 1999.

[KnopKnop90a] KNOPFMACHER, A., and KNOPFMACHER, J., Counting polynomials with a given number of zeros in a finite field, Linear Multinear Algebra, 26, 1990, pages 287-292.

[Knuth65] KNUTH, D. E. Construction of a random sequence, Bit Numerical Mathematics, Vol. 5, Num 4, (1965) pp. 246-250.

[Knuth97] KNUTH, D. E. The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms. Addison-Wesley Longman Publishing Co., Inc., 1997.

[LL11] LANGEVIN, P., LEANDER, G. Counting all bent functions in dimension eight. Designs, Codes and Cryptography, 59 (1), 193-205, 2011.

[LBV10] LE BARS, J-M., VIOLA. A. Equivalence classes of Boolean functions for first-order correlation. IEEE Transactions on Information Theory, 56 (3) , 1247 - 1261, 2010.

[LhoVal08] LHOTE, L. and VALLÉE, B. Gaussian laws for the main parameters of the Euclid Algorithms, Algorithmica (2008) 50 pp 497—554

[Massey69] MASSEY, J. L. Shift register synthesis and BCH decoding. IEEE Transactions on

Information Theory, 15, 22-127, 1969.

[Mat10] MATERA, G., The computation of rational solutions of polynomials systems over a finite field, in D. Sadornil Renedo, D Gómez Pérez and F. Santos Leal (editors), *Libro de actas* de las VII Jornadas de Matemática Discreta y Algorítmica, (2010) , pp. 9-33.

[MaVa10] MADRITSCH, M., and VALLÉE, B., Modelling the LLL algorithm via sandpiles, LATIN 2010: Theoretical Informatics, Lecture Notes in Computer Science, 2010, Volume 6034/2010, 267-281

[NgVa10] NGUYEN, P., and VALLÉE, B., (ed.) The LLL algorithm. Survey and applications, Information Security and Cryptography. Dordrecht: Springer, (2010).

[Obi] http://algo.inria.fr/pfac/PFAC/Obituary.html

[PolSharp98] POLLICOT, M., and SHARP, R., Exponential error terms for growth functions on negatevely curved surfaces, Amer. J. Math., 120, 1998, pages 1019-1042.

[RoVa11] ROUX, M. and VALLÉE, B., Information theory: Sources, Dirichlet series, and realistic analyses of data structures., Proceedings of the Conference Words'11.

[Scho1] SCHOISSENGEIER, J., On the discrepancy of (n .alpha), Acta Arithmetica 44, (1984) pp 24--279.

[Scho2] SCHOISSENGEIER, J., The discrepancy of (n alpha), Math. Ann. 296 (1993), pp 529--545.

[Sch97] SCHNEIDER, M., On the construction and upper bounds of balanced and correlation-immune functions. 6th IMA conference, 295-306, 1997.

[Sch00] SCHWEIGER, F., Multi-dimensional continued fractions, Oxford Science Publications, Oxford Univ. Press, Oxford (2000).

[Shannon49] SHANNON, C. E., Communication theory of secrecy systems. Bell Systems Technical Journal, 28, 656-715, 1949.

[Siege85] SIEGENTHALER, T., Cryptanalysis Representation of Nonlinearly Filtered M-Sequences Advances in Cryptology: EUROCRYPT ’85. 103-110.

[Siege84] SIEGENTHALER, T., Correlation-immunity of linear combining functions for cryptographic applications. IEEE Transactions on Information Theory, 30(5), 776-780, 1984.

[Szp] SZPANSKOWSKI, W., Average case analysis of algorithms on sequences, Wiley, Interscience series in Discrete Mathematics and Optimization, 2001

[Uchi55] UCHIYAMA, S., Note on the Mean Value of V(f). II, Proc. Japan Acad., 31, 6, 1955, pages 321-323.

[Val98] VALLÉE, B., Dynamique des fractions continues à contraintes périodiques, Journal of Number Theory, 72, no. 2, 1998, pages 183-235.

[Val98b] VALLÉE, B., Dynamics of the Binary Euclidean Algorithm: Functional analysis and operators, Algorithmica (1998), vol 22 (4) pp 660--685.

[ValLem98] VALLÉE, B., and LEMÉE , C, Algorithms for computing the Jacobi symbol unpublished note, 1998. Available electronically from B. Vallée's home page.

[Val01] VALLÉE, B., Dynamical sources in Information Theory: Fundamental Intervals and Word prefixes, Algorithmica (2001), vol 29 (1/2) pp 262—306

[Val03] VALLÉE, B., Dynamical Analysis of a class of Euclidean Algorithms, Theoretical Computer Science, vol 297/1-3 (2003) pp 447--486

[Val06] VALLÉE, B., Euclidean Dynamics. *Discrete and Continuous Dynamical Systems*, vol. 15:1, 2006, pages 281—352.

[Val12a] VALLÉE, B., The Euclid Algorithm is totally Gaussian, to appear in the proceedings of AofA'12, Discrete Mathematics and Theoretical Computer Science (2012)

[ValCleFlajFill09] VALLÉE, B., CLEMENT, J., FLAJOLET, Ph., FILL, J., Albers et al. (Eds.): ICALP 2009, Part I, LNCS 5555, 2009, pages 750-763.

Submitted or in preparation

[BerLhoVal12] BERTHÉ, V., LHOTE, L., and VALLÉE, B., Dynamical Analyses of some continued fraction algorithms in higher dimensions, in preparation.

[BerNakNatVal12] BERTHÉ, V., NAKADA, H., NATSUI, R., and VALLÉE, B., The Farey map and the fine complexity of the Euclid algorithm on *F_q[X]*, submitted

[Cafure et al.12] CAFURE, A., CESARATTO, E., MATERA, G., PEREZ, M., PRIVITELLI, M., Average-case complexity of finding rationals points in hypersurfaces over finite fields, work in progress.

[CesMaGat11] CESARATTO, E., VON ZUR GATHEN, J., MATERA, G., The number of reducible space curves over a finite field, submitted to Journal of Number Theory.

[CesVal11b] CESARATTO, E., and VALLÉE, B., Gaussian distribution of trie depth for dynamical sources, [40 p], submitted.

[CLBV11] CARRASCO, N., LE BARS, J-M. VIOLA, A., Enumerative encoding of correlation-immune Boolean functions, submitted to Theoretical Computer Science.

[Geor12] GEORGIEVA, M., Analyse probabiliste des réseaux cryptographiques, PhD of the University of Caen, in preparation, defence planed in December 2012.

[Val12b] VALLÉE, B., A main step towards the distributional analysis of periodic trajectories under geometrical conditions for the dynamical system, preprint.

6- Organisation of the project

6.1. Description of the teams and their contributions.

There are three teams in the project, and we now describe them. The Curriculum vitae of participants can be found in 6.7.

The team in Montevideo. The team gathers one permanent member (Alfredo Viola) and two students (Nicolás Carrasco and Fernando Fernández). They belong to the Algorithmics group, inside the Laboratorio de Ciencias de la Computación at the Instituto de Computación, Universidad de la República. The main research activities of the group are based on the design and analysis of algorithms in several areas related with computer science. Besides working in theoretical computer science, the group has collaboration with other research teams, some of them in relation with the industry.

The group mainly uses methods based on Analytic Combinatorics to study the probabilistic behavior of algorithms and underlying data structures. Recently, it adopts a combinatorial point of view to study Boolean Functions to be used in cryptographic applications. There is also joint collaboration with the group on Information Theory. These techniques have proved to be very useful to study problems related with both source coding and error-corrector coding. The group has also recently started collaboration with teams working in telecommunications. In this regard, the mathematical background of our group has proved to be very useful to analyze, understand and propose better algorithmic solutions to several important practical problems in communications and networking.

The group is also involved in the organization of seminars, workshops and conferences. Their members participate in several research projects with both, national and internacional financial support, and in the Master and Ph.D. programs in computer science and electrical engineering of the Facultad de Ingeniería. They also make lecture courses in the undergraduate programs of the Facultad.

The team in Buenos-Aires. The team coincides with the research Group In Geometry and Arithmetics (GIGA) at the National University of Gral. Sarmiento. The group is lead by Guillermo Matera and its members are Antonio Cafure and Eda Cesaratto (senior researchers) and the Ph. D. students Melina Privitelli and Mariana Pérez.

The National University of Gral. Sarmiento (UNGS) is located in a suburb on the North-West of the city of Buenos Aires and it has been created in the nineties with the aim at developing a pole of research in this "social not-favoured" area of the country. The University counts with a Ph. D school in Science and Technology. One of the main objects of this school is to help the local industries to improve their technological resources.

The GIGA group has been created in 2003 and it aims at developing efficient (symbolic or numeric) algorithms for solving polynomial systems, and it concentrates on algorithms for computing selected solutions of the input system. It is also mainly concerned in analysing the probabilistic behavior of these algorithms, and in related combinatorial problems which arise in the probabilistic analysis. The GIGA group has a previous experience of similar projects, in particular Conicet projects.

The team in Caen. The team gathers six members of the GREYC Laboratory (permanent members: Julien Clément, Jean-Marie Le Bars, Loïck Lhote and Brigitte Vallée – two PhD students: Thu Hien Nguyen Thi and Kanal Hun) and two associate researchers: Valérie Berthé (LIAFA, Paris) and Valérie Girardin (LMNO, Caen).

