SPECIAL SESIONS

Applications of Computer Algebra - ACA2018

June 18–22, 2018

Santiago de Compostela, Spain

S1
General Session

Thursday

Thu 21st, 16:30 - 17:00, Aula 1 – Armin Jamshidpey:
Randomized Algorithms for Normal Basis in Characteristic Zero

Thu 21st, 17:30 - 18:00, Aula 1 – Gereon Kremer:
Computer Algebra and Computer Science

Thu 21st, 18:00 - 18:30, Aula 1 – Juan Carlos Ku-Cauich:
Conversion of element representations in Galois rings

Thu 21st, 18:30 - 19:00, Aula 1 – Eugenio Roanes-Lozano:
Automatic generation of diagrammatic subway maps for any date with Maple

Thu 21st, 19:00 - 19:30, Aula 1 – Pilar Vélez:
Detecting truth, just on parts, in automated reasoning in geometry

Organizer

Michael Wester:
University of New Mexico, USA

Aim and scope

This session is for talks that do not fit into any of the other ACA sessions. All proposals in the scope of the conference are welcome.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Randomized Algorithms for Normal Basis in Characteristic Zero

Mark Giesbrecht[1], **Armin Jamshidpey**[1], **Éric Schost**[1]

For a finite Galois extension K/F with $G = \mathrm{Gal}(K/F)$, there exists an element $\alpha \in K$ such that its conjugates form an F-basis of K (as a vector space)[4, Theorem 6.13.1]. Having such a basis, which is known as normal basis, is useful for certain computational purposes.

There are efficient algorithms for constructing a normal basis in positive characteristics. For a deterministic algorithm see [1] and for randomized algorithms see [6] and [3]. In characteristic zero, deterministic algorithms are introduced in [2] and [5](for abelian extensions).

Our aim is to introduce randomized algorithms for constructing a normal basis in characteristic zero. We will present an algorithm for cyclic extensions and more generally abelian extensions. We also give a solution for Galois extensions with dihedral group as Galois group.

Keywords: Normal Basis, Cyclic Extension, Abelian Extension

References

[1] DANIEL AUGOT; PAUL CAMION, *Forme de Frobenius et vecteurs cycliques*. *C. R. Acad. Sci. Paris Sér. I Math.*, 318(2):183–188, 1994.

[2] KURT GIRSTMAIR, *An algorithm for the construction of a normal basis*. *J. Number Theory*, 78(1):36–45, 1999.

[3] ERICH KALTOFEN; VICTOR SHOUP. *Subquadratic-time factoring of polynomials over finite fields*. *Math. Comp.*, 67(223):1179–1197, 1998.

[4] SERGE LANG, *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[5] ALAIN POLI, *A deterministic construction for normal bases of abelian extensions*. *Comm. Algebra*, 22(12):4751–4757, 1994.

[6] JOACHIM VON ZUR GATHEN; MARK GIESBRECHT, *Constructing normal bases in finite fields*. *J. Symbolic Comput.*, 10(6):547–570, 1990.

[1]David R. Cheriton School of Computer Science
University of Waterloo
200 University Avenue West Waterloo, ON, Canada N2L 3G1
mwg@uwaterloo.ca
armin.jamshidpey@uwaterloo.ca
eschost@uwaterloo.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computer Algebra and Computer Science

Gereon Kremer[1]

Certain fields within computer science commonly make use of methods from computer algebra. A prominent example for that is satisfiability modulo theories (SMT) solving that extends the traditional question of satisfiability of propositional logic formulas to first-order theories. We consider nonlinear real problems in particular which produces a need for methods to deal with nonlinear real constraints.

This topic is also an important topic in computer algebra, a community that deals with very similar questions but is surprisingly disjoint from the SMT solving community. The disjointness of these groups used to be a significant obstacle for any transfer of knowledge. The SC^2 project tries to resolve this hurdle by forging new collaborations between the communities of satisfiability checking and symbolic computation.

We present SMT solving as an application of methods from computer algebra and motivate functional requirements and use cases for these methods that are uncommon but very important for SMT solving. Though we can modify existing methods to a certain degree, we as computer scientists depend on the computer algebra community to solve some issues. We show several projects that yielded successful adaptations of methods like Gröbner bases[JLCA13], virtual substitution[CA11] or cylindrical algebraic decomposition[KCA16] to our applications.

