Scientific report, BOOLE project

September 2009 – August 2013

Danièle Gardy with members of the BOOLE project

October 31, 2013

1 F1: Circuits and Boolean Normal Forms.

This axis is centered on representations of boolean functions and extensions thereof.

1.1 Boolean circuits.

Nadia Creignou collaborated with Heribert Vollmer and other researchers of Hannover University (Germany) on various algorithmic problems on boolean circuits, such as the equivalence of two circuits, or the enumeration of all the solutions of a circuit. They were able to obtain a complete classification of these problems according to the type of gates, and to exhibit efficient algorithms for several sets of types of gates. They also showed that, for the other sets of gates, theses problems are at least NP-hard [8]. Finally, they studied similar questions for the satisfiability problem and parametrized complexity [34].

1.2 Representation of booleans and integers.

Jean Vuillemin has focussed his work on Strong Normal Forms for large Integers, Boolean functions and finite Automata, with applications to circuits and software verification and synthesis. He has written [56] a primer on Boolean functions for Engineering Sciences, which also extends the classical Decision Diagrams to handle efficient integer representations and operations. It allows to efficiently perform arithmetic operations on gigantic integers, as long as they remain sparse. Other results show that XOR non-deterministic Automata can be efficiently minimized and automatically processed. The situation is different from classical OR non-deterministic Automata where testing for equality and minimization are exponential time operations. This new branch of computational automata theory is further explored for general regular languages (paper submitted for publication). The special case of finite languages (i.e. Boolean functions) is detailed in a recently submitted paper which showed that: (i) the ordered dimension of a Boolean function is a lower bound on the size of ordered

Decision Diagrams; (ii) minimal dimension diagrams can be efficiently built and operated upon.

1.3 Arithmetic circuits and counting.

Hervé Fournier has also extended the initial framework of boleean circuits, to arithmetic ones and to questions about counting; this pertains to algebraic complexity and representation of polynomials by arithmetic circuits.

In collaboration with Guillaume Malod (Univ. Paris 7) and Stefan Mengel (Univ. Paderborn, Germany), he studied the complexity of two questions on such a representation of polynomials: checking whether a monomial is present, and counting monomials. Various classes of circuits lead to problems which are complete for sub-classes of the counting hierarchy [45].

He then turned to the question of obtaining polynomial lower bounds on the size of complex arithmetic circuits for uniform polynomials. For any constant k, it was possible to build circuit-less polynomials without circuits of size n^k, and whose coefficients belong to the class MA, or which can be evaluated at the integer points of the class AM. Finally, he studied the relation between fixed polynomial lower bounds in the boolean and arithmetic frameworks. This research was carried out in collaboration with S. Perifel (Paris 7) and R. de Verclos (ENS Lyon) [46].

1.4 Random circuits.

Nicolas Broutin has been interested in the shape of a class of random circuits, and has been able to give precise results on the length of paths (both typical and non-typical) between incoming and output gates (collaboration with O. Fawzi, McGill Univ., Canada) [10].

2 F2: Boolean Functions and Cryptography.

This axis is about classification and building of boolean functions.

2.1 Bent and hyperbent functions.

Bent functions and o-polynomials. Claude Carlet and Sihem Mesnager [18] established a connection between the class called H introduced by J. Dillon in his thesis, the bent functions constructed via Niho power functions by Dobbertin et al., and the o-polynomials well-known in finite geometry. This has enabled them to deduce a large number of new infinite classes of bent functions in trace forms from the connection with o-polynomials; this has also answered an open question raised in 2006 by Dobbertin et al., by explicitely calculating the dual of one of these functions.

They have shown [19] that any Boolean function in even dimension, which is equal to the sum of a Boolean function g constant on each element of a spread

and of a Boolean function h whose restrictions to these elements are all linear, is semi-bent if and only if g and h are both bent; they deduced from this result a large number of infinite classes of semi-bent functions in explicit bivariate (resp. univariate) polynomial form. In collaboration with L. Budaghyan, T. Helleseth and A. Kholosha [15] they computed the dual of the Niho bent function consisting of 2^r exponents that was found in 2006 by Leander and Kholosha.

With F. Zhang and Y. Hu, C. Carlet showed in [20] how to design the initial functions in the Rothaus construction, using Boolean permutations and orthomorphic permutations. These authors also presented a new secondary construction of bent functions which generalizes the Rothaus construction, and requires initial functions with stronger conditions. Finally, C. Carlet has obtained the first example of an infinite class of nonquadratic rotation symmetric bent functions, in a collaboration with G. Gao, X. Zhang and W. Liu [47].

Sihem Mesnager has also contributed more deeply to the study on the connection between bent functions from the class H, Niho bent functions, and the oval polynomials, in the continuation of her work with C. Carlet mentioned above. Indeed, in a joint work with T. Helleseth and A. Kholosha [51] she has studied the first binomial Niho bent function discovered by Dobbertin et al., and showed that the relation between those Niho bent functions and the o-polynomials give rise to Subiaco class of hyperovals. This allowed her to expand the original class of bent functions in some cases, and to derive new bent functions. In the same paper, the three authors studied the relation between the second binomial Niho bent function discovered by Dobbertin et al. and o-polynomials, and showed that those bent functions give rise to the Adelaide classes of hyperovals.

Hyperbent functions. Sihem Mesnager, in a collaboration with J.P. Flori [54], was interested in the generalization of all the hyper-bent functions with multiple trace terms (including binomial functions) via Dillon-like exponents. They have shown how the approach developed in former papers fits into a much more general setting, and presented generalizations of previous approaches in different directions. To this end, firstly they have observed that the original restriction for Charpin–Gong criterion can be weakened. Afterwards they tackled the problem of devising infinite families of extension degrees for which a given exponent is valid and applied these results not only to give a new, straightforward proof of results previously appearing in the literature, but also to characterize the hyper-bentness of several potentially new infinite classes of Boolean functions. Finally, they also provided an algorithm and the corresponding software to extend this approach to an infinity of other new families.

Exponential sums. The connection between exponential sums and algebraic varieties has been known for at least six decades. Connecting exponential sums and numbers of points on algebraic varieties is classical folklore. Such ideas go back, at least, to the work of Weil where the Riemann hypothesis is used to bound the values of Kloosterman sums. Leonard and Williams then devised the

connection between Kloosterman sums and elliptic curves, and Lachaud and Wolfmann exploited the theory of elliptic curves to study the distribution of Kloosterman sums. In 2011, Lisonk followed this approach to reformulate the Charpin-Gong characterization of a large class of hyper-bent functions in terms of numbers of points on hyper-elliptic curves. As a consequence, he obtained a polynomial time and space algorithm for certain subclasses of functions in the Charpin-Gong family. In the line of these works, Sihem Mesnager was heavily involved in the connection between exponential sums and special functions: bent/hyper-bent functions and semi-bent functions. She showed, in collaboration with J.P. Flori [53, 42], how to transform the characterizations of bentness and semi-bentness in terms of hyper-elliptic curves, providing an analysis of the asymptotic complexity of the generation of hyper-bent and semi-bent functions, experimental results for their practical generation, and some practical and theoretical applications.