The members of GREYC belong the AMACC team (Algorithmique, Modèles de Calcul, Aléa, Cryptographie, Complexité), one of eight teams of the GREYC Laboratory (around 120 permanent members). The main interests of the group coincide with all the main themes of the project, and its interest in general cryptography is also due to the presence of specialists in cryptography inside the AMACC team. The Caen team has a previous experience of similar projects. It was the coordinator of a previous ANR project (LAREDA 2007—2010), its members work in various other ANR projects. Furthermore, it plays an important rôle in the Groupe de Recherches en Informatique Mathématique (GdR IM) which gathers all the French researchers who work at the interface between Mathematics and Computer Science.

Two French associate researchers. They represent an opening for the main thematics of the project, respectively towards statistical and probabilistic concepts, brought by Valérie Girardin (LMNO: Laboratoire de Mathématiques Nicolas Oresme, Caen) and symbolic dynamics, brought by Valérie Berthé (LIAFA Laboratory, Paris). These two members will be associated with the GREYC laboratory for the present project.

In 2007, Valérie Berthé and Brigitte Vallée realized that they are interested in the same objects (continued fraction expansions), with complementary points of view: symbolic dynamics for Valérie Berthé, analytical dynamics for Brigitte Vallée. They decided to be joint coordinators of the LAREDA project (funded by the French ANR, 2007-2010) (LAREDA:Lattice reduction algorithms: Dynamics, Probabilities, Experiments, Applications), and they now develop a regular and fruitful collaboration, together with Loïck Lhote.

In 2007, Valérie Girardin (LMNO) and three members of GREYC (Julien Clément, Loïck Lhote and Brigitte Vallée) realized that they were using the same mathematical/algorithmic objects in their research, and decided in 2007 to join in a periodic working group on the concept of information source. This group closely combines statistical and probabilistic concepts (represented by Girardin) and formalization of general sources (represented by Vallée, Lhote and Clément).

6.2. PhD and Master students.

In the beginning of our project, there will be four PhD students and two Master students (and future PhD students).

– Mariana Pérez (UNGS) was doing her PhD under the direction of Guillermo Matera since 2011. “Probabilistic algorithms for searching rational roots of polynomial systems over finite fields”.

Melina Privitelli (UNGS) is doing her PhD under the direction of Guillermo Matera “Existence and number of rational solutions of polynomial systems over finite fields. Applications”.

– Nicolás Carrasco (UdelaR) is doing his Master Thesis under the joint direction of Alfredo Viola and Jean-Marie Le Bars and will begin a PhD thesis under their joint supervision "Towards a combinatorial approach to study bent functions".

– Fernando Fernández (UdelaR) is finishing his Master Thesis under the joint direction of Alfredo Viola and Marcelo Weinberger. He will begin a PhD thesis under their joint supervision “Efficient algorithms for constructing bi-directional context sets”.

– Thu Hien Nguyen Thi (GREYC) is doing her PhD under the joint supervision of Julien Clément and Brigitte Vallée: « Realistic analysis of sorting and searching algorithms ». She has begun her thesis in October 2010.

– Kanal Hun (GREYC) is doing his PhD under the direction of Brigitte Vallée: « Analysis of digital search trees on general sources ». He has begun his thesis in October 2011.

6.3. History of the strong existing collaborations.

We describe the state of existing collaborations inside the present project. The first three items describe existing international collaborations which form the historic basis, under which the project is based, and the last second items describe more recent internal collaborations which can spread into the whole group.

The international AofA Group. The French team and Alfredo Viola began to regularly meet together during the nineties, when Philippe Flajolet founded the international Analysis of Algorithms Group (AofA). The annual meetings of the group have had a deep influence on the resarch in the domain, and created a natural and friendly framework for collaborations.

Ecos Project. The Ecos project "Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en Criptografía y Teoría de la Información" (2009—2011; coordinator: Frédérique Bassino) gathered three members of the present project: Julien Clément, Jean-Marie Le Bars, Alfredo Viola. This project led Jean-Marie and Alfredo to a regular collaboration on the use of Analytic combinatorics methods in study of Boolean functions (see description of their results in Section 4). The present project wishes to be a successor for this "success story".

PhD Thesis of Eda Cesaratto. Eda Cesaratto and Brigitte Vallée met (via e-mail) around 2003. Brigitte became the supervisor of Eda for the second part of her thesis that is defended in 2005. Since then, they have established a strong and regular collaboration which led them to numerous and important joint results, in the heart of the present project, mainly in Dynamical Combinatorics methodology, and its application to Number Theory (see Sections 1 and 2 and the bibliography). They have written together more than six papers. They already meet twice or three times a year, without special funds, and the present project may help to establish this collaboration on a clearer financial basis.

Creation of the GIGA Group. When the group was created in 2003, it mainly focussed on studying algorithms for solving polynomial systems. When Eda Cesaratto became a member of the group in 2008, this created a second theme inside it. Then, the GIGA group has already adopted the two complementary points of view that are described in the beginning of Section 2. The present project wishes to reinforce this strategy and spread it inside the whole team.

Collaborations of the French Team. As mentioned in the description of the team (6.1), the GREYC group has initiated new collaborations in order to develop two "mixed" points of view in Dynamical Combinatorics: the first one at the interface of symbolic and analytic dynamics, the second one at the interface of probability and information theory. As in the previous item, the present project wishes to reinforce this strategy and spread it inside the whole team.

6.4. Main goals of the project.

One of our main goals is to consolidate strong research collaborations between different research groups. Even though they have already strong bilateral collaborations, they have never worked altogether as a group.

Reinforcements of existing collaborations and existing thematics and integration of new students there. As we have seen in 6.4, there is a strong, rich and productive history of strong

existing collaborations. We aim at reinforce it. In this regard, one of the main goals is to integrate graduate students. This is one of the key components of our proposal.

Development of new interactions. In particular, the two South-American teams, Montevideo and Buenos-Aires, wish to start a more consolidated collaboration. Even though there have been some visits to the laboratories, there is no formal collaboration with joint publications and results. We aim to profit from the complementary point of views of the different research groups, and integrate algebraic geometry and analytic combinatorics. In particular, Matera and Viola wish to strengthen their collaboration.

There are also two other possible interfaces which already exist inside the French team project and may be developed inside the whole group

– Symbolic dynamics vs analytic dynamics;

– Dynamic combinatorics vs probabilistic approaches.

Specific actions towards students. A large number of students are involved in the project, and an important goal is to strongly integrate them into our existing collaboration. This project will benefit their scientific contributions in their thesis. Besides joint supervision of some of them, the interaction with specialists in their research domain will help in the quality of the thesis. Moreover, general meetings are also very important. We plan to do presentations of our advances, but furthermore to discuss strategic issues related with the project. This is a very important component in the students education for their scientific career.

6.5. Organisation of the project.

We first describe the general organisation and then our three main types of actions: plenary events, small thematic meetings, an intensive school, and, more generally, specific actions towards young people.

General organisation. The main scientific coordinator of the project is Eda Cesaratto, and there are four scientific sub-ccordinators, one for each of the main four scientific themes of the project. Their tasks are essential in the scientific life of the project.

Theme 1: Brigitte Vallée (Caen) –Theme 2: Eda Cesaratto (Buenos Aires) –Theme 3: Julien Clément (Caen) –Theme 4: Alfredo Viola (Montevideo).

There are also administrative sub-coordinators, one for each academic partner: Alfredo Viola (UdelaR)-- Eda Cesaratto (UNGS) – Brigitte Vallée (GREYC). They have to deal with administrative tasks (money, for instance).

Meetings. We plan to organize internal meetings, of two types: plenary meetings and partial meetings. There would be three plenary meetings (one each year) which will gather all the project members during a whole week. Each plenary meeting has two components: during the first part, there would be parallel small meetings on precise points of the project, whereas the second part is devoted to a large meeting where the results of small meetings are reported. In the meantime between these plenary meetings, some small meetings would be organized, corresponding for instance to one of the four main themes of the project.

Precisions about the three plenary meetings.

– A kick-off meeting with all the research team, on February/March 2013 in Argentina. This is important to have a first meeting at the very beginning of the project. There will be mainly plenary talks to share the main subjects (each member has to learn in the subjects of the others), but also small working groups, more centered on a precise subject of the project.

– An intensive school with short courses on February/March 2014 (see 6.6) in Buenos-Aires.

– A closing meeting on February/March 2015 (if possible, since this would take place after the closing dates for the project), with the same organizations as the kick-off meeting. This meeting could take place in Uruguay.

6.6. *Organisation of the intensive school on the scientific themes of the project.*

Analytic and Dynamical Combinatorics. Applications

In the present days, the probabilistic point of view in the analysis of algorithms, more precisely the methods of Analytic Combinatorics, and their applications are widely spreading in the international community. However, research and teaching in these fields are under-represented in Argentina.

We plan to organize a small intensive school oriented to graduate students in the region, to be held at UNGS in 2014. It would be a very important tool for developing strong research groups in the region with the participation of young researchers. These young people will not only be able to integrate to our research groups, but also will be able to work and have impact in general fields of academic or industrial research.

This mini-school would have an important institutional impact because it would reinforce the role of the UNGS School of Science and Technology and it would give the opportunity to students and young researchers meet researchers from other countries. It will be a very important tool for developing strong research groups and training young people. This young people will not only be able to integrate to our research groups, but also be able to work and have impact in general fields of academic and/or industrial research.