Finally we give multiple examples of existing implementations of methods from computer algebra – CoCoALib and Maple – that we struggled to integrate in a meaningful way. We provide insights into the actual problems and hope to suggest new directions of research that ease the cooperation between computer science and computer algebra in the future.

Keywords: Computer Algebra, Computer Science, Satisfiability Modulo Theories Solving, Gröbner Bases, Cylindrical Algebraic Decomposition, Virtual Substitution

References

[CA11] Florian Corzilius and Erika Abraham. Virtual Substitution for SMT Solving. In *FCT'11*, volume 6914 of *LNCS*, pages 360–371. Springer, 2011.

[JLCA13] Sebastian Junges, Ulrich Loup, Florian Corzilius, and Erika Abraham. On Gröbner Bases in the Context of Satisfiability-Modulo-Theories Solving over the Real Numbers. In *CAI'13*, volume 8080 of *LNCS*, pages 186–198. Springer, 2013.

[KCA16] Gereon Kremer, Florian Corzilius, and Erika Abraham. A Generalised Branch-and-Bound Approach and its Application in SAT Modulo Nonlinear Integer Arithmetic. In *CASC'16*, volume 9890 of *LNCS*, pages 315–335. Springer, 2016.

[1]Theory of Hybrid Systems
RWTH Aachen University
52056 Aachen Germany
gereon.kremer@cs.rwth-aachen.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Conversion of element representations in Galois rings

Juan Carlos Ku-Cauich[1], **Guillermo Morales-Luna**[2]

A Galois ring is a finite ring with unity such that the divisors of zero, together with zero itself, form a principal ideal, generated by an element of the form pe, where e is the ring unit and p is a prime number. For any prime p and two integers s, m, the map

$$\pi_p : \mathbb{Z}_{p^s}[X] \to \mathbb{F}_p[X]\ ,\ g(X) = \sum_{j=0}^{m-1} a_j X^j \mapsto g(X) \bmod p = \sum_{j=0}^{m-1} (a_j \bmod p) X^j,$$

is a ring homomorphism. An irreducible polynomial $h(X) \in \mathbb{Z}_{p^s}[X]$ is basic if $\pi_p(h(X))$ is irreducible in $\mathbb{F}_p[X]$ and in this case $\mathbb{Z}_{p^s}/\langle h(X)\rangle$ is a Galois ring, denoted $GR(p^s, m)$. Let $\eta = X + \langle h(X)\rangle \in GR(p^s, m)$, then $h(\eta) = 0$ and $\mathbb{F}_{p^m} \approx [\mathbb{Z}_p[X]/\langle \pi_p(h(X))\rangle]$. Hence, $GR(p^s, m) = \mathbb{Z}_{p^s}[\eta]$ and each element in the Galois ring can be written in an additive form: $\sum_{j=0}^{m-1} a_j \eta^j$, with $a_j \in \mathbb{Z}_{p^s}$.

A polynomial $g(X) \in \mathbb{Z}_{p^s}[X]$ is basic primitive if $\pi_p(g(X))$ is primitive in $\mathbb{F}_p[X]$. It is well known [4] that there is an element $\xi \in GR(p^s, m)$ and a basic primitive polynomial $g(X) \in \mathbb{Z}_{p^s}[X]$ of degree m such that $o(\xi) = p^m - 1$, $g(\xi) = 0$, $g(X)|(X^{p^m-1} - 1)$ in $\mathbb{Z}_{p^s}[X]$ and the following two properties hold:

- $GR(p^s, m) = \mathbb{Z}_{p^s}[\xi]$
- Each element in $GR(p^s, m)$ can be written uniquely in a p-adic form: $\sum_{k=0}^{s-1} b_k p^k$, with $b_k \in \mathcal{T}(g(X))$, where $\mathcal{T}(g(X)) = \{0\} \cup \left(\xi^i\right)_{i=0}^{p^m-2}$ is a Teichmüller set.

Each primitive polynomial in $\mathbb{F}_p[X]$ characterizes a set of basic primitive polynomials in $\mathbb{Z}_{p^s}[X]$, namely its inverse image under the projection π_p. The p-adic representation depends on the chosen basic primitive polynomial.