2.2 Boolean functions and attacks.

Algebraic attacks. Claude Carlet has continued his research on Boolean functions suitable for stream ciphers. In collaboration with X. Zeng, L. Hu and J. Shan [57], he obtained three constructions of balanced Boolean functions with optimal algebraic immunity and analysed their good algebraic degree, non-linearity, and behaviour against fast algebraic attacks. With D. Tang and X. Tang [55], he has proposed two infinite classes of balanced Boolean functions with optimal algebraic immunity having maximal algebraic degree and high non-linearity; at least for numbers of variables $n \leq 16$, these functions have a good behaviour against fast algebraic attacks. Compared with the known Boolean functions resisting algebraic attacks and fast algebraic attacks, they possess the highest lower bounds on non-linearity.

Counter-measures to channel attacks. Claude Carlet has also worked in the new domain of research of Boolean functions for counter-measures against side channel attacks (an important emerging domain in cryptography). With J.-C. Faugère, C. Goyet and G. Renault, he presented a theoretical study in order to explain the algebraic phase of the Algebraic Side-Channel Attacks introduced by Renauld, Standaert and Veyrat-Charvillon. They showed that side-channel information leads to effective algebraic attacks and that the complexity of the Gröbner basis computations in these attacks depends on a new notion of algebraic immunity.

With L. Goubin, E. Prouff, M. Quisquater and M. Rivain [17], he introduced the first masking scheme against side channel attacks which can be applied in software. He also worked [52] on the countermeasure of masking, and showed that it can be improved at the first order by manipulating the mask through a bijection F; he showed that dth-order zero-offset attacks, that consist in applying correlation power analysis on the dth power of the centered side-channel traces, can be thwarted for $d \geq 2$ with a single mask. He demonstrated that optimal choices for F relate to binary codes called complementary information set codes

with greatest dual distance, exhibited optimal linear F functions, and showed that for values of n where optimal non-linear codes exist, better non-linear F can be found. In the case $n = 8$, F can be derived from the Nordstrom-Robinson $(16, 256, 6)$ code. This example protects against all zero-offset HO-CPA attacks of order $d \leq 5$. This "leakage squeezing" strategy was then extended to several independent random masks. Another result pertained to a different masking strategy for hardware, called Rotating Substitution boxes Masking (RSM). In this masking scheme, to any mask corresponds a masked substitution box. C. Carlet and S. Guilley proved that there exists such a masking of the AES substitution boxes with 16 masks (hence a number of substitution boxes equal to that of the same algorithm without masking) that resists third-order side-channel attacks. Furthermore, even if the masking set is public, each byte of the correct key is found only ex-aequo with 15 incorrect ones, making the side-channel analysis insufficient alone, allowing both to increase the number of side-channel measurements and to demand for a final non negligible brute-forcing (of complexity 2^{64} for AES).

With P. Gaborit, J.-L. Kim and P. Solé [16], C. Carlet has worked on the binary codes mentioned above, called complementary information set codes, having two disjoint information sets. They have given optimal or best known CIS codes of length < 132, derived general constructions based on cyclic codes and on double circulant codes, and a Varshamov-Gilbert bound for long CIS codes.

Jean Vuillemin also has been concerned with circuit protection; the paper [9] (in collaboration with several authors)presents an approach to circuit protection against side-channel attacks based on a statistical analysis of power traces derived from actual measures of the circuit in operation.

2.3 Method of classes for boolean functions.

This methodology, which is due to J.-M. Le Bars and A. Viola (Montevideo, Uruguay), aims at studying cryptographic properties of boolean functions, by a recursive decomposition of classes which are then easier to enumerate than the full set of functions satisfying the properties. Its initial applications was on 1-resilient functions, and further studies in the BOOLE project were concerned with enumerative coding and random generation (J.-M. Le Bars with A. Viola again and N. Carrasco, Montevideo, Uruguay). The method is suited to the use of the recursive method for enumerative coding and uniform random generation, presented in 1994 by P. Flajolet, P. Zimmermann and B. Van Cutsem. The most challenging question was how to generate efficiently a random function among the 10^{68} 1-resilient functions on 8 variables, and required to develop algorithms which are both time and space-efficient (to avoid the combinatorial explosion of the number of classes).

Another parameter that was considered is the algebraic immunity (J. Clément, A. Genitrini and J.-M. Le Bars,with A. Viola). It has lead to the experimental computing of all the possible dimensions of the vectorial spaces of annulators, up to 4 variables. Finally, a presentation of Alfredo Viola at the final meet-

ing of the project, on correlation-immune functions, raised the possibility of a connexion with a project of Claude Carlet on intelligent cards.

2.4 Dual of monotone boolean functions.

Consider a monotone boolean function, and its expression in conjunctive normal form : what about computing the conjunctive normal form of its dual function? An open problem is whether, in worst case, building the dual belongs to the output-polynomial class (complexity polynomial in the sum of the input and output sizes). L. Lhote, collaborating with F. Rioult (Greyc, Caen), was able to obtain information on the average complexity of this problem.

When the number of variables is fixed but the number of clauses is allowed to vary, it is well known that the problem is probably output-polynomial. But a similar question was open when the numbers of variables and clauses are both fixed, with one of them possibly dependent on the other. Under suitable conditions, Llhote and Rioult have shown, through the analysis of an algorithm, that the problem is output-polynomial, and that the average size of the output is super-polynomial.

3 F3: Satisfiability.

The goal of this axis was a study of satisfiability problems that would mix several different tools: analytic combinatorics, graph theory, and statistical physics.

3.1 Constraint Satisfaction Problems.

Constraint Satisfaction Problems (CSP) stand at the crossroads between probabilities, combinatorics, theoretical computer science and statistical physics. Detailed study of the random expressions appearing in the problem 3Sat, which is maybe the most famous of all NP-complete problems, has uncovered the existence of a critical domain, in which "hard" instances are concentrated. There is a critical threshold for satisfiability in this domain, whose exact value remains an open problem although it has been the object of numerous studies. The wide spectrum of methods represented in the Boole project has provided a fruitful environment for exploring and describing the phase transitions associated to new, alternative boolean expressions. Our methodology has been twofold : to analyse very precisely specific, well structured problems; and to obtain a global view of the landscape of boolean CSPs. Our major goal has been the identification of structures and invariants that lie at the root of transition phenomena.