The plan is to organize this school at the beginning of the year 2014 (around the end of February or the begining of March 2014). We plan to organize it in 2014, since there will be already a CIMPA school on Modern Methods in Combinatorics which will be held in July 2013, in the city of Merlo, San Luis, Argentina.

The school will be one week long. Our plan is to have several courses (between four and six). Each of them will be between three and six hours long, and is followed with exercices. They will be mainly given by the senior participants of the project. There will be also a large amount of time devoted for students' scientific talks.

Subject of planed courses: The scientific subjects are those of the present project.

– Analytic combinatorics (Julien Clément, Brigitte Vallée, Alfredo Viola)

– Dynamical Combinatorics and its applications in number theory (Eda Cesaratto, Loïck Lhote, Brigitte Vallée)

– Algebraic methods and combinatorial problems on polynomials over finite fields. (Antonio Cafure, Eda Cesaratto, Guillermo Matera,)

– Analytic combinatorics and cryptography (Jean-Marie Le Bars, Alfredo Viola,)

– Analytic combinatorics and information theory (Julien Clément, Brigitte Vallée)

Other actions towards young people. We expect to be able to get several specific results with their corresponding publications. We feel that student participation in conferences,

as well as their formal presentation of the results in them, is also a key component in their scientific education.

6.7. Towards a south-american network in Mathematical Informatics ?

We first describe the landscape of existing interactions between Uruguay, Argentina and France both in Theoretical Computer Science (the INFINIS laboratory) and in Dynamical Systems (The IFUM laboratory). We then mention previous initiatives and finally explain how the present project may play a role in this scientific landscape.

Two existing laboratories between France, Uruguay and Argentina. There already exist two structures we can interact with: the INFINIS Laboratory and the IFUM Laboratory.

The INFINIS laboratory was created three months ago. This is a French-Argentinean Laboratory (Laboratoire International Associé) between Centre National de la Recherche Scientifique (CNRS) and Université Paris Diderot, on the one hand, and Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) and the Universidad de Buenos Aires, on the other. The acronym stands both for "INformatique Fondamentale, LogIque, LaNgages, VérIficacion et Systèmes" and also "INformática Fundamental, lógIca, leNguajes, vérIficación y Sistemas". It is co-directed by Delia Kesner (Professor at Université Paris Diderot) et Sergio Yovine (Research director at CNRS and CONICET).

It is devoted to research in Computer Science. Specific focus is placed on formal methods, for modeling, verification and development of complex software artifacts. There are four research groups: verification, semantics, natural language and complexity & randomness.
These scientific domains are not so close to those developed in the present project, even if the last group is clearly the closest one. During the submission of the project, we began to study and discuss with Delia Kesner the possibility for our group to have stronger interactions with this laboratory. In the future, can it be inserted as a next axis in the laboratory?

The IFUM Laboratory. The French-Uruguayan Institute of Mathematics (IFUM) was created on December 2009. It associates a number of French laboratories in Paris, Montpellier, and Toulouse, with the University of the Republic and the Program for the Development of Basic Sciences (PEDECIBA) in Montevideo (Uruguay). Following a long-standing cooperation in mathematics between the two countries, this International Associated Laboratory (LIA) will coordinate research in three mathematical fields: algebra and geometric algebra; dynamic systems; and statistics and probability.

Each project of the LIA IFUM must be built with asking other financial supports to other organisations (for instance, projects funded by the French ANR, French laboratories, PEDECIBA, UdelaR, etc..). More recently, the IFUM laboratory "encourages the interested mathematicians to apply for financial aid for the organization of workshops involving a short period of concentrated work for small groups and within a specific thematic interest (for example to start, continue or finish a specific paper in subjects of joint interest, or to organize a crash course in a subject of current interest for the development of some particular line of work, etc.)". It is also written that projects that are also based on cooperation with Argentinean laboratories are specially appreciated.

Eda Cesaratto and Brigitte Vallée belong to the third theme of the laboratory, and are on its mailing list. This theme is co-directed by Viviane Baladi (DMA - CNRS and ENS-Paris) and Ezequiel Maderna (Centro de Matemática de la Facultad de Ciencias – Montevideo). During the submission of the project, we began to make explicit the relations between the present project and the IFUM Laboratory, and we think that the possible overlapping between the two points of view on dynamical systems may be used as a reinforcement of this theme. The head of the laboratory, Claude Cibils thinks that the present project may enhance, complement and perhaps boost existing collaborations.

Some previous initiatives of the members of the project. We give three main examples:

– In 2000, the international conference LATIN was organized by Daniel Panario and Alfredo Viola in Uruguay, with a strong participation of the Analytic Combinatorics community (AofA, see 6.3), including two keynote talks given by Andrew Odlyzko and Philippe Flajolet.

– In 2008 the International Conference on the Analysis of Algorithms (AofA'08) was organized by Daniel Panario, in Maresias, Brazil, with strong participation of students and researchers from the region, specially from Chile and Brazil.

– At the level of STIC-AMSUD, the project "FMCrypto: Formal Methods for Cryptographically Secure Distributed Computations" (2009-2011) gathered researchers from France, Brazil, Chile and Uruguay, with the participation of Alfredo Viola. The main achievement of this extremely successful project was the creation of the international conference LATINCRYPT, whose first edition was held in 2010 in Puebla, Mexico and the second edition will be held in 2012 in Santiago, Chile. This conference counted with the strong participation of french researchers.

Conclusion. The present project may be an important step towards the creation of a regional network related to Analytic Combinatorics and applications (specially in computational number theory, symbolic computation, information theory and cryptography).

The participation of French partners can can be very helpful to this regard, since they have the experience of such networks in France. The French team plays an important role inside the Groupe de Recherche en Informatique Mathématique (a French CNRS structure called GDR IM) which gathers all the French scientists who work in the field of "Mathematical Informatics".

It is important to notice that, even though there are already strong academic relations, there does not exist yet a well-connected network of collaborations. Besides a stronger collaboration between UdelaR and UNGS, this network could integrate with other initiatives, and other existing structures, including the French-Argentinean LIA Laboratory INFINIS in Buenos-Aires and the French-Uruguayan IFUM Laboratory.

6.8. Curriculum-vitae of participants

We list the curriculum vitae of the members of the project:

First the CV of the coordinators:

Eda Cesaratto, Alfredo Viola, Brigitte Vallée.

Then the CV's of the other permanent members (by alphabetical order)

Valérie Berthé, Antonio Cafure, Julien Clément, Valérie Girardin,

Jean-Marie Le Bars, Loick Lhote, Guillermo Matera.

Eda Cesaratto (UNGS-Buenos Aires)

1/ **Personal data**

Name: Cesaratto, Eda **Birth date**: 01/09/1969

Professional address :

National University of General Sarmiento. Instituto del Desarrollo Humano– J. M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Bs. As, Arg. -- Phone: +54 11 44 69 77 24

email: ecesarat@ungs.edu.ar

Current job title and size of the research group:

Member of the GIGA group (research group in geometry and arithmethics) (four permanent members and 3 Ph. D. students)

2/ **Highest obtained degree (with indication of place and date)**

Ph. D. Thesis at the University of Buenos Aires (Argentina) 2005. In Spanish: "Dimensión de Hausdorff y esquemas de representación de números" Director: Brigitte Vallée

3/ **Professional activity – Last 5 years :**

– Conicet researcher at National University of Gral. Sarmiento (Argentina) since 2008

– Adjoint professor since March 2008

4/ Other duties/ positions – Last 5 years

– Coordinator of the admission system of UNGS (Area: Mathematics).

– CNRS post-doctoral position at GREYC laboratory, University of Caen (2006)

7/ Projects approved in the least 5 years

Member of the following projects

– March 2010-February 2012, "Algoritmos eficientes en geometría y aritmética", Conicet Director: G. Matera.

2007 – 2011: " Algoritmos eficientes para problemas de geometría y aritmética". IDH. Instituto de Desarrollo Humano. Universidad de Gral. Sarmiento'. Director: G. Matera

8/ Publications

Most important publications in the last 5 years related to the project theme

[1] E. Cesaratto, B. Vallée, Pseudorandomness of a random Kronecker sequence, en David Fernández-Baca (Ed.): Latin 2012, Theoretical Informatics, *LNCS*, 7256, Springer-Verlag, Berlin-Heilderberg, (2012) pp. 157—171, 2012.

[2] E. Cesaratto, B. Vallée, Small quotients in Euclidean algorithms, *Ramanujan Journal*, Vol 24, No 2, (2011) pp. 183-218.

[3] E. Cesaratto, A note on "Euclidean Algorithms are Gaussian" by V. Baladi and B. Vallée, *Journal of Number Theory*, 129 (2009) pp. 2267–2273.

[4] E. Cesaratto, J. Clément, B, Daireaux, L. Lhote, V. Maume, B. Vallée, Regularity of the Euclid Algorithm. Application to the analysis of fast gcd Algotithms. *Journal of Symbolic Computation*, 44 (2009) 726-767.

