Symbolic Pattern Solving for Equational Reasoning

Olga Caprotti
Olga.Caprotti@risc.uni-linz.ac.at
RISC-Linz, Research Institute for Symbolic Computation,
J. Kepler University, Linz, Austria

Abstract

Symbolic pattern solving is a new approach for finding symbolic solutions of equational constraints over arbitrary algebraic structures. Despite the deep results and methods already produced in equational constraint solving, real-world applications still cannot be tackled. To reduce the original complexity, the approach advocated here uses the *solution pattern*, the skeleton of the solution often suggested by the problem instance. Pattern solving is successful if some substitution, of the unknown coefficients within the pattern, turns the pattern into a solution. The core of the method is the possibility of straightforward elimination of universally quantified variables from certain formulas related to the input problem and solution pattern. It is shown that fast elimination of universal quantifiers is complete in infinite integral domains, torsion-free modules over an infinite domain, finite dimensional division algebras over infinite fields, and in graded exterior algebras, if the underlying scalar field is infinite.

1 Motivation

This paper introduces a new approach for finding symbolic solutions of equational constraints over arbitrary algebraic structures [4]. Solving constraints symbolically in a specific algebraic structure means either deciding their truth, or finding terms of the language that, substituted for the free variables, make the constraints true. Intensive research, for instance in unification theory [5, 1] and in computer algebra [6], has produced a wealth of deep results and there are now several computational methods available. However, all this is not yet sufficient. The state of the art symbolic methods usually cannot tackle real-world applications. As soon as the problems increase in complexity, whether for the number of constraints, or their degree or for the number of symbols involved, the symbolic methods fail to perform as efficiently as the numeric methods do.

Depending on the algebraic structure, the complexity of symbolic solving of equational constraints ranges from polynomial-time decidable to undecidable. As example, take Hilbert's Tenth Problem: given a polynomial equation with integer coefficients, find whether there are solutions over some algebraic structure. The famous results of [7] and of [9] show that it is unsolvable over the integers and decidable over the real numbers. It is also believed to be undecidable over the rational numbers, where is still an open problem [8].

The basic observation leading to the method introduced here is that often the nature of the constraint solving problem at hand suggests a "skeleton" of the solution, a *solution pattern*. For instance, in the following problem from quantum chemistry, the typical question of expressing some implicitly defined quantity in terms of some other given quantities arises. The magnetic field produced by the apparent nuclear motion is:

$$\mathbf{B} = \frac{Ze}{cr^3} \cdot \mathbf{v_N} \times \mathbf{r}$$

when viewed from the electron, where $\mathbf{v_N}$ is the apparent velocity of the nucleus. From the laboratory view, the magnetic field of the nucleus of the electron is

$$\mathbf{B} = \frac{\mathbf{E} \times \mathbf{v}}{\mathbf{c}} = \frac{(Ze \cdot \mathbf{r}/r^3) \times \mathbf{v}}{c}$$

where $\mathbf{v}$ is the actual velocity of the electron. What is the relation between $\mathbf{v}$ and $\mathbf{v_N}$? The problem is solved if $\mathbf{v_N}$ can be expressed in terms of $\mathbf{v}$.

Moreover, skeletons of solutions are often available to engineers and physicists who "in practice" are more interested in solutions of a special form rather than in all solutions. They do not try to solve a problem by finding all solutions like the automatic methods do. Rather, they verify whether the expected solution is truly a solution and in this fashion they are able to deal with structures far more complex than those that can be tackled automatically.

When the problem instance provides a solution pattern, "solving" becomes partly "verifying" whether this pattern is indeed a solution. As a side effect, the complexity of constraint solving is reduced by requesting only solutions of a specific form and guiding the solving process through this pattern.

This paper formalizes this methodology, henceforth referred to as symbolic *pattern solving*, explains it, and derives an algorithm from it. Finally, it applies it to a problem of equational reasoning in quantum mechanics.

2 Symbolic Pattern Solving

To define a pattern solving problem, parametric solutions and solution patterns have to be defined. Parametric solutions are symbolic solutions in which some parameters occur. As these parameters vary over elements of the structure domain, so does the solution. Examples of parametric solutions are the most general unifiers for problems in equational theories and the rational parametrizations of algebraic curves for problems in fields of characteristic zero. Solution patterns are parametric solutions in which some coefficients are left unspecified. A pattern solving problem is then defined as follows.

GIVEN: $\mathfrak{A}$ a structure for an arbitrary signature Σ.

$\Gamma = \{t_1 = u_1, \ldots, t_n = u_n\}$ a system of equations among Σ-terms in variables X.