Sensibility of expressions. A boolean function has a sensibility. Nadia Creignou and Hervé Daudé have adapted this notion to the boolean expressions associated with CSPs. When symmetries allow it, they have shown [32] that enumerating expressions according to their sensibility has direct connexions to sensibility invariants of the constraints that engender these expressions. The

combinatorial expressions they obtain lead to upper bounds for the thresholds of a wide family of boolean CSPs. This result shows how it is possible to derive global results on the behaviour of a CSP, from the local properties of the problem.

Monotone properties of the hypercube. Hervé Daudé and Raphaël Rossignol have considered how the size of the transition window for a monotone property of the hypercube is influenced by symmetries. In the restricted framework of CSPs, their goal was to improve the sharp transition criterion established by Friedgut and Bourgain. They have been able to prove that problems with mixed clauses (i.e. the number of variables is no longer fixed, but remains bounded) can be described through a product of Bernoulli measures with varying parameters.

Quantified expressions. Nadia Creignou, Hervé Daudé and Raphaël Rossignol, joined by Uwe Egly from the T.U. Wien (Austria), have considered the satisfiability of quantified boolean expressions of the type $\forall X \exists \varphi(X, Y)$, where φ is a conjunction of clauses, each of which contains a variable of X and two variables of Y. They have shown that the transition from satisfiability to unsatisfiability is determined by the ratio Number of clauses / Number of existential variables. This has brought to light the cyclic structures that determine the sharp threshold when the number of variables grows. An experimental study of the critical ratio associated with the threshold has allowed the computation of its limiting value.

Generation of random expressions. Nadia Creignou has collaborated further with Uwe Egly, and with Martina Seidl from Johannes Kepler University (Linz, Austria) on building a random generator for expressions, either quantified or not, which are not required to be in normal form [33]. Their system can generate random instances from XML specifications of the desired expressions. A single software can thus generate easily instances of many types, and requires no programmation. The generation of random data is necessary for testing and evaluating solvers dedicated to Sat and Qsat.

MaxCut and 2XorSat. With Conrado Martinez (UPC Barcelone, Espagne), Hervé Daudé, Vonjy Rasendrahasina and Vlady Ravelomanana have studied the maximal number of edges in a cut of a random graph (MaxCut). Through the systematic use of combinatorial analysis technics, as promoted by D. Knuth, P. Flajolet, S. Janson, T. Luczak and B. Pittel, and starting from the methods and results of [36], they have been able to obtain limiting distributions, that are also proof that the core of bipartite graphs is an essential notion for such questions [35]. Élie de Panafieu and Vlady Ravelomanana have worked out a precise description of the threshold associated to a quantified version of 2XorSAt, through the analysis of a family of inhomogeneous graphs through analytic combinatorics [37].

3.2 Algorithms.

Part of the initial research plan on satisfiability was to consider local search algorithms for combinatorial optimisation problems, focussing on the Sat-like problems and using random distributions as benchmarks to evaluate the performance of these algorithms. This was to be carried out by Rémi Monasson, who left France right at the beginning of the project and spent several years at the Institute of Advances Studies in Princeton (USA).

A new line of research was developed by V. Bapst and G. Semerjian. They were concerned with understanding and quantifying exactly the same type of problems, but within a totally different computation model : quantum computing. The quantum adiabatic algorithm, which requires the existence of a quantum computer (similarly to Schor's algorithm for factoring integers), is indeed an all-purposes proposal for solving combinatorial optimisation problems. Bapst and Semerjian, with collaborators, studied its performance on random problems, through an extension of statistical physics methods [3].

3.3 Performance evaluation of a constraint solver.

In early 2010, Danièle Gardy and Charlotte Truchet made preliminary inquiries regarding the evaluation of the performances of a constraint solver; these inquiries lead them to sketch out a new research area, in collaboration with Xavier Lorca (Ecole des Mines de Nantes). Jérémie du Boisberranger was then recruited as a Ph. D. student in September 2010 to carry out this research project. The long-term goal was, through the evaluation of various probabilities that a filtering algorithm does reduce domains of variables, to define and make available tools for avoiding operations that would lead to insufficient reduction of the domains and for optimising the choice of resolution methods. The project began with an in-depth study of the global constraint *AllDifferent;* it was expected that, if successful, the approach would be extended to further constraints. The first phase was about defining a theoretical model that allowed to work out an probabilistic analysis of the performance of the constraint *AllDifferent* [39]. The second phase was concerned with experimental evaluation of several different strategies for solving constraints, and used the constraint solver *Choco/Galak* developed by the Nantes team. It turned out that actually improving on the (already heuristically optimised) solver required very precise tuning. Conversely, our present results can also be seen as providing a mathematical, rigorous proof of heuristics used in the implementation of solvers.

Unfortunately, Jérémie du Boisberranger chose early during the summer of 2012 to switch fields and to stop his thesis, which was a severe setback for the study. Vincent Armant then joined the project for a short period (8 months); the results he obtained have yet to be validated and interpreted.

4 F4: Quantitative Logic.

This axis was about various models for boolean expressions, and the probability distributions they induce on boolean functions.

4.1 Random boolean expressions and tree distributions on boolean functions.

Results on the study and comparison of different models for propositional logic and their expressive power were among the earliest ones of the project [43, 44, 50]. Further results have shown that properties of operators such as associativity and commutativity have a limited influence on the probability distributions on boolean functions: such distributions belong to a family of distributions whose behaviour remains the same (the probability of a boolean function f is given by $P(f) = \frac{\gamma(f)}{n^{L(f)+1}}$, with $L(f)$ the tree complexity of the function and $\gamma(f)$ a constant depending on the function), and the modification of the model is only reflected by a corresponding modification of the parameters.

An interesting result is that, for at least one of these distributions, it was possible to disprove the Shannon effect [48].[1] Working out a similar proof for different models is probably doable, but involves quite intricate computations. Another important result on tree distributions is the possibility to consider an infinite number of boolean variables, or rather a number of variables that grows with the size of the formula.

As regards satisfiability, a recent by-product of the results on tree distributions on boolean functions is that, e.g., And/Or trees, in the setting where the number of variables is proportional to the size of the expression, correspond to expressions which present no threshold transition (the probability of satisfiability tends to 1). The characterization of probability distributions associated to classical satisfiability models has turned out to be quite intricate in the classical cases, for which our present results are limited to the 2XorSat distribution.