[5] E. Cesaratto, B. Vallée, Hausdorff Dimension of real numbers with bounded digits averages, *Acta Arithmetica* Vol 125, Nº 2 pp 115-162, 2006, pp. 1730-6264(e)

[6] E. Cesaratto, A. Plagne, B. Vallée, On the non randomness of modular arithmetic progressions, *Fourth Colloquium on Mathematics and Computer Science. Algorithms, trees, Combinatorics and Probabilities, DMTCS Proceedings Series Volume AG*, (2006) pp. 271- 288.

Submitted papers

[7] E. Cesaratto, J. von zur Gathen, and G. Matera, The number of reducible space curves over a finite field, submitted to Journal of Number Theory.

[8] E. Cesaratto, B. Vallée, Gaussian distribution of trie depth for dynamical sources, [40 p], submitted.

8.2 – Publications in cooperation with the project partners: All the papers in 8.1

AlfredoViola (UdelaR, Montevideo)

1/ **Personal data**

Name: Alfredo Viola **Birth date**: January 15, 1960

Professional address :

Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Julio Herrera y Reissig 566, Montevideo URUGUAY, CP: 11300

Email : viola@fing.edu.uy

Current job title and size of the research group:

Full Professor, 3 people

2/ **Highest obtained degree (with indication of place and date)**

Ph. D. in mathematics, mention Computer Science, University of Waterloo (1996)

3/ **Professional activity – Last 5 years :**

-- Main area of research: Analytic Combinatorics and applications to analyze problems in Data Structures, Information Theory and Cryptography.

-- Graduate and undergraduate courses in Coding Theory, Cryptography and Analytic Combinatorics.

. -- Member of several committes to evaluate researchers and research projects at national level.

-- International member of committee to accredit graduate programs in Computer Sciences in several Universities of Argentina (CONEAU).

-- President of the committee to evaluate the "Concurso Latinoamericano de Tesis de Maestría" (2009, 2010).

-- Member of program committee of LATIN (2008, 2010, 2012), LATINCRYPT (2010, 2012), ANALCO (2008), LAGOS/GRACO (2009), AOFA (2007).

-- Referee for several journal papers at IEEE Transactions on I.T., ACM TALG, CPC.

4/ Other duties – Last 5 years

-- 2011--2012: Sabbatical leave at UPC in Barcelona.

-- May 2010 – June 2010: Visit at Université Paris Nord (Paris XIII)

Visit at Université Pierre et Marie Curie (Paris VI)

-- June and July 2008 : Visit at Université de Caen and Université de Marne la Vallée

-- July 2009 and June and July 2010 : Visit at Université de Caen

-- December 2007 and December 2008: Visit at the Universidad de Chile (2 weeks)

-- May 2009: Visit at the University of Carleton (2 weeks)

-- June 2009: Visit at UPC in Barcelona (2 weeks)

7/ Projects approved in the least 5 years

-- 2006 – 2008 "Codigos libres de prefijos óptimos con alfabetos infinitos y su uso en algoritmos eficientes de compresión". Support PDT (National funding).

-- 2009 – 2011 "Análisis de Funciones Booleanas y sus Aplicaciones a la Criptografía". Support CSIC (National Funding).

-- 2009 – 2011 "FMCrypto: Formal Methods for Cryptographically Secure Distributed Computations", STIC-AMSUD.

-- 2009 – 2011 "Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en criptografía y Teoría de la Información", ECOS Project.

8/ Publications

8.1 –**Most important publications in the last 5 years related to the project theme**

[1] Jean-Marie Le Bars, Alfredo Viola. Equivalence classes of boolean functions for first-order correlation. IEEE Transactions on Information Theory, v. 56 3, p.: 1247 – 1261, 2010.

[2] Conrado Martínez, Daniel Panario and Alfredo Viola, Adaptive Sampling Strategies for Quickselect . ACM Transactions on Algorithms, v.: 6 (3), Article 53, 2010.

[3] Alfredo Viola, A. Distributional Analysis of the Parking Problem and Robin Hood Linear Probing Hashing with Buckets. Discrete Mathematics and Theoretical Computer Science (DMTCS), v.: 12 2, p.: 307 - 332, 2010.

[4] Ahmed Helmi, Jerémie Lumbroso, Conrado Martínez and Alfredo Viola. Counting Distinct Elements in Data Streams: the Random Permutation Viewpoint. AofA 2012, Montreal, Canadá , 2012

[5] Fernando Fernández, Alfredo Viola and Marcelo Weinberger. Efficient algorithms for constructing bi-directional context sets.IEEE Data Compression Conference, 2010.

[6] Frédérique Bassino, Julien Clément, Gadiel Seroussi, and Alfredo Viola, A. Optimal prefix codes for pairs of geometrically-distributed random variables. Accepted at IEEE Transactions on Information Theory, 2012.

Submitted :

[1] Nicolás Carrasco, Jean-Marie Le Bars; and Alfredo Viola. Enumerative Encoding of first order correlation immune Boolean Functions. Submitted at Theoretical Computer Science, 2011.

[2] Joachim von zur Gathen, Konstantin Ziegler, Alfredo Viola. Counting reducible, squareful, and relatively irreducible multivariate polynomials over finite fields. Submitted to Siam Journal on Discrete Mathematics, 2011.

8.2 – Publications in cooperation with the project partners: See [1] [5], [6]

9/ Theses oriented and post-doctoral fellows supervised

9.2 – Ongoing

Master theses: Nicolás Carrasco, Eduardo Cota, Jorge Merlino and Fernando Fernández.

Brigitte Vallée (GREYC, Caen)

1/ **Personal data**

Name: Vallée, Brigitte **Birth date**: June, 3 1950

Professional address :

Laboratoire GREYC (UMR 6072), Campus Côte de Nacre, Boulevard du Maréchal Juin, BP 5186 - 14032 Caen CEDEX

FAX: +33 (0)2 31 56 73 30 - Office: S3-381-Telephone: +33 (0)2 31 56 74 09

email: brigitte.vallee@unicaen.fr

Current job title and size of the research group:

CNRS full-time researcher (Directrice de Recherche) at GREYC (about 120 persons)

2/ **Highest obtained degree (with indication of place and date)**

Habilitation Thesis, 1989, Université de Caen, France. (In French "Habilitation à diriger des recherches").

3/ **Professional activity – Last 5 years :**

Full-time CNRS researcher at GREYC (directrice de recherches)

4/ Other duties/ positions – Last 5 years

-- Since 2006, head of the Groupement de Recherche (GdR) "Mathematical Informatics" which gathers all the French teams which work at the interface of Mathematics and Computer Science (around 1200 permanent members, and 600 PhD students)

– Since 2007, vice-presidente of the Computer Science section of the ANR Committee

– Since 2009, head of one of the six sub-committees of the Allistene organization which gathers all the main french institutions which work in Computer Science (Universities, CNRS, Engineer Schools, etc..)

– Member (2008-2011) of the CNU committee (Conseil National des Universit´es). which evaluates the applications for assistant professors and professors, at the national level.

5/ Awards, fellowships and external recognition

6/ **Ongoing funded research projects with dates, titles, sources of funding**

– Member of the ANR Project BOOLE (2010-2013) funded by the French ANR (Agence nationale de la recherche)

– Member of the ANR Project MAGNUM (2011-2014) funded by the French ANR

7/ Projects approved in the least 5 years

--Main coordinator of the ANR Project "LAREDA"(2007-2010) funded by the French ANR.

8/ Publications

8.1 –**Most important publications in the last 5 years related to the project theme**

[1] Brigitte Vallée. Euclidean Dynamics, Discrete and Continuous Dynamical Systems, 15 (1) May 2006, pp 281-352

[2] Loick Lhote, Brigitte Vallée, Gaussian laws for the main parameters of the Euclid Algorithms, Algorithmica (2008) 50 pp 497–554

[3] Julien Clément et Loïck Lhote, Entropy for dynamical sources International Conference on Applied Probability (IWAP 08), 6p.

[4] Brigitte Vallée, Antonio Vera, Probabilistic behaviour of lattice reduction algorithms, Comptes- Rendus du Colloque LLL+25, pp 128–169, chapter of the book ''The LLL Algorithm", collection "Information Security & Cryptography series" (2009) pp 55–125.

[5] Brigitte Vallée, Julien Clément, James Allen Fill, Philippe Flajolet., The Number of Symbol Comparisons in QuickSort and QuickSelect, S. Albers et al. (Eds.): ICALP 2009, Part I, LNCS 5555, pp. 750-763, 2009.

[6] Manfred Madritsch and Brigitte Vallée, Modelling the LLL algorithm by sandpiles, Conference LATIN 10, LNCS 6034 (2010) pp 267–281

[7] Philippe Flajolet, Mathieu Roux and Brigitte Vallée, Digital trees and memoryless sources: from arithmetics to analysis, Proceedings of AofA'10, DMTCS, proc AM, pp 231–258 (2010)

[8] Mathieu Roux and Brigitte Vallée, Information theory: Sources, Dirichlet series, and realistic analysis of data structures, Proceedings of Words, 11, Volume 63 of Electronic Proceedings of Theoretical Computer Science, pp 199-214 (2011)

[9] Eda Cesaratto, Brigitte Vallée, Hausdorff dimension of real numbers with bounded digit averages, Acta Arithmetica 125 (2006), pp 115-162

[10] Eda Cesaratto, Alain Plagne and Brigitte Vallée, On the non-randomness of modular arithmetic progressions: a solution to a problem by V. I. Arnold, Proceedings of the Colloquium on Mathematics and Computer Science: Algorithms, Trees, Combinatorics and Probability, pp 271–288, DMTCS, 2006.