We have developed a series of programs, basically in `sage`, to find monic basic primitive polynomials and convert additive representations into p-adic representations of the Galois ring elements, and conversely.

For any $m \in \mathbb{Z}^+$ there is [2] a monic primitive polynomial $f_{pm}(X) \in \mathbb{F}_p[X]$ dividing $P_{pm}(X) = X^{p^m-1} - 1$ in $\mathbb{F}_p[X]$. Then, by Hensel Lift [3] there is a monic basic primitive polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ dividing $P_{pm}(X)$ in $\mathbb{Z}_{p^s}[X]$ with projection $f_{pm}(X)$. Since $f_{pm}(X) \in \mathbb{F}_p[X]$ is irreducible with no multiple roots, the polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ is unique [4]. Hence, a natural correspondence $f_{pm}(X) \leftrightarrow f_{psm}(X)$ arises, and in most cases it is not the identity, namely $f_{pm}(X) \neq f_{psm}(X)$ in $\mathbb{Z}_{p^s}[X]$.

In the worst case, for small values of m and s the search of the Hensel lift polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ can be done exhaustively. Alternatively, a list [2] of monic primitive polynomials in the ring $\mathbb{F}_p[X]$ may be provided in order to consider the inverse images of those polynomials under the projection modulus p.

The interest in finding effective and efficient representation conversions is due to the implementation of authentication codes based on the Gray transform [1].

Keywords: Galois rings, Teichmüller elements, symbolic computation

References

[1] Juan Carlos Ku-Cauich and Horacio Tapia-Recillas. Systematic authentication codes based on a class of bent functions and the Gray map on a Galois ring. *SIAM J. Discrete Math.*, 27(2):1159–1170, 2013.

[2] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[3] B.R. McDonald. *Finite Rings With Identity*. Pure and Applied Mathematics Series. Marcel Dekker Incorporated, 1974.

[4] Z.X. Wan. *Lectures on Finite Fields and Galois Rings*. World Scientific, 2003.

[1]Computer Science
CINVESTAV-IPN
Mexico City, Mexico
jckc35@hotmail.com

[2]Computer Science
CINVESTAV-IPN
Mexico City, Mexico
gmorales@cs.cinvestav.mx

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Automatic generation of diagrammatic subway maps for any date with Maple

Alberto Almech[1], **Eugenio Roanes-Lozano**[2]

The second author was one of the authors of a computer package written in Maple that could automatically generate railway maps of a network for any date. This package was presented at ACA'2008 and its design and implementation is described in [1]. Each section of the network was coloured accordingly to its characteristics (single / double track, electrified / non electrified, opened / closed / greenway,...). The position of the nodes (stations, junctions,...) was obtained from a list of geographical coordinates.

The work presented here deals with a similar although not identical case: subway networks are treated as graphs with the help of a computer algebra system in order to obtain the diagrammatic map for any date.

Most metro network plans follow more or less closely the ideas introduced by Harry Beck in his diagrammatic design of London subway map (the distances between stations and geographic orientation of the lines don't have to be respected, as the clarity and the number of stations between two stations is the key information to be visualized).

Therefore allocating nodes is far simpler, and we have decided to manually allocate the stations on a predefined grid.

The situation is also simpler because all lines are double track and electrified. For instance in Madrid subway there are minor differences between lines, such as the kind of catenary (classic or rigid), the gauge (narrow / broad),... that will not be considered here. Each node and edge of the graph has dates associated: inauguration date / closure date –the latter if applies.

The package takes advantage of the simplifications w.r.t. [1] mentioned above and the features of *Maple's Networks* package. This way the approach, although general, can be implemented in relatively few lines of code.

We know of no other similar works.

The work is illustrated with the case of Madrid subway network, one of the biggest ones in the world.