4.2 Influence of the growing model for the tree.

Cécile Mailler considered the And/Or and implication models for boolean expressions, but with a twist: the underlying tree is no longer distributed as a Catalan tree, but according to the binary search tree model (this amounts to defining a process where the tree grows at each step by splitting a random leaf into two new leaves) [24, 25]. Although this model may seem quite natural, and leads to rather balanced trees (their average height has order $\log n$), it leads to degenerate distributions on the space of boolean functions: the only functions that get an asymptotic non-zero probability are the constants! When operators and literals are given non-uniform probabilities, the asymptotic distribution on boolean functions will be non-zero for a larger number of functions, although this

[1] The so-called "Shannon effect" is the fact that, for a uniform distribution on the set of all boolean functions on n variables, almost all functions have almost maximal complexity.

number still remains ridiculously small w.r.t. the total number 2^{2^n} of boolean functions on n variables.

4.3 Influence of operator properties.

Antoine Genitrini and Cécile Mailler have led an in-depth study of boolean expressions with associative or commutative operators, in collaboration with Bernhard Gittenberger and Veronika Kraus (both at T.U. Wien, Austria) [49]. They were able to show that associativity and commutativity have a limited effect on the induced probability distribution on boolean functions : the probability of a boolean function f remains of the type $\gamma(f)/n^{L(f)+1}$, just as for And/Or trees (non-commutative and non-associative operators). As a consequence, all these distributions do not exhibit a Shannon effect.

4.4 Influence of the definition of size.

The same French-Austrian team also introduced a different notion of size for a boolean expression (or equivalently a tree) : the size is no longer the number of occurrences of boolean variables (or the number of leaves; let us call this the usual model), but includes the occurrences of operators (the total size of the tree). This model, which is currently fully worked out only for non-commutative operators, is equivalent to the usual one when the operators are not associative, and differs from it for associative operators in the later case, where it allows to analyze the memory that is actually needed to store the expression. Surprisingly, there is a significant difference in the shape of the trees, most notably as the number of leaves that are children of the root becomes large, i.e. the trees are comparatively "flat". Most of the classical properties of the usual model thus no longer hold, and this fact has required new strategies to study the distribution induced by such flat trees on boolean functions. Once the technical questions were solved, finding the same kind of distributions ($\gamma(f)/n^{L(f)}$) came quite as a surprise. As regards the two constant functions, their probability is bounded from below when then number n of boolean variables grows to infinity, which fits the large number of first-level leaves; hence this model again does not exhibit a Shannon effect.

4.5 Influence of exchanging the limits on the expression size and the number of variables.

Antoine Genitrini and Cécile Mailler finally considered the following problem : in almost every result on quantitative logic (with the notable exception of former work by Antoine Genitrini with Jakub Kozik and Marek Zaionc), the size m of the expression/tree, built on n boolean variables, grows to infinity; *then* the number n of variables grows to infinity; we shall call this the "classical" model. The order in such a double limit cannot be changed for fundamental technical reasons. By studying an equivalence relation between boolean expressions (two expressions are equivalent if one of them can be obtained from the other by

renaming or negating some variables), Antoine Genitrini and Cécile Mailler were able to define a general model, that includes as extremal cases both the classical model and the model of Genitrini/Kozik/Zaionc. After computing the limiting probability distribution induced on the boolean functions, they have presented an explanation of the similarities between the two, apparently opposite, extremal models.

This work paves the way to a direct study of satisfiability-like problems, in which boolean formulae are no longer "flat" as in, e.g., k-Sat models, but can be described by the (perhaps more realistic) Catalan-tree model and its extensions. In such a framework, the probability of the constant function *False* goes to 0, which means that, a.s., every expression is satisfiable.

4.6 Probabilities for satisfiability problems.

Élie de Panafieu and Danièle Gardy, together with Bernhard Gittenberger and Markus Kuba (T.U. Wien, Austria), have recently derived the probability for a given boolean function to be realized by a random conjunction of 2-Xor clauses. One important tool was defining a model for a random 2Xor expressions by multi-graphs with multiple types of vertices and edges. Those results are a refinement of a previous work of Hervé Daudé and Vlady Ravelomanana [36], which was restrained to the function *True* (i.e. the probability of satisfiability).

5 M1: Methodology: Combinatorial-analytic Methods.

Many participants were active in this axis, which has seen a wealth of significant results, both expected : non-planar or enriched trees, graphs and multi-graphs,... and unplanned : Pólya urns (with a possible extension to non-balanced urns), inhomogeneous hyper-graphs (with an alternative proof, through analytic combinatorics tools, of results first obtained by probabilistic methods), ...

5.1 Non-planar trees.

The results in this area are relative to two parameters of random non-planar trees, which are, e.g., the underlying structure when studying probability distributions on boolean functions induced by boolean expressions on commutative operators. Philippe Flajolet and Nicolas Broutin studied the distance distribution in the trees; distances such as the ones from the root to leaves are crucial for the complexity of the boolean functions that can be represented by such trees, where the absence of order on nodes embodies the symmetry of logical gates w.r.t. inputs. With Miklos Bóna (Univ. of Floride, U.S.A.), Philippe Flajolet also studied the distribution of the number of symmetry points in non-planar trees. This allows for a precise quantification of the (exponential) bias w.r.t. the uniform measure on planar trees.

5.2 Enriched trees.

Enriched trees are trees, to which we add edges from internal nodes to some of the leaves of their sub-trees. They are a natural model for quantified logical expressions, and as thus fit naturally into extensions of boolean expressions. Such structures actually are no longer trees, but rather a special class of directed acyclic graphs; their enumeration and statistical study thus requires a new approach quite different from those that have proved their efficiency on various classes of trees. Danièle Gardy has worked on the enumeration of enriched trees (in the guise of lambda-terms), in collaboration with Olivier Bodini and Alice Jacquot from LIPN, and Bernhard Gittenberger from T.U. Wien (Austria) [6, 7]. They have been able to enumerate asymptotically several families of terms, restricted either by the number of edges from a given node (this corresponds to conditions on the number of variables that can be bound by a quantifier), or by the number of nested quantifiers. They have also obtained bounds on the number of unrestricted terms, although their asymptotic enumeration remains an open problem. It is worth noticing that, even for a bounded number h of nested quantifiers, the enriched trees behave very differently from trees, and their behaviour exhibits "jumps" according to h, which is in itself a new combinatorial phenomenon worthy of consideration.