[11] Eda Cesaratto, Julien Clément, (Benoît) Daireaux, (Loïck) Lhote, Véronique Maume-Deschamps and Brigitte Vallée Regularity of the Euclid Algorithm. Application to the analysis of fast gcd Algorithms, in Journal of Symbolic Computation 44(7): 726-767 (2009).

[12] Eda Cesaratto, Brigitte Vallée, Small quotients in Euclidean Algorithms, Ramanujan Journal, 24 (2011), pp 183–218

[13] Eda Cesaratto, Brigitte Vallée, Pseudo-randomness of a random Kronecker sequence, Proceedings of LATIN 2012, LNCS.

8.2 – Publications in cooperation with the project partners: [2, 3 ,5 ,6 ,9, 10,11,12, 13]

9/ Theses oriented and post-doctoral fellows supervised

9.1 – Finished/defended in the last 5 years

Theses.

[1] Loick Lhote (2002-2006) « Gcd Algorithms and mining data algorithms : the point of view of dynamical analysis ».

[2] Antonio Vera (2005-2009) : « Analyses of the Gauss Algorithm. Applications to the analysis of the LLL Algorithm »

[3] Mathieu Roux (2007-2011) « Information Theory, Dirichlet series and analysis of algorithms ». jointly supervised with Driss Essouabri par Driss Essouabri, (Saint-Etienne).

Post-doctoral fellows supervised: Manfred Madritsch (during the ANR Project Lareda)

9.2 – Ongoing

[1] Mariya Georgieva has begun a PhD Thesis in 2009 « Probabilistic analysis of cryptographic lattices » (joint supervision with Julien Clément and Loïck Lhote)

[2] Nguyen Thi, Thu Hien has begun a PhD Thesis in 2010 « Realistic analysis of sorting and searching algorithms » (joint supervision with Julien Clément).

[3] Kanal Hun has begun a PhD Thesis in 2011 « Analysis of digital search trees on general sources »

Valérie Berthé (LIAFA, Paris) –Associate to GREYC (Caen)

1/ **Personal data**

Name: Berthé, Valérie **Birth date**: 16/12/1968

Professional address :

LIAFA Laboratory, Université Paris Diderot Paris 7 – Case 7014 F-75205 Paris Cedex 13--Phone: 33 (0)1 57 27 93 35

email: berthe@liafa.jussieu.fr

Current job title and size of the research group:

Full time researcher ``Directrice de Recherches'' (DR) at the ``Centre National de la Recherche Scientifique'' (CNRS): member of the LIAFA (Laboratoire d'Informatique Algorithmique: Fondements et Applications) (60 permanent, 110 people in total)

2/ **Highest obtained degree (with indication of place and date)**

1999: Habilitation à diriger des recherches, Univ. Aix-Marseille II "Etude arithmétique et dynamique de suites algorithmiques"

3/ **Professional activity – Last 5 years :**

CNRS researcher at LIRMM (Montpellier), and then since Feb 2010, at LIAFA (Paris 7).

4/ Other duties/ positions – Last 5 years

Vice-director of the Fondation Sciences Mathématiques de Paris, since 10/ 2011.

7/ Projects approved in the least 5 years

-- Co-coordinator of the ANR project LAREDA: Lattice Reduction Algorithms: Dynamics, Probabilities, Experiments, Applications

-- Member of the ANR Project Subtile: Substitutions and tilings

-- Member of the ANR Project Kidico: Knowledge Integration for Digital convolution, Image Segmentation and Measurement.

8/ Publications

8.1 –**Most important publications in the last 5 years related to the project theme**

[1] V. Berthé, T. Jolivet, A. Siegel, Substitutive Arnoux-Rauzy sequences have pure discrete spectrum, Uniform distribution theory, 7 (2012) 173-197.

[2] V. Berthé, A. Lacasse, G. Paquin, X. Provençal A study of Jacobi-Perron boundary words for the generation of discrete planes, Theoret. Comput. Sci., to appear.

[3] V. Berthé, Numeration and discrete dynamical systems, Computing, 94 (2012) 369--387.

[4] V. Berthé, Multidimensional Euclidean algorithms, numeration and substitutions, Integers 11B (2011) A2.

[5] V. Berthé, About thin arithmetic discrete planes, Theoret. Comput. Sci. 412 (2011) 4757-4769.

[6] V. Berthé, S. Labbé, An Arithmetic and Combinatorial Approach to three-dimensional Discrete Lines, DGCI 2011, Lecture Notes in Computer Science 6607 Springer (2011) 47--58.

[7] V. Berthé, T. Fernique, Brun expansions of stepped surfaces, Discrete Mathematics 311 (2011) 521-543.

[8] V. Berthé, A. Siegel, P. Surer, W. Steiner, J. Thuswaldner, Fractal tiles associated with shift radix systems, Advances in Mathematics 226 (2011) 139--175.

[9] V. Berthé, M. Rigo, Combinatorics, Automata and Number Theory, V. Berthé, M. Rigo (Eds), Encyclopedia of Mathematics and its Applications 135, Cambridge University Press (2010).

-- V. Berthé, M. Rigo, Introduction

– V. Berthé, M. Rigo, Preliminaries (Chapter 1),

-- V. Berthé, A. Siegel, J. Thuswaldner, Substitutions, Rauzy fractals, and tilings (Chapter 5),

[10] V. Berthé Arithmetic discrete planes are quasicrystals DGCI 09 LNCS 5810 (2009), 1--12.

[11] V. Berthé, L. Imbert, Diophantine approximation, Ostrowski numeration and the double-base number system, Discrete Mathematics & Computer Science, 11 (2009).

[12] V. Berthé, N. Nakada, R. Natsui, Asymptotic behavior of the number of solutions for non-Archimedean Diophantine approximations with restricted denominators, Finite Fields and their Applications 14 (2008), 849--866.

8.2 – Publications in cooperation with the project partners

[1] V. Berthé, L. Lhote, B. Vallée, Dynamical Analyses of some continued fraction algorithms in higher dimensions, in preparation

9/ Theses oriented and post-doctoral fellows supervised

9.1 – Finished/defended in the last 5 years

Theses:

[1] T. Fernique (now full time researcher CNRS),

[2] G. Delalleau

[3] S. Labbé (now postdoctorant).

Post-doctoral fellows supervised:

A. Lacasse, X. Provençal, A Novocin**.**

9.2 – Ongoing

[1] T. Jolivet has begun a PhD Thesis in 2009.

Antonio Cafure (UNGS-Buenos Aires)

1/ **Personal data**

Name: Cafure, Antonio **Birth date**: 28/01/1970

Professional address :

National University of General Sarmiento. Instituto del Desarrollo Humano– J. M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Bs. As, Arg. -- Phone: +54 11 44 69 77 24

email: acafure@ungs.edu.ar

Current job title and size of the research group:

Member of the GIGA group (research group in geometry and arithmethics) (four permanent members and 3 Ph. D. students)

2/ **Highest obtained degree (with indication of place and date)**

Ph. D. Thesis at the University of Buenos Aires (Argentina) 2006.

3/ **Professional activity – Last 5 years :**

Conicet researcher at National University of Gral. Sarmiento (Argentina) and adjoint professor

7/ Projects approved in the least 5 years

Member of the following projects

March 2010-February 2012, Algoritmos eficientes en geometría y aritmética, Conicet. Director: G. Matera.

2007 – 2011 Algoritmos eficientes para problemas de geometría y aritmética. IDH. Instituto de Desarrollo Humano. Universidad de Gral. Sarmiento. Director: G. Matera

8/ Publications

8.1. Most important publications in the last 5 years related to the project theme

[1] A. Cafure, G. Matera and M. Privitelli. Singularities of symmetric hypersurfaces and Reed-Solomon codes. Advances in Mathematics of Communication, 6 (1): 69-94,

[2] A. Cafure and G. Matera. Fast computation of a rational point of a variety over a finite field. Mathematics of Computation, 75 (256): 2049-2085, 2006.

[3] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. Finite Fields and Their Applications, 12 (2): 155-185, 2006.

[4] A. Cafure, G. Matera and A. Waissbein. Inverting bijective polynomial maps over finite fields. En G. Seroussi and A. Viola, editores, Proceedings of the 2006 Information Theory Workshop, ITW2006 (Punta del Este, Uruguay, Marzo 13-17, 2006), páginas 27--31. IEEE Information Theory Society, 2006.

8.2 – Publications in cooperation with the project partners

9/ Theses oriented and post-doctoral fellows supervised

9.1 – Finished/defended in the last 5 years

Melina Privitelli. Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires. Master Thesis in Mathematics, 30th march 2009.

Julien Clément (GREYC, Caen)

1/ **Personal data**

Name: Clément, Julien **Birth date**: August 19, 1972

Professional address :

Laboratoire GREYC (UMR CNRS 6072), Campus Côte de Nacre, Boulevard du Maréchal Juin, BP 5186 - 14032 Caen CEDEX

FAX: +33 (0)2 31 56 73 30 - Office: S3-393A -Telephone: +33 (0)2 31 56 74 09

email: Julien.Clement@unicaen.fr

Current job title and size of the research group:

CNRS full-time researcher (Chargé de recherche) at GREYC (about 120 permanent members)

2/ **Highest obtained degree (with indication of place and date)**

Habilitation Thesis, December 12, 2012, Université de Caen, France. (In French "Habilitation à diriger des recherches").