Keywords: Graph theory, Network models, Diagrammatic maps, Subways

References

[1] E. ROANES-LOZANO, A. MARTÍNEZ-ZARZUELO, A. GARCÍA-ÁLVAREZ, M. J. WESTER, E. ROANES-MACÍAS Automatically Obtaining Railway Maps from a Set of Historical Events *RACSAM (Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales, Serie A, Matemáticas)* **105**(1), 149–165 (2011). DOI 10.1007/s13398-011-0010-1

[1]Facultad de CC. Matemáticas, Universidad Complutense de Madrid
Plaza de Ciencias s/n, 28040-Madrid, Spain
albermech@gmail.com

[2]Instituto de Matemática Interdisciplinar &
Depto. de Álgebra, Geometría y Topología
Facultad de Educación, Universidad Complutense de Madrid
c/ Rector Royo Villanova s/n, 28040-Madrid, Spain
eroanes@mat.ucm.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Detecting truth, just on parts, in automated reasoning in geometry*

Zoltán Kovács[1], **Tomás Recio**[2] and **M. Pilar Vélez**[3]

We introduce and discuss, through a computational algebraic geometry approach, the automatic reasoning handling of propositions that are simultaneously true and false over some relevant collections of instances. A rigorous, algorithmic criterion is presented for detecting such cases, and its performance is exemplified through the implementation of this test on the dynamic geometry program *GeoGebra*.

The algebraic geometry approach to automated reasoning in geometry proceeds by translating a geometric statement $\{H \Rightarrow T\}$ into polynomial expressions, after adopting a coordinate system. Then, the geometric instances verifying the hypotheses can be represented as the solution of a system of polynomial equations $V(H) = \{h_1 = 0, \ldots, h_r = 0\}$ (*hypotheses variety*) they are represented algebraically by the ideal (of hypotheses) $H = \langle h_1 = 0, \ldots, h_r = 0\rangle$ generated by such polynomials. Analogously, the thesis is represented as the solution of a polynomial $V(T) = \{f = 0\}$, describing the hypotheses (resp. the thesis) variety.

Thus, when $V(H) \subseteq V(T)$ we can say that the theorem is *always true*. But this fact rarely happens, even for well established theorems, because the algebraic translation of the geometric construction described by the hypotheses usually forgets explicitly excluding some degenerate cases, cf. [4].

Thus, a delicate, but more useful, approach for automated reasoning consists in exhibiting, first, a collection of independent variables modulo H, so that no polynomial relation among them holds over the whole $V(H)$ (*independent variables modulo* H). Now, the irreducible components of $V(H)$ where these variables do remain independent are assumed to describe *non-degenerate* instances.

Accordingly, a statement is called *generally true* if the thesis holds, at least, over all the non-degenerate components. On the other hand, if over each non-degenerate component the thesis does not identically vanish, the statement is labeled as *generally false*. Remark that this last includes the *always false* case, where the thesis does not hold at all. A more detailed description of this quite established terminology (with small variants) can be consulted, for instance, at [6], [3] or [7]. It follows from the definition that to be generally true and to be generally false are incompatible.

However—and this is the object of interest in this talk—there are statements which happen to be, simultaneously, not generally true and not generally false, i.e. statements that are *true, just on some components*. Recently, in [7], a new terminology

*Partially supported by the Spanish Research Project MTM2017-88796-P Computación simbólica: nuevos retos en álgebra y geometría y sus aplicaciones

to describe such cases has been introduced, labelling as *generally true on components* or, simply, as *true on components*; moreover [7] presents an algorithmic test to check this property. We have decided—for the better comprehension of this notion by general users of dynamic geometry programs implementing this feature, such as *GeoGebra*—to label such statements in a more colloquial way, as statements *true on parts, false on parts*, in some specific sense we will describe in detail below.

Let us first start analyzing a simple example. Consider points $A(0,0), B(2,0)$ in the plane and construct circles $c = (x-0)^2 + (y-0)^2 - 3$ and $d = (x-2)^2 + (y-0)^2 - 3$, i.e. circle c is centered at A and circle d is centered at B and both have the same radius $r = \sqrt{3}$. Finally, we consider the two points of intersection of these circles, namely, $E(u,v)$ and $F(m,n)$. Thus, the hypotheses ideal is $\left\langle u^2+v^2-3, (u-2)^2+v^2-3, m^2+n^2-3, (m-2)^2+n^2-3 \right\rangle$.