5.3 Graphs and multi-graphs.

The inhomogeneous graph model, introduced by Söderberg in 2002, is a generalization of the Erdös-Rényi model $G(n, p)$. Élie de Panafieu and Vlady Ravelomanana presented in [38] a new analytic approach to locate the critical density of edges at which the first component with two cycles appears; this allowed them to improve the description of the structure of a graph with a density of edges equal or close to the critical value. Those informations translate into precise descriptions of the phase transitions of two problems modelled by the inhomogeneous graph model: the probability of satisfiability of 2QXor expressions (cf. Section 6.3.1), and the probability for a graph to be bipartite.

In [37], Élie de Panafieu introduced a new general model of non-uniform hyper-graphs, where each edge of size t comes with a weight ω_t, then derived the critical excess at which the first connected component with two cycles appears and described the structure of the hyper-graph nearby. A surprising universal behaviour emerged. As expected, the value of the critical excess varies with the weights (ω_t); but – rather unexpectedly – the distribution of the excesses of the connected components in a hyper-graph with critical excess is independent of these weights.

5.4 Pólya urns.

In the spirit of the pionnering work of Philippe Flajolet, Philippe Dumas and Vincent Puyhaubert in 2006, Basile Morcrette has been concerned with an analytic combinatorics approach to Pólya urns. Firstly, he considered a class

of balanced, additive two-colors Pólya urns whose generating function is algebraic. Analytic combinatorics methods, most notably a saddle-point approach involving coalescent saddle points, have allowed him to obtain results on the asymptotic distribution of the urn content: central and local limit theorems, and large deviations; such properties were not yet available through classical probabilistic methods.

Secondly, B. Morcrette established necessary conditions on the replacement rules for additive balanced urns, to ensure that the generating function coding the behaviour of the urn remains algebraic. This work, which involves heavy use of a Computer Algebra System and was carried out in collaboration with Alin Bostan, Frédéric Chyzak and Philippe Dumas (Inria Rocquencourt), has allowed him to extend the class of urns that can be submitted to a straightful analysis through generating functions and asymptotic analysis.

B. Morcrette also cooperated with H. Mahmoud (Washington University, U.S.A.) in studying balanced urns whose evolution rules are defined through random variables. A suitable use of analytic combinatorics allowed them to obtain a differential system describing the relevant generating function. This system then gave exact expressions of the probability distributions for many cases.

Finally, B. Morcrette considered, in collaboration with P. Dumas, non-balanced urns. The behaviour of such urns was again obtained through an analytic approach, which involved a partial differential equation.

5.5 Realistic analysis of algorithms.

Sorting and searching algorithms. Julien Clément, Thu-Hien Nguyen-Thi and Brigitte Vallée have developed the so-called "realistic" complexity analysis of sorting and searching algorithms [30, 31]. Their goal is to revisit the analysis of fundamental algorithms of Computer Science (sorting or searching algorithms) in a "doubly realistic" model, where the data are very general, and the measure for complexity is more refined than the usual count of operations on global data. Such a study combines several quite different approaches. On the one hand, analytic combinatorics [41] aims at assessing the algorithm performance in probabilistic models and uses techniques related to complex analysis and combinatorics. On the other hand, the originality of the approach is that it can model a wide class of data sources, and evaluate the influence of the representation of data on the performance of the algorithms that handle them.

Clément et al. have thus introduced a model for the source that gives the data as words, by considering the collection of probabilities of prefixes of words. To the source is then associated a mathematical object calleda Dirichlet series, that syntheses many of the properties of the source. For each algorithm they consider, an essential step was to compute the probability that the execution of this algorithm compares two items produced by the source. Such a model has immediate advantagse : the analysis can take into account a wider set of models, and the constants appearing in the analysis can thus be connected to the source. The amount of computation, compared to previous approaches, is

also significantly decreased.

Arithmetical algorithms. Loïck Lhote and Brigitte Vallée, together with Valérie Berthée and Jean Creusefond [5], provided a probabilistic analysis of the naive algorithm for calculating the GCD of several polynomials or integers. This is a first step towards the analysis of more complex algorithms for diophantine approximations and discrete geometry. The algorithm performs successive calls to the classical Euclidean algorithm that acts on two polynomials or integers. The analysis accurately describes the probabilistic behaviour of the main parameters, namely the number of iterations of the Euclidean algorithm at each call, the total number of iterations, as well as the evolution of the size of the current GCD during the execution. An average case analysis and a distributional analysis are provided, giving rigorous proof of two phenomena: (i) most of the work is done during the first call to Euclid's algorithm, (ii) the algorithm has a similar behaviour whether we consider polynomials or integers.

5.6 Digital search trees.

Brigitte Vallée and Kanal Hun have begun a study of digital search trees under a general source model. They aim at comparing the main parameters (including path length) with the equivalent parameters in tries or Patricia tries. The first step (writing down an expression for the generating functions) has been carried out nicely, and has brought to attention the rôle played by a Dirichlet generating function for the source, which has some resemblance with – but is not identical to – the Dirichlet generating function for tries.

5.7 Random allocations.

Jérémie du Boisberranger and Danièle Gardy have revisited the classical Coupon Collector's Problem when the coupons are words built on an alphabet with non-uniform probabilities on the letters. Such a case leads to non-uniform distributions on the coupons; however words with the same number of occurrences of letters get the same probability; hence the probability distribution does not satisfy the assumptions made by previous works on non-uniform coupons. The asymptotic waiting time for the full collection was computed under general assumptions on the language; this has allowed to analyse an algorithm for the random generation of ARN (collaboration with Y. Ponty, LIX, École Polytechnique) [40].

6 M2: Methodology: Probabilistic Methods.

In this second methodological axis, many participants were again active, with important results on phase transition on random graphs (which also gave results on minimal spanning trees), and on the influence of the saturation level of a tree on the shape of the distribution such trees induce on the set of boolean functions.

Non-anticipated results cover a variation on Markov chains (VLMC), Pólya urns (again), ...

6.1 Saturation level.

Nicolas Broutin and Cécile Mailler have worked out a probabilistic approach to And/Or boolean expressions. They have been able to prove that, under easily checked conditions, it was possible to encode a boolean function by an infinite tree, and that such an encoding was continuous in the local topology (local convergence of neighbourhoods of the root). Such an approach allowed them to introduce several new tree-induced distributions on the set of boolean functions. They have also shown that, if the local limit is a tree without leaves, the sequence of functions that can be obtained from finite trees is asymptotically degenerate (it charges either True or False). This result is of methodological importance, as its proof required establishing a clear distinction between the two types of randomness in boolean expressions, stemming either from the underlying trees, or from the random labelling of internal nodes by operators and leaves by literals.