3/ **Professional activity – Last 5 years :**

Full-time CNRS researcher at GREYC (chargé de recherches)

6/ **Ongoing funded research projects with dates, titles, sources of funding**

– Member of the ANR Project BOOLE" (2010-2013) funded by the French ANR (Agence nationale de la recherche)

7/ **Projects approved in the least 5 years**

– Member of the ECOS Sud Project (exchange project with Uruguay), "Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en criptografía y Teoría de la Información" 2008-2011 funded by the French ministry of foreign affairs.

– Member of the ANR Project "LAREDA" (2007-2010) funded by the French ANR.

8/ Publications

8.1 –**Most important publications in the last 5 years related to the project theme**

[1] Brigitte Vallée, Julien Clément, James Allen Fill, Philippe Flajolet., The Number of Symbol Comparisons in QuickSort and QuickSelect, S. Albers et al. (Eds.): ICALP 2009, Part I, LNCS 5555, pp. 750-763, 2009.

[2] Eda Cesaratto, Julien Clément, (Benoît) Daireaux, (Loïck) Lhote, Véronique Maume-Deschamps and Brigitte Vallée Regularity of the Euclid Algorithm. Application to the analysis of fast gcd Algorithms, in Journal of Symbolic Computation 44(7): 726-767 (2009).

8.2 – Publications in cooperation with the project partners

[1] Julien Clément, Philippe Flajolet, Brigitte Vallée, Dynamical Sources in Information Theory: A General Analysis of Trie Structures, - In Algorithmica (2001) 29:307-369. Springer-Verlag. (INRIA Research report version, 61 pages).

[2] Julien Clément, Philippe Flajolet, Brigitte Vallée, The Analysis of Hybrid Trie Structures- In Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (Philadelphia, 1998), pp. 531-539. SIAM Press, Philadelphia, PA, 1998. (INRIA Research report version).

Submitted.

[3] Frédérique Bassino, Julien Clément, Gadiel Seroussi, Alfredo Viola., Optimal prefix codes for pairs of geometrically-distributed random variables. (38 pages, submitted to IEEE Transactions on Information Theory, 2010).

9/ Theses oriented and post-doctoral fellows supervised

9.2 – Ongoing

[1] Mariya Georgieva has begun a PhD Thesis in 2009 "Probabilistic analysis of cryptographic lattices" (joint supervision with Brigitte Vallée and Loïck Lhote)

[2] Nguyen Thi, Thu Hien has begun a PhD Thesis in 2010 "Realistic analysis of sorting and searching algorithms" (joint supervision with Brigitte Vallée).

Valérie Girardin (LMNO, associate to GREYC, Caen)

1/ **Personal data**

Name: Girardin Valérie **Birth date**: June 16th 1962

Professional address :

LMNO Laboratoire de Mathématiques Nicolas Oresme) Université de Caen Basse Normandie, UCBN BP5186 14032 Caen France Telephone: 33-0-231567468

email: valerie.girardin@unicaen.fr

Current job title and size of the research group:

Maître de Conférences (associate professor) at LMNO.

2/ **Highest obtained degree (with indication of place and date)**

Habilitation Thesis, December 2nd 2001 Caen, France (In French "Habilitation à diriger des recherches").

3/ **Professional activity – Last 5 years :**

Maître de Conférences (associate professor) at LMNO

8/ Publications

8.1 – Highlight the most important publications in the last 5 years related to the project

[1] G. Ciuperca and V. Girardin , Estimation of the Entropy Rate of a Countable Markov Chain, Communication in Statistics: Theory and Methods}, V78, pp. 158--164, (2007)

[2] G. Ciuperca, V. Girardin and L. Lhote, Computation and Estimation of Generalized Entropy Rates for Denumerable Markov Chains, IEEE Communications on Information Theory, V57, pp. 4026--4034 (2011)

[3] V. Girardin and Ph. Regnault, On the Estimation of Entropy of Markov Chains, 58th World Statistic Conference ISI 2011, Dublin, (2011)

8.2 – Publications in cooperation with the project partners: see [2]

9/ Theses oriented and post-doctoral fellows supervised

9.1 – Finished/defended in the last 5 years.

Philippe Regnault, September 2008 - November 2011, PhD Thesis "Different Problems linked to the Estimation of the Entropy of a distribution, of a MarkovProcess"

9.2 – Ongoing:

Justine Lequesne since October 2011, PhD Thesis "Entropy and Goodness-of-fit Tests".

Jean-Marie Le Bars (GREYC, Caen)

1/ **Personal data**

Name: Le Bars Jean-Marie **Birth date**: 01/12/1966

Professional address :

Laboratoire GREYC (UMR 6072), Campus Côte de Nacre, Boulevard du Maréchal Juin, BP 5186 - 14032 Caen CEDEX

FAX: +33 (0)2 31 56 73 30 - Office: S3-393A -Telephone: +33 (0)2 31 56 74 09

Email : lebars @unicaen.fr

Current job title and size of the research group:

Maître de conférences (Associate professor) at GREYC (about 120 permanent members)

2/ **Highest obtained degree (with indication of place and date)**

PhD thesis in january 1998, University of Caen

3/ **Professional activity – Last 5 years :**

Maitre de conférences (associate Professor) (1999--), University of Caen Basse-Normandie.

5/ Awards, fellowships and external recognition

International price : Kleene Award for the Best Student Paper « Fragments of Existential Second-Order Logic without 0-1 Laws », LICS 1998, Indianapolis, IN, USA

National price Thesis award: SPECIF 1998 (Accessit of the SPECIF price) (SPECIF is the French Society for Education and Research in CS. It aims at promoting Education and Research in the academic world. Since 1998, SPECIF awards each year three PhD theses in Computer Science.

6/ **Ongoing funded research projects with dates, titles, sources of funding**

– Member of the ANR Project BOOLE (2010-2013) funded by the French ANR (Agence nationale de la recherche)

7/ Projects approved in the least 5 years

– Member of the ECOS Sud Project (exchange project with Uruguay), "Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en criptografía y Teoría de la Información" 2008-2011 funded by the French ministry of foreign affairs.

8/ Publications

8.1 –**Most important publications in the last 5 years related to the project theme**

1] N. Carrasco, J.M Le Bars and A. Viola. Enumerative encoding of correlation- immune Boolean functions. IEEE Information TheoryWorkshop, Paraty, Brésil, 2011.

[2] J-M. Le Bars and A. Viola. Equivalence classes of boolean functions for first- order correlation. 2007 IEEE International Symposium on Information Theory (ISIT 2007).

[3] J-M. Le Bars and A. Viola. Equivalence classes of Boolean functions for first-order correlation. IEEE Transactions on Information Theory, 56 (3), 1247 - 1261, 2010.

8.2 I**n cooperation with the project partners** See [1, 2, 3,]

9/ Theses oriented and post-doctoral fellows supervised

9.1 – Finished/defended in the last 5 years

Cyril Bazin (joint supervision with Jacques Madelaine, GREYC, Caen) (2007--2010)

Loïck Lhote (GREYC, Caen)

1/ **Personal data**

Name: Lhote, Loïck **Birth date**: 03/30/1978

Professional address :

Laboratoire GREYC (UMR 6072), Campus Côte de Nacre, Boulevard du Maréchal Juin, BP 5186 - 14032 Caen CEDEX

FAX: +33 (0)2 31 56 73 30 - Office: S3-387A -Telephone: +33 (0)2 31 56 74 82

email: loick.lhote@unicaen.fr

Current job title and size of the research group:

– Assistant professor (Maître de Conférences) at the Engineering School of Caen (ENSICAEN).

– Research Group in side GREYC Laboratory (about 120 permanent members)

– Research team: AmacC (Algorithmique, Modèles de calcul, Aléa, Cryptographie, Complexité), about 20 members including 15 permanent members

2/ **Highest obtained degree (with indication of place and date)**

PhD Thesis at the University of Caen France (2006)

3/ **Professional activity – Last 5 years :**

Since 2007, Assistant professor (Maître de Conférences) at ENSICAEN.

6/ **Ongoing funded research projects with dates, titles, sources of funding**

– Member of the ANR Project « BOOLE » (2009-2013) funded by the French Agence nationale de la recherche

7/ **Projects approved in the least 5 years**

Member of the ANR Project French ANR Project "LAREDA" (2007-2010) funded by the French ANR.