The thesis states the parallelism of the lines AE and BF, that is, the vanishing of the polynomial $u \cdot n - v \cdot (m-2)$. The ideal of hypotheses is clearly zero-dimensional, so there are no independent variables, nor degenerate components. Its primary components, over the rationals, are

$$\left\langle v-n, (m-2)^2+n^2-3, (u-2)^2+v^2-3, m^2+n^2-3, u^2+v^2-3 \right\rangle$$
$$\left\langle v+n, (m-2)^2+n^2-3, (u-2)^2+v^2-3, m^2+n^2-3, u^2+v^2-3 \right\rangle.$$

It easy to check that the thesis is false over the first one and true over the second. This a clear, simple example of a neither true nor false, i.e. of a *true on components*, statement arising in an elementary geometry context (see other, less artificial examples in [6, 1]).

Obviously, since the idea of *true on components*, or *true on parts, false on parts*, is based on the concepts of degeneracy and of irreducible component, it follows that both the choice of the field over which the prime decomposition is performed (for example, the ideal H of the previous example has four components instead, if $\mathbb{Q}(\sqrt{2})$ is considered as base field) and the choice of the independent variables –which determine which components are to be considered as degenerate– could be essential.

About this last issue we would like to remark that when dealing with geometric statements it seems logical to take as independent variables the coordinates of the free points in the geometric construction we are dealing with; and we expect that its cardinality is the dimension of the hypotheses ideal. In most cases this "intuitively" maximal set of independent variables is maximum-size, but there are examples in which the coordinates of the free points in the geometric construction do not provide a maximum-size set of independent variables. See, for instance, Example 7 in [4], concerning Euler's formula regarding the radii of the inner and outer circles of a triangle with vertices $(-1,0), (1,0), (u[1], u[2])$. Here the dimension of the hypotheses variety is expected to be 2 (referring to the two coordinates of the only free vertex of the triangle), but applying the algebraic definition of independence it turns out to be three…, unless it is explicitly required, and added as a new hypothesis, that $(u[1], u[2])$ does not lie in the x-axis! This is a quite common problem—

related, as mentioned above, to the difficult *a priori* control and detail of all geometric degeneracies—and is already considered in the basic reference of [2].

The aim of this talk is to justify the specific interest of statements that, according to our terminology, are simultaneously *true on parts, false on parts* statements in the context of automated reasoning in geometry, pointing out the subtle, involved, issues deriving from the quirky algebraic behavior described in some of the examples above, as well as exhibiting a new, simpler way, of testing if a statement is true and false on parts, by just detecting if a pair of elimination ideals are zero or not. This test has been implemented in the dynamic geometry software GeoGebra and some illustrative examples can be found in `https://www.geogebra.org/m/zpDq7taB`.

This extended abstract is based on a recent work by the authors [5].

Keywords: geometry theorem proving and discovery, elementary geometry, Gröbner basis, elimination, true on components, GeoGebra

References

[1] F. BOTANA AND T. RECIO, On the unavoidable uncertainty of truth in dynamic geometry proving, *Mathematics in Computer Science* **10** (1), 5-25 (2016).

[2] S.C. CHOU, *Mechanical geometry theorem proving*, Mathematics and its Applications (41), D. Reidel Publishing Co., Dordrecht (1988).

[3] D.A. COX, J. LITTLE AND D. O'SHEA, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, 4th revised ed. Undergraduate Texts in Mathematics, Springer International Publishing, Switzerland (2015).

[4] G. DALZOTTO AND T. RECIO, On protocols for the automated discovery of theorems in elementary geometry, *Journal of Automated Reasoning* **43**, 203-236 (2009).

[5] Z. KOVÁCS, T. RECIO AND M.P. VÉLEZ, *Detecting truth, just on parts*, Preprint: arXiv: 1802.05875 [cs.AI] (2018).

[6] T. RECIO AND M.P. VÉLEZ, Automatic discovery of theorems in elementary geometry, *Journal of Automated Reasoning* **23**, 3-82 (1999).

[7] J. ZHOU, D. WANG AND Y. SUN, Automated reducible geometric theorem proving and discovery by Gröbner basis method, *Journal of Automated Reasoning* **59** (3), 331-344 (2017).

[1]Private Pädagogische Hochschule der Diözese Linz
Salesianumweg 3, 4020 Linz
zoltan@geogebra.org

[2]Universidad de Cantabria
Avda. de los Castros, s/n, 39005 Santander (Spain)
tomas.recio@unican.es

[3]Universidad Antonio de Nebrija
C/ Pirineos, 55, 28040 Madrid (Spain)
pvelez@nebrija.es