6.2 Phase transitions in random graphs.

Nicolas Broutin has been interested in threshold phenomena in random graphs. In collaboration with Louigi Addario-Berry (McGill Univ., Montreal, Canada) and Christina Goldschmidt (Oxford, U.K.), he showed that random graphs, when considered as metric spaces (with the graph distance) and suitably rescaled, converge towards a sequence of compact continuous metric spaces [1]. This convergence theorem was then used to obtain the limit for another important random structure, namely the minimal spanning tree of a complete graph [2]. These results also establish a link between boolean frameworks and threshold phenomena in combinatorial optimization problems such as 2XorSat [36] or 2-coloring, and could be crucial when studying more complex problems, such as 2Sat.

Nicolas Broutin and Jean-François Markert [11] then made a first step towards a generalization to other models of graphs, in a paper on trees with fixed node distribution. The expected result for critical graphs with a fixed degree sequence should allow for the study of constrained distributions in combinatorial optimization problems.

6.3 Costs in search trees.

Nicolas Broutin, together with Ralph Neininger and Henning Sulzbach (both at Frankfurt University, Germany), has begun the study of new functional aspects of the cost of queries in search trees. They were able to quantify very precisely the joint cost of all possible queries in quadtrees [12, 13]; among other consequences, this yields asymptotics for the cost of the worst query. The techniques they developed to solve this problem have also proved useful to answer

another question on a class of trees that appear when recursively partitionning a disk [14].

6.4 Operator on a regular tree.

Victor Bapst and Guilhem. Semerjianhave mixed probabilistic and combinatorial approaches when studying a random operator problem : the adjacency operator of a regular tree with random weights (Anderson's model on trees) [4]. Its density has an essential singularity (so-called Lifshitz tail); they have been able to give a combinatorial characterization of this through enumeration of various walks on the tree.

6.5 Variable Length Markov Chains.

Brigitte Chauvin and Nicolas Pouyanne, with Peggy Cenac (Univ. of Bourgogne, France) and Frédéric Paccaut (Amiens, France), have been involved in the analysis of a variation of Markov chains. Infinite random sequences of letters can be viewed as stochastic chains or as strings produced by a source, in the sense of information theory. The relationship between Variable Length Markov Chains (VLMC) and probabilistic dynamical sources is studied in [22]. A probabilistic frame for context trees and VLMC is established. Two examples, the "comb" and the "bamboo blossom", are detailed: a necessary and sufficient condition is found for the existence and the uniqueness of a stationary probability measure for these particular VLMC.

A second work [23] goes further on this topic, and considers the suffix trie built by insertion of the words produced by the source. Common assumptions on the source producing the words inserted in a suffix trie with n leaves lead to a height and saturation level of order $\log n$. The authors then show, for two particular cases of "comb" and thanks to the mixing properties of such a source, that the height of the tree that appears in the first case increases faster than a power of n, and that the saturation level of the tree in the second case is negligible with respect to $\log n$. The first example corresponds to a "logarithmic infinite comb" and enjoys a non uniform polynomial mixing. The second one corresponds to a "factorial infinite comb" for which mixing is uniform and exponential.

In [21], Brigitte Chauvin and collaborators consider a random walk whose increments X_n are the letters generated by a VLMC source. The increments are very far from being independent and this fact produces a so-called "persistent" random walk, which is not Markovian. Under suitable conditions, this random walk converges to a stochastic process, the Integrated Telegraph Noise process. The key fact is to consider the non Markovian letter process (X_n) as the margin of a couple $(X_n, M_n)_{n\geq 0}$ where $(M_n)_{n\geq 0}$ stands for the memory of the process (X_n).

6.6 Polya urns.

Brigitte Chauvin and Nicolas Pouyanne, with co-authors, have used probabilistic methods to study new distributions that appear as limit objects in large Pólya urns.

Consider a balanced non triangular two-color Pólya-Eggenberger urn process, assumed to be large – this means that the ratio σ of the replacement matrix eigenvalues satisfies $1/2 < \sigma < 1$. The composition vector of both discrete time and continuous time models admits a drift which is carried by the principal direction of the replacement matrix. In the second principal direction, this random vector admits also an almost sure asymptotic limit, and a real-valued limit random variable arises; this limit is denoted by W^{DT} in discrete time and by W^{CT} in continuous time. The articles [29] and [28] deal with the distributions of both versions of W. Appearing as martingale limits, known to be non-normal, these laws remained rather mysterious before these works.

In [29] the dislocation equations associated with the continuous-time process lead to a system of two differential equations satisfied by the Fourier transforms of the limit distributions. The resolution is carried out in the complex field and it turns out that the Fourier transforms are explicitly related to Abelian integrals over Fermat curves. The limit laws W^{CT} appear as a new family of probability densities supported by the whole real line and not bounded at the origin.

In [28] it is shown by exploiting the underlying tree structure of the urn process that W^{DT} and W^{CT} are the unique solutions of two distributional systems in some suitable spaces of integrable probability measures. These systems are natural extensions of distributional equations that already appeared in famous algorithmic problems, such as Quicksort analysis. The existence and unicity of the solutions of the systems are obtained by means of contracting smoothing transforms. Via the equation systems, upper bounds for the moments of W^{DT} and W^{CT} are found and it is shown that the laws of W^{DT} and W^{CT} are moment-determined. It is also proven that W^{DT} is supported by the whole real line, that its exponential moment generating series has an infinite radius of convergence, and that W^{DT} admits an infinitely differentiable density.

Both articles [27] and [26] deal with the composition vector of the m-ary search tree, with techniques that are of the same vein. The space requirement of an m-ary search tree satisfies a well-known phase transition: when $m \leq 26$, the second order asymptotic behaviour is Gaussian. When $m \geq 27$, it is not Gaussian any longer and a limit W of a complex-valued martingale arises. It is shown in [26] that the distribution of W has a square integrable density on the complex plane, that its support is the whole complex plane, and that it has finite exponential moments. The proofs are based on the study of the distributional equation $W \stackrel{d}{=} \sum_{k=1}^{m} V_k^{\lambda} W_k$, where $V_1, ..., V_m$ are the spacings of $(m-1)$ independent random variables uniformly distributed on $[0, 1]$, $W_1, ..., W_m$ are independent copies of W which are also independent of $(V_1, ..., V_m)$, and λ is a complex number.