8/ Publications

8.1 –**Most important publications in the last 5 years related to the project theme**

[1] Manuel Lladser, Loïck Lhote, Towards the asymptotic count of bi-modular hidden patterns under probabilistic dynamical sources: a case study, AofA'12 Conference, Montreal

[2] Gabriela Ciuperca, Valérie Girardin, Loïck Lhote, Computation of Generalized Entropy Rates, IEEE Transactions on Information Theory, V57, pp. 4026-4034 (2011)

[3] Eda Cesaratto, Julien Clément, Benoît Daireaux, Loïck Lhote, Véronique Maume-Deschamps, Brigitte Vallée, Regularity of the Euclid Algorithm. Application to the analysis of fast gcd Algorithms, Journal of Symbolic Computation, 44, 2009, pages 726-767

[4] Loïck Lhote, Brigitte Vallée, Gaussian Laws for the Main Parameters of the Euclid Algorithms, Algorithmica, 50-4, 2008, pages 497-554

[5] Julien Clément, Loïck Lhote, Brigitte Vallée, Entropy for dynamical sources, pages 1-10, Proceedings of IWAP 2008, 2008, Compiègne, France

8.2 – Publications in cooperation with the project partners See [2, 3, 4, 5]

9/ Theses oriented and post-doctoral fellows supervised

9.2 – Ongoing

[1] Mariya Georgieva has begun a PhD Thesis in 2009 "Probabilistic analysis of cryptographic lattices" (joint supervision with Brigitte Vallée and Julien Clément)

Guillermo Matera (UNGS-Buenos Aires)

1/ **Personal data**

Name: Matera, Guillermo **Birth date**: 13/05/1965

Professional address :

National University of General Sarmiento. Instituto del Desarrollo Humano– J. M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Bs. As, Arg. -- Phone: +54 11 44 69 77 24

email: gmatera@ungs.edu.ar

Current job title and size of the research group:

Director of the GIGA group (research group in geometry and arithmethics) (four permanent members and 3 Ph. D. students)

2/ **Highest obtained degree (with indication of place and date)**

Ph. D. Thesis at the University of Buenos Aires (Argentina) 1999.

3/ **Professional activity – Last 5 years :**

Conicet researcher at National University of Gral. Sarmiento (Argentina) and associate professor

7/ Projects approved in the least 5 years

Coordinator of the following projects

March 2010-February 2012, Algoritmos eficientes en geometría y aritmética, Conicet.

2007 – 2011 Algoritmos eficientes para problemas de geometría y aritmética. IDH. Instituto de Desarrollo Humano. Universidad de Gral. Sarmiento.

8/ Publications

8.1–**Most important publications in the last 5 years related to the project theme**

[1] A. Cafure, G. Matera and M. Privitelli. Singularities of symmetric hypersurfaces and Reed-Solomon codes. Advances in Mathematics of Communication, 2012, 6 (1): 69-94.

[2] N. Giménez, J. Heintz, G. Matera, P. Solernó. "Lower complexity bounds for interpolation algorithms". J. Complexity 27(2), 2011, 151-187.

[3] A. Cafure and G. Matera. Fast computation of a rational point of a variety over a finite field. Mathematics of Computation, 75 (256): 2049-2085, 2006.

[4] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. Finite Fields and Their Applications, 12 (2): 155-185, 2006.

Submitted papers

[5] E. Cesaratto, E., J. von zur Gathen and G. Matera, The number of reducible space curves over a finite field, submitted to Journal of Number Theory.

8.2 – Publications in cooperation with the project partners

9/ Theses oriented and post-doctoral fellows supervised

9.1 – Finished/defended in the last 5 years

A. Cafure, "Rational points on varieties over finite fields. Estimates, algorithms and applications". University of Buenos Aires, 25.8.06.

E. Dratman, "Efficient algoritmos for certain systems derived from differential equations". University of Buenos Aires, 18.8.10.

9.2 Ongoing thesis

Mariana Pérez (UNGS) "Probabilistic algorithms for searching rational roots of polynomial systems over finite fields", since 2011.

Melina Privitelli (UNGS) "Existence and number of rational solutions of polynomial systems over finite fields. Applications" since 2010.

C. Project Budget

Project title: Advances in Analytic Combinatorics: dynamical combinatorics, and applications to number theory, information theory and cryptography.

Participating institutions: Université de Caen Basse-Normandie (France), CNRS (France); Universidad de la República (Uruguay), Universidad Nacional de General Sarmiento (Argentina)

The STIC-AmSud program **funds travel expenses** (air tickets and *per diem*) to researchers in research missions and workshops.

General remarks.

The expenses of this project are important. There are 16 people involved. The call for proposals stress out the importance of general meetings, so we plan two of those per year (one in France and one in South America). We think it will strengthen collaboration in STIC between the three countries (Uruguay, Argentina, and France).

Also, we feel it is important that students attend to all meetings so that they are really involved in the project from the beginning.

Extra funding.

Eda Cesaratto and Brigitte Vallée are planning to apply to the IFUM (Instituto Franco Uruguayo de Matemáticas) call for activities within its framework for the second half of the year 2012 and the first half of the year 2013. For instance, travel expenses for Brigitte Vallée and Valérie Berthé could be taken in charge in this context (2 400€ each year will be asked).

The GREYC members (France) plan to fund some longer stays in France with the financial support of the GREYC lab and some of the projects of the ANR they are involved in (1 500 € each year).

Some funding will be asked also to the INFINIS CNRS Laboratory in Buenos Aires.

Other complimentary sources will be searched in Uruguay, for example in Pedeciba, or programa 720 if applicable.

C1. First year (2013)

Planned missions – Year 1

Mission description. Goals and participants.

Kick-off meeting in Uruguay: February/March 2013. One of our main goals is to consolidate strong research collaborations between different research groups. Even though they have already strong bilateral collaborations, they have never worked altogether as a group. For this reason it is important to have a first meeting at the very beginning of the project.

There will be mainly plenary talks to share the main subjects (each member has to learn in the subjects of the others), but also small working groups, more centered on a precise subject of the project. With the conclusions of the working group and the plenary talk, a detailed scientific plan of activities will be produced. We expect that new connections between themes

and methods become apparent and be able to start some news collaborations in specific problems inside of the subjects of research of this project.

Also, it is an excellent opportunity to strengthen collaboration and coordinate this project with the CNRS Lab IFUM in Uruguay.

We plan a longer stay for those researchers from different countries who already have work in progress or with a specific problem already delimited.

–Brigitte Vallée and Eda Cesaratto, see Sections 2.1 and 2.2 of the General Description.

–Jean-Marie Le Bars, Julien Clément and Alfredo Viola, see 4.2

–Valérie Berthé, Brigitte Vallée and Alfredo Viola and UNGS team, see 2.4. and 2.5.

Ideally, all the members of the project should attend this meeting. This means that 11 people, 8 from France and 5 from Argentina should travel to Uruguay.

Other missions.

Meeting in France: September/October

Eda Cesaratto (Argentina) and Alfredo Viola (Uruguay) plan to travel to France for a stay of 20 to 30 days.

The plan for this meeting is the following:

Eda Cesaratto, Loick Lhote and Brigitte Vallée will work in the specific objective described in Section 1.4.

Eda Cesaratto, Brigitte Vallée, completion of 2.1 and continuation/completion of 2.2.

Valérie Berthé, Eda Cesaratto, Loïck Lhote and Brigitte Vallée will work on 2.3.

Julien Clément, Loick Lhote, Brigitte Vallée, Thu Hien Nguyen Thi, Kanal Hun, Valérie Girardin, Alfredo Viola and Eda Cesaratto will work in specific objectives described in 3.

Alfredo Viola, Julien Clément, Jean-Marie Le Bars, Loïck Lhote and Brigitte Vallée will work on the specific project described in section 4.

Again we believe that it is important for students to be an active part of the project. That is why we plan that three students from South America will travel to France and work with the confirmed researchers of the project.

Planned missions – Year 1

Evaluated costs per day for welcoming institutions: CNRS 100 €/day, MINCYT: 60€/day, ANII:77€/day

Researcher	Status (student, junior, senior)	Institution	Origin	Destination	Planned date	Duration (max. 30d)	Estimated cost of the trip (€)	Trip funding institution[1]	Estimate of total *per diem* (€)	Mission funding institution (*per diem*)[2]	Mission objectives
Berthé, Valérie	senior	LIAFA, CNRS, U. Paris 7	Paris	Montevideo+ Buenos-Aires	February/ March	10	1100 €	IFUM	600 €	ANII	Kick-off meeting
Clément, Julien	senior	GREYC, CNRS, U. Caen	Caen	Montevideo	February/ March	10	1100 €	CNRS	600 €	ANII	Kick-off meeting
Girardin, Valérie	senior	LMNO, CNRS, U. Caen	Caen	Montevideo	February/ March	10	1100 €	CNRS	600 €	ANII	Kick-off meeting
Hun, Kanal	Student	GREYC, CNRS, U. Caen	Caen	Montevideo	February/ March	10	1100 €	CNRS	600 €	ANII	Kick-off meeting
Le Bars, Jean-Marie	senior	GREYC, CNRS, U. Caen	Caen	Montevideo	February/ March	10	1100 €	CNRS	600 €	ANII	Kick-off meeting
Lhote, Loïck	senior	GREYC, CNRS, U. Caen	Caen	Montevideo	February/ March	10	1100 €	CNRS	600€	ANII	Kick-off meeting
Thu Hien, Nguyen Thi	Student	GREYC, CNRS, U. Caen	Caen	Montevideo	February/ March	10	1100 €	CNRS	600 €	ANII	Kick-off meeting
Vallée, Brigitte	senior	GREYC, CNRS, U. Caen	Caen	Montevideo+ Buenos Aires	February/ March	10	1100 €	IFUM	600 €	ANII	Kick-off meeting
Cesaratto, Eda	senior	UNGS	Buenos-Aires	Montevideo	February/ March	10	100 €	MINCYT	600 €	ANII	Kick-off meeting
Cafure, Antonio	senior	UNGS	Buenos-Aires	Montevideo	February/ March	10	100 €	MINCYT	600 €	ANII	Kick-off meeting
Matera, Guillermo	senior	UNGS	Buenos-Aires	Montevideo	February/ March	10	100 €	MINCYT	600 €	ANII	Kick-off meeting
Pérez, Mariana	Student	UNGS	Buenos-Aires	Montevideo	February/ March	10	100 €	MINCYT	600 €	ANII	Kick-off meeting
Privitelli, Melina	Student	UNGS	Buenos-Aires	Montevideo	February/ March	10	100 €	MINCYT	600 €	ANII	Kick-off meeting
Viola, Alfredo	senior	UdelaR	Montevideo	Caen	Sept./Oct.	10	1100 €	ANII	800 €	CNRS	meeting
Carrasco, Nicolas	Student	UdelaR	Montevideo	Caen	Sept./Oct.	10	1100 €	ANII	800 €	CNRS	meeting
Cesaratto, Eda	senior	UNGS	Buenos-Aires	Caen	Sept./Oct.	10	1100 €	MINCYT	800 €	CNRS	meeting
Matera, Guillermo	senior	UNGS	Buenos-Aires	Caen	Sept./Oct.	10	1100 €	MINCYT	800 €	CNRS	meeting
Privitelli, Melina	Student	UNGS	Buenos-Aires	Caen	Sept./Oct.	10	1100 €	MINCYT	800 €	CNRS	meeting