$\pi = \{x_1 \leftarrow \tau_1(Y, Z), \ldots, x_k \leftarrow \tau_k(Y, Z)\}$ a solution pattern in parameters Y and unknowns Z.

FIND: γ an *easily computable* ground term substitution for the unknowns Z such that $\pi \cdot \gamma$ is a parametric solution for Γ in the structure $\mathfrak{A}$, that is:

$$\mathfrak{A} \models (\forall Y) t_1\pi\gamma = u_1\pi\gamma \wedge \ldots \wedge t_n\pi\gamma = u_n\pi\gamma.$$

A substitution γ is easily computable if the corresponding system of equations is effectively solvable by using some available constraint solving method. An example is the computation of solutions of a system of polynomial equations by using the method of Gröbner basis [3, 2] in the case of zero-dimensional varieties. If a ground term substitution exists and can be effectively computed, then the solution pattern can be instantiated and pattern solving is successful. Otherwise, the method fails, which means that the proper pattern was not given.

The algorithm for solving symbolic constraints by solution patterns has a logical and an algebraic core. The "logical" core is the elimination of universally quantified variables from formulas related to the input problem and solution pattern. Pattern solving, in a specific algebraic structure, is effective only if the structure admits "straightforward" elimination of universal quantifiers for these specific formulas. In particular, the emphasis is on finding properties of the structure that allow efficient, fast elimination of universal quantifiers. The "algebraic" core is to solve a system of equations, related to the quantifier-free formula, for the unknown coefficients occurring in the solution pattern. The symbolic solution of this system, if it exists, yields an instance of the solution pattern that is a symbolic solution of the input problem. Since using a "good" pattern reduces the original complexity of the input problem, it is assumed that the resulting system of equations is simple enough to be effectively solvable by the available computational methods, specific to each algebraic structure.

Initially, the problem formula $\psi(Y, Z)$:

$$t'_1(Y, Z) = u'_1(Y, Z) \wedge \ldots \wedge t'_n(Y, Z) = u'_n(Y, Z) \tag{1}$$

is constructed by applying the solution pattern π to all terms $t_1, u_1, \ldots, t_n, u_n$ in the system of equations Γ. The problem formula $\psi(Y, Z)$ is the universal closure of the conjunction of the resulting equations. If the structure $\mathfrak{A}$ admits "straightforward" quantifier elimination for formulas having the form of $\psi(Y, Z)$, then an equivalent quantifier-free formula, $\phi(Z)$, in terms of the unknown coefficients only, can be obtained. This formula $\phi(Z)$ is such that:

$$\mathfrak{A} \models \forall Y \ \psi(Y, Z) \leftrightarrow \phi(Z). \tag{2}$$

If the quantifier-free formula $\phi(Z)$ is a conjunction of equations in the unknown coefficients, then the final step consists of finding a ground term solution for this system of equations. When a solution exists and can be easily computed by known techniques, the algorithm returns it and yields one instance of the solution pattern. If no solution exists, then the user is warned that no instance of the solution pattern is a parametric solution. If a solution cannot be easily computed, the user is asked for further information on the solution pattern.

For the procedure to be effective, the step of quantifier elimination must be done straightforwardly and without losing completeness. This is possible in many cases because it is an elimination of universal quantifiers only from a conjunction of equations. Even if the structure might not admit elimination of quantifiers in the general case, it can still admit a fast elimination of universal quantifiers for this particular type of formulas. These cases yield a practical overall algorithm. It turns out that fast elimination of universal quantifiers is complete in infinite integral domains, torsion-free modules over an infinite domain, finite dimensional division algebras over infinite fields, and in graded exterior algebras, if the underlying scalar field is infinite.

Summarizing, to perform pattern solving in an algebraic structure $\mathfrak{A}$, two ingredients must be available:

1. A fast method to eliminate universal quantifiers from universally quantified conjunctions equational constraints expressed in a many-sorted language.
2. An effective method to solve equational constraints in a ground term structure of $\mathfrak{A}$.