In [27] the multi-type branching process which is the continuous time version

of the m-ary search tree is considered. This process satisfies a phase transition similar to that of the standard m-ary tree. In particular, when $m \geq 27$, a limit W^{CT} of a complex-valued martingale intervenes in its asymptotic behaviour. Thanks to the branching property, the law of W^{CT} satisfies a so-called smoothing equation of the type $Z \stackrel{d}{=} e^{-\lambda T}(Z^{(1)} + \cdots + Z^{(m)})$, where λ is a particular complex number, $Z^{(k)}$ are complex-valued random variables having the same law as Z, T is a $\mathbb{R}_+$-valued random variable independent of the $Z^{(k)}$. This distributional equation is extensively studied by various approaches. The existence and uniqueness of solution of the equation are proved by contraction methods. The fact that the distribution of W^{CT} is absolutely continuous and that its support is the whole complex plane is shown via Fourier analysis. Finally, the existence of exponential moments of W is obtained by considering W as the limit of a complex Mandelbrot cascade.

References

[1] L. Addario-Berry, N. Broutin, and C. Goldschmidt. The continuum limit of critical random graphs. *Probability Theory and Related Fields*, 152:367–406, 2012.

[2] L. Addario-Berry, N. Broutin, C. Goldschmidt, and G. Miermont. The scaling limit of the minimum spanning tree of the complete graph. arXiv:1301.1664, 2013.

[3] V. Bapst, L. Foini, F. Krzakala, G. Semerjian, and F. Zamponi. The quantum adiabatic algorithm applied to random optimization problems: The quantum spin glass perspective. *Physics Reports*, (3):127 – 205, 2013.

[4] V. Bapst and G. Semerjian. Lifshitz tails on the bethe lattice: A combinatorial approach. *Journal of Statistical Physics*, 145(1):51–92, 2011.

[5] V. Berthé, J. Creusefond, L. Lhote, and B. Vallée. Multiple GCDs. probabilistic analysis of the plain algorithm. In *ISSAC 2013, Boston, Massachusetts (USA)*.

[6] O. Bodini, D. Gardy, and B. Gittenberger. Lambda-terms of bounded unary height. In P. Flajolet and D. Panario, editors, *Proceedings of the Eighth Workshop on Analytic Algorithmics and Combinatorics, ANALCO 2011, San Francisco, California, USA, January 22, 2011*, pages 23–32. SIAM, 2011.

[7] O. Bodini, D. Gardy, and A. Jacquot. Asymptotics and random sampling for BCI and BCK lambda terms. *Theor. Comput. Sci.*, 502:227–238, 2013.

[8] E. Böhler, N. Creignou, M. Galota, S. Reith, H. Schnoor, and H. Vollmer. Boolean circuits as a data structure for boolean functions: Efficient algorithms and hard problems. *Logical Methods in Computer Science*, 8(3), 2010.

[9] E. Brier, Q. Fortier, R. Korkikian, K. W. Magld, D. Naccache, G. Ozari de Almeida, A. Pommellet, A. H. Ragab, and J. Vuillemin. Defensive leakage camouflage. In *CARDIS'12 Proceedings of the 11th international conference on Smart Card Research and Advanced Applications*, pages 277–295, December 2012.

[10] N. Broutin and O. Fawzi. Longest distance in random circuits. *Combinatorics, Probability & Computing*, 21:856–881, 2012.

[11] N. Broutin and J.-F. Marckert. Asymptotic of trees with a prescribed degree sequence and applications. *Random Structures and Algorithms*, 2012.

[12] N. Broutin, R. Neininger, and H. Sulzbach. A limit process for partial match queries in random quadtrees. *The Annals of Applied Probability*, 2012.

[13] N. Broutin, R. Neininger, and H. Sulzbach. Partial match queries in random quadtrees. In Y. Rabani, editor, *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1056–1065, 2012.

[14] N. Broutin and H. Sulzbach. The dual tree of a recursive triangulation of the disk. arXiv:1211.1343 [math.PR], 2012.

[15] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager. Further results on Niho bent functions. In *IEEE Transactions on Information Theory-IT, Vol 58, no.11*, pages 6979–6985, 2012.

[16] C. Carlet, P. Gaborit, J.-L. Kim, and P. Solé. A new class of codes for boolean masking of cryptographic computations. *IEEE Transactions on Information Theory*, 58:6000–6011, 2012.

[17] C. Carlet, L. Goubin, E. Prouff, M. Quisquater, and M. Rivain. Higher-order masking schemes for s-boxes. In *Fast Software Encryption FSE 2012*, volume 7549 of *Lecture Notes in Computer Science*, pages 366–384. 2012.

[18] C. Carlet and S. Mesnager. On Dillon's class H of bent functions, Niho bent functions and O-polynomials. In *Journal of Combinatorial Theory, Series A, Vol 118, no. 8*, pages 2392–2410, 2011.

[19] C. Carlet and S. Mesnager. On Semi-bent Boolean Functions. In *IEEE Transactions on Information Theory-IT, Vol 58 No 5*, pages 3287–3292, 2012.

[20] C. Carlet, F. Zhang, and Y. Hu. Secondary constructions of bent functions and their enforcement. *Advances in Mathematics of Communications*, 6:305 – 314, 2012.

[21] P. Cénac, B. Chauvin, S. Herrmann, and P. Vallois. Persistent random walks, variable length Markov chains and piecewise deterministic Markov processes. *Markov Processes and Related Fields*, 2013. To appear.

[22] P. Cénac, B. Chauvin, F. Paccaut, and N. Pouyanne. Context trees, variable length Markov chains and dynamical sources. *Séminaire de Probabilités*, 44:1–39, 2012.

[23] P. Cénac, B. Chauvin, F. Paccaut, and N. Pouyanne. Uncommon suffix tries. *Random Structures and Algorithms*, 2013. To appear.

[24] B. Chauvin, D. Gardy, and C. Mailler. The growing trees distribution on boolean functions. In P. Flajolet and D. Panario, editors, *Proceedings of the Eighth Workshop on Analytic Algorithmics and Combinatorics, ANALCO 2011, San Francisco, California, USA, January 22, 2011*, pages 45–56. SIAM, 2011.

[25] B. Chauvin, D. Gardy, and C. Mailler. A growing tree model for random boolean functions. *Random Structures and Algorithms*, to appear, 2014.

[26] B. Chauvin, Q. Liu, and N. Pouyanne. Support and density of the limit m-ary search trees distribution. *23rd Intern. Meeting on Probabilistic, Combinatorial, and Asymptotic Methods for the Analysis of Algorithms (AofA'12), DMTCS*, pages 191–200, 2012.