1 Each institution will pay for the trip of its own researchers.
2 Expenses for per diem will be paid by welcoming institution.

CONSOLIDATED BUDGET: Year 1

Funding requested to the STIC-AmSud Program

Estimated costs (€)

	MAEE France	**CNRS France**	**INRIA France**	**Institut TELECOM France**	**MINCYT Argentina**	**CAPES Brazil**	**CONICYT Chile**	**CONACYT Paraguay**	**CONCYTEC Peru**	**ANII Uruguay**	**Total requested funding to STIC-AmSud**	**Other funding**	**TOTAL**
A- Travel costs (air tickets)		**6600€**			**3800 €**					**2 200 €**	**12600 €**	**2 200 €**	**14800 €**
B- Maintenance costs (*per diem)*		**4000 €**			**0 €**					**10000 €**	**11800 €**	**1.500 €**	**13300 €**

See Page 46 for more information on other funding.

C2. Second year (2014)

Second year funding depends on approval of intermediate progress report.

Planned missions – Year 2

Mini-school in Argentina (February/march 2014) One of the main goals of this activity is to contribute to the scientific background of students Nicolás Carrasco, Fernando Fernández (UdelaR) Thu Hien Nguyen Thi, Kanal Hun (GREYC), Mariana Pérez and Melina Privitelli (UNGS). Another goal is to interact with the School of Science and Technology of UNGS and bring other students from other parts of Argentina and Uruguay. We hope to have more graduate and advance undergraduate students for the region participating in the school, since we think it will be an excellent opportunity to introduce new students to these type of problems and the methodology used to analyze them. Courses will be given by Brigitte Vallée, Julien Clément, Jean-Marie Le Bars, Loïck Lhote (GREYC) and Alfredo Viola (UdelaR).

After the school, different working groups will advance or complete specific projects 2.4, 2.5, 3 and 4.
Again, missions from the french partners will help to strengthen the relation with the CNRS Lab in Buenos Aires.

Second small meeting in France (September/October 2014): Eda Cesaratto and Alfredo Viola travel to France in September/October. In this mission, Julien Clément, Valérie Girardin, Loïck Lhote, Brigitte Vallée, Thu Hien NguyenThi, Kanal Hun, Alfredo Viola and Eda Cesaratto plan to advance/complete works related to specific projects described in Section 1 and continue the work about the subjects described in section 3. Alfredo Viola and Jean-Marie Le Bars will continue/complete their work about the subjects described in section 4.

Small meeting in Uruguay (February/march 2014). Julien Clément, Jean-Marie Le Bars, Brigitte Vallée, Valérie Berthé, Eda Cesaratto and one of the other members of GIGA group travel to Uruguay to continue/complete the work on specific projects 2.3, 2.5, 3 and 4 with Alfredo Viola and the Uruguayan students. This small meeting is also intended to strengthen the relation with the CNRS Lab IFUM in Uruguay, and maybe initiate new collaborations.

Planned missions – Year 2

Evaluated costs per day for welcoming institutions: CNRS 100 €/day, MINCYT: 60€/day, ANII:77€/day

Researcher	Status (student, junior, senior)	Institution	Origin	Destination	Planned date	Duration (max. 30d)	Estimated cost of the trip (€)	Trip funding institution[3]	Estimate of total *per diem* (€)	Mission funding institution (*per diem*)[4]	Mission objectives
Berthé, Valérie	senior	LIAFA, CNRS, U. Paris 7	Paris	Buenos-Aires+ Montevideo	February/ March	10	1100 €	IFUM	600 €	MINCYT	Mini-School
Clément, Julien	senior	GREYC, CNRS, U. Caen	Caen	Buenos-Aires+ Montevideo	February/ March	10	1100 €	CNRS	600 €	MINCYT	Mini-School
Girardin, Valérie	senior	LMNO, CNRS, U. Caen	Caen	Buenos-Aires	February/ March	10	1100 €	CNRS	600 €	MINCYT	Mini-School
Hun, Kanal	Student	GREYC, CNRS, U. Caen	Caen	Buenos-Aires	February/ March	10	1100 €	CNRS	600 €	MINCYT	Mini-School
Le Bars, Jean-Marie	senior	GREYC, CNRS, U. Caen	Caen	Buenos-Aires +Montevideo	February/ March	10	1100 €	CNRS	600 €	MINCYT	Mini-School
Lhote, Loïck	senior	GREYC, CNRS, U. Caen	Caen	Buenos-Aires	February/ March	10	1100 €	CNRS	600 €	MINCYT	Mini-School
Thu Hien, Nguyen Thi	Student	GREYC, CNRS, U. Caen	Caen	Buenos-Aires	February/ March	10	1100 €	CNRS	600 €	MINCYT	Mini-School
Vallée, Brigitte	senior	GREYC, CNRS, U. Caen	Caen	Buenos-Aires+ Montevideo	February/ March	10	1100 €	IFUM	600 €	MINCYT	Mini-School
Viola, Alfredo	senior	UdelaR	Montevideo	Buenos-Aires	February/ March	10	100 €	ANII	600 €	MINCYT	Mini-School
Carrasco, Nicolas	Student	UdelaR	Montevideo	Buenos-Aires	February/ March	10	100 €	ANII	600 €	MINCYT	Mini-School
Fernandez, Fernando	Student	UdelaR	Montevideo	Buenos-Aires	February/ March	10	100 €	ANII	600 €	MINCYT	Mini-School
Cafure, Antonio	senior	UNGS	Buenos-Aires	Caen	Sept./Oct.	10	1100 €	MINCYT	800 €	CNRS	meeting
Viola, Alfredo	senior	UdelaR	Montevideo	Caen	Sept./Oct.	10	1100 €	ANII	800 €	CNRS	meeting
Carrasco, Nicolas	Student	UdelaR	Montevideo	Caen	Sept./Oct.	10	1100 €	ANII	800 €	CNRS	meeting
Cesaratto, Eda	senior	UNGS	Buenos-Aires	Caen	Sept./Oct.	10	1100 €	MINCYT	800 €	CNRS	meeting
Pérez, Mariana	Student	UNGS	Buenos-Aires	Caen	Sept./Oct.	10	1100 €	MINCYT	800 €	CNRS	meeting

3 Each institution will pay for the trip of its own researchers.

4 Expenses for per diem will be paid by welcoming institution.

CONSOLIDATED BUDGET: Year 2

Funding requested to the STIC-AmSud Program

Estimated costs (€)

	MAEE France	**CNRS France**	**INRIA France**	**Institut TELECOM France**	**MINCYT Argentina**	**CAPES Brazil**	**CONICYT Chile**	**CONACYTParaguay**	**CONCYTEC Peru**	**ANII Uruguay**	**Total requested funding to STIC-AmSud**	**Other funding**	**TOTAL**
A- Travel costs (air tickets)		**6600 €**			**3500 €**					**2 500 €**	**12600€**	**2 200 €**	**14800 €**
B- Maintenance costs (*per diem)*		**4400 €**			**6.600 €**					**2 500 €**	**11000 €**	**1.500 €**	**12500 €**

See Page 46 for more information for other funding.

C3. BUDGET TOTALS

	Year 1	Year 2	Total
Funding requested to MAEE (France)			
Funding requested to INRIA (France)			
Funding requested to CNRS (France)	10600 €	11000 €	**21600 €**
Funding requested to Institut TELECOM (France)			
Funding requested to MINCYT (Argentina)	3800 €	10 100 €	**13900 €**
Funding requested to CAPES (Brazil)			
Funding requested to CONICYT (Chile)			
Funding requested to CONACYT (Paraguay)			
Funding requested to CONCYTEC (Peru)			
Funding requested to ANII (Uruguay)	10000 €	2500 €	**12500 €**
Matching funds from the partners	1.500 €	1.500 €	**3.000 €**
Other sources (IFUM)	2 200 €	2 200 €	**4 400 €**
TOTAL	**28100 €**	**27300 €**	**55400 €**

[1] Each institution will pay for the trip of its own researchers.

[2] Expenses for per diem will be paid by welcoming institution.