3 Equational Reasoning by Pattern Solving

Recall the quantum chemistry problem mentioned in the introductory motivation. The problem can be formalized as a pattern solving problem in vector spaces where a skew-commutative vector product $\times$ is defined. Fast elimination of universal quantifiers can be shown as is done for graded exterior algebras. The major difficulty with vector multiplication, as it is known in vector analysis, is that it is not associative. This problem can be side-stepped when all exterior terms occurring in the computation at most have total grade equal to two. In what follows, $\cdot$ denotes the multiplication by a scalar. Let the input system Γ be:

$$\{\mathbf{B} - \frac{Ze}{cr^3} \cdot \mathbf{v_N} \times \mathbf{r} = \mathbf{0}\}.$$

To simplify the denominator, assume the side condition: $cr^3 \neq 0$. The input becomes:

$$\{cr^3 \cdot \mathbf{B} - Ze \cdot \mathbf{v_N} \times \mathbf{r} = \mathbf{0}\}.$$

Let the solution pattern π:

$$\begin{aligned} \mathbf{v_N} &= \quad x \cdot \mathbf{v}, \\ \mathbf{B} &= \tfrac{(Ze \cdot \mathbf{r}/r^3) \times \mathbf{v}}{c} \end{aligned}$$

The vector parameter is $\mathbf{v}$, and $\mathbf{v_N}$, $\mathbf{B}$ are vector variables while $\mathbf{r}$ and r are constants defined elsewhere. After substitution of π in the problem Γ, the problem formula is:

$$\forall \mathbf{v}\ cr^3 \cdot \frac{(Ze \cdot \frac{\mathbf{r}}{\mathbf{r^3}}) \times \mathbf{v}}{c} - Ze \cdot (x \cdot \mathbf{v}) \times \mathbf{r} = \mathbf{0} \wedge cr^3 \neq 0.$$

Observe that the denominators appearing in the solution pattern do not introduce any side conditions beside the initial one. By simplifying the denominators:

$$\forall \mathbf{v}\ cr^3 \cdot (Ze \cdot \frac{\mathbf{r}}{\mathbf{r^3}}) \times \mathbf{v} - cZe \cdot (x \cdot \mathbf{v}) \times \mathbf{r} = \mathbf{0}.$$

$$\forall \mathbf{v}\ Ze \cdot \mathbf{r} \times \mathbf{v} - Ze \cdot (x \cdot \mathbf{v}) \times \mathbf{r} = \mathbf{0}.$$

Assuming the ordering on the exterior symbols: $\mathbf{v} < \mathbf{r}$, the formula can be reordered and rewritten as:

$$\forall \mathbf{v}\ (Ze + Zex) \cdot \mathbf{r} \times \mathbf{v} = \mathbf{0}.$$

Straightforward elimination of the quantifier yields:

$$(Ze + Zex) \cdot \mathbf{r} = \mathbf{0}.$$

Since the constant $\mathbf{r}$ is not zero, this is equivalent to:

$$Ze + Zex = 0$$

can be easily solved for x:

$$x = -1.$$

The solution pattern can be instantiated to a solution, assuming $cr^3 \neq 0$:

$$\mathbf{v}_\mathbf{N} = (-1) \cdot \mathbf{v} = -\mathbf{v}.$$

4 Conclusion

The results obtained so far are very promising and suggest that pattern solving applies to algebraic structures richer than those considered here. This will enable reasoning in complex domains arising from real-world applications. It will also be interesting to define the class of algebraic structures in which fast elimination of universal quantifiers is possible.

References

[1] Franz Baader and Jörg H. Siekmann. *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 2, chapter Unification Theory. Oxford University Press, 1994.

[2] T. Becker and V. Weispfenning. *Gröbner Bases: a Computational Approach to Commutative Algebra.* Graduate Texts in Mathematics. Springer–Verlag, 1993.

[3] B. Buchberger. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal.* PhD thesis, Universität Innsbruck, Institut für Mathematik, 1965. German.

[4] Olga Caprotti. *Symbolic Pattern Solving in Algebraic Structures.* PhD thesis, RISC-Linz, Research Institute for Symbolic Computation, March 1997.

[5] Jean-Pierre Jouannaud and Claude Kirchner. Solving Equations in Abstract Algebras: A Rule-Based Survey of Unification. In J.-L. Lassez and G. Plotkin, editors, *Computational Logic. Essays in honour of Alan Robinson*, chapter 8, pages 257–321. MIT Press, Cambridge, (MA) USA, 1991.

[6] Deepak Kapur and Yagiti N. Lakshman. *Symbolic and Numerical Computation for Artificial Intelligence*, chapter Elimination Methods: an Introduction, pages 45–87. Academic Press, 1992.

[7] Y. Matijasevič. Diophantine representation of recursively enumerable predicates. In *Actes du Congrès International des Mathématiciens*, volume 1, pages 235–238, Nice, France, 1970.

[8] Thanases Pheidas. Extensions of Hilbert's Tenth Problem. *Journal of Symbolic Logic*, 59(2):372–397, June 1994.

[9] A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* Univ. of California Press, Berkeley, second edition, 1951.