[27] B. Chauvin, Q. Liu, and N. Pouyanne. Limit distributions for multitype branching processes of m-ary search trees. *Ann. Inst. Henri Poincaré*, to appear, 2013.

[28] B. Chauvin, C. Mailler, and N. Pouyanne. Smoothing equations for large Pólya urns. *Accepted to JTP*, 2013.

[29] B. Chauvin, N. Pouyanne, and R. Sahnoun. Limit distributions for large Pólya urns. *Annals Applied Prob.*, 21(1):1–32, 2011.

[30] J. Clément, T. H. Nguyen Thi, and B. Vallée. A general framework for the realistic analysis of sorting and searching algorithms. Application to some popular algorithms. In N. Portier and T. Wilke, editors, *30th International Symposium on Theoretical Aspects of Computer Science (STACS 2013)*, volume 20 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 598–609, Dagstuhl, Germany, 2013. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[31] J. Clément, T. H. Nguyen Thi, and B. Vallée. Realistic analysis of sorting and searching algorithms: design of a general framework and application to some popular algorithms. *Combinatorics, Probability and Computing*, 2014. accepted (31 pages).

[32] N. Creignou and H. Daudé. Sensitivity of boolean formulas. *Eur. J. Comb.*, 34(5):793–805, 2013.

[33] N. Creignou, U. Egly, and M. Seidl. A framework for the specification of random SAT and QSAT formulas. In *Tests and Proofs - 6th International Conference, TAP 2012, Prague, Czech Republic, May 31 - June 1, 2012. ProceedingsTAP*, volume 7305 of *Lecture Notes in Computer Science*, pages 163–168. Springer, 2012.

[34] N. Creignou and H. Vollmer. Parameterized complexity of weighted satisfiability problems. In *Theory and Applications of Satisfiability Testing - SAT 2012 - 15th International Conference, Trento, Italy, June 17-20, 2012. Proceedings*, volume 7317 of *Lecture Notes in Computer Science*, pages 341–354. Springer, 2012.

[35] H. Daudé, C. Martínez, V. Rasendrahasina, and V. Ravelomanana. The max-cut of sparse random graphs. In *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2012, Kyoto, Japan*, pages 265–271. SIAM, 2012.

[36] H. Daudé and V. Ravelomanana. Random 2-XorSat phase transition. *Algorithmica*, 59(3):48–65, 2011.

[37] É. de Panafieu. Phase transition of random non-uniform hypergraphs. *IWOCA2013*, 2013.

[38] É. de Panafieu and V. Ravelomanana. Analytic description of the phase transition of inhomogeneous multigraphs. *Eurocomb*, 2013.

[39] J. du Boisberranger, D. Gardy, X. Lorca, and C. Truchet. When is it worthwhile to propagate a constraint? a probabilistic analysis of alldifferent. In M. Nebel and W. Szpankowski, editors, *Proceedings of the 10th Meeting on Analytic Algorithmics and Combinatorics, ANALCO 2013, New Orleans, Louisiana, USA, January 6, 2013*, pages 80–90. SIAM, 2013.

[40] J. du Boisberranger, D. Gardy, and Y. Ponty. The weighted words collector. In *AofA'12, International Conference on the Analysis of Algorithms*, Montréal, Canada, June 2012.

[41] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.

[42] J-P Flori and S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions. In *7th International conference SETA 2012, LNCS 7280, Springer*, pages 40–52, 2012.

[43] H. Fournier, D. Gardy, A. Genitrini, and B. Gittenberger. The fraction of large random trees representing a given boolean function in implicational logic. *Random Struct. Algorithms*, 40(3):317–349, 2012.

[44] H. Fournier, D. Gardy, A. Genitrini, and M. Zaionc. Tautologies over implication with negative literals. *Math. Log. Q.*, 56(4):388–396, 2010.

[45] H. Fournier, G. Malod, and S. Mengel. Monomials in arithmetic circuits: Complete problems in the counting hierarchy. In *STACS*, pages 362–373, 2012.

[46] H. Fournier, S. Perifel, and R. de Verclos. On fixed-polynomial size circuit lower bounds for uniform polynomials in the sense of valiant. In *MFCS*, 2013.

[47] G. Gao, X. Zhang, W. Liu, and C. Carlet. Constructions of quadratic and cubic rotation symmetric bent functions. *IEEE Transactions on Information Theory*, 58:4908–4913, 2012.

[48] A. Genitrini and B. Gittenberger. No Shannon effect on probability distributions on Boolean functions induced by random expressions. In *21st International Meeting on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms*, pages 303–316, Vienna, Austria, July 2010.

[49] A. Genitrini, B. Gittenberger, V. Kraus, and C. Mailler. Probabilities of boolean functions given by random implicational formulas. *Electronic Journal of Combinatorics*, 19(2):P37, 20 pages, (electronic), 2012.

[50] A. Genitrini and J. Kozik. In the full propositional logic, 5/8 of classical tautologies are intuitionistically valid. *Annals of Pure and Applied Logic*, 163(7):875–887, 2012.

[51] T. Helleseth, A. Kholosha, and S. Mesnager. Niho Bent Functions and Subiaco/Adelaide Hyperovals. In *Proceedings of the 10-th International Conference on Finite Fields and Their Applications (Fq'10), Contemporary Math., AMS. Vol 579*, pages 91–101, 2012.

[52] H. Maghrebi, C. Carlet, S. Guilley, and J.-L. Danger. Optimal first-order masking with linear and non-linear bijections. In *AFRICACRYPT 2012*, volume 7374 of *LNCS*, pages 360–377. 2012.

[53] S. Mesnager. Semi-bent functions with multiple trace terms and hyperelliptic curves. In *Proceeding of International Conference on Cryptology and Information Security in Latin America (IACR), Latincrypt 2012, LNCS 7533, Springer*, pages 18–36, 2012.

[54] S. Mesnager and J-P Flori. On hyper-bent functions via Dillon-like exponents. In *IEEE International Symposium on Information Theory, IMT, Cambridge, MA, USA, July 1–6*, 2012.

[55] D. Tang, C. Carlet, and X. Tang. Highly nonlinear boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. *IEEE Transactions on Information Theory*, 59:653–664, 2013.

[56] J. Vuillemin. Algèbre de Boole. *Techniques de l'ingénieur, Editions T. I.*, AF118:113, 2010.

[57] X. Zeng, C. Carlet, L. Hu, and J. Shan. More balanced boolean functions with optimal algebraic immunity, and good nonlinearity and resistance to fast algebraic attacks. *IEEE Transactions on Information Theory*, 57:6310–6320, 2011.

Contents