Enhanced CAD-Based Quantifier Elimination with Multiple Equational Constraints

James H. Davenport[1 [0000-0002-3982-7545]], Matthew England[2 [0000-0001-5729-3420]], and Scott McCallum[3 [0000-0002-5682-7993]]

[1] University of Bath, Bath, UK masjhd@bath.ac.uk
[2] Coventry University, Coventry, UK matthew.england@coventry.ac.uk
[3] Macquarie University, Sydney, Australia scott.mccallum@mq.edu.au

Abstract. We announce two enhancements to cylindrical algebraic decomposition based quantifier elimination for cases in which multiple equational constraints are present in the given input formula. The first enhancement provides more detail in the output when there is a partition of the set of variables of the formula into parameters and unknowns. The second enhancement is an efficiency gain due to a reduction of the second equational projection step, valid if certain conditions are met.

Keywords: Quantifier Elimination · Cylindrical Algebraic Decomposition · Equational Constraints.

1 Introduction

Quantifier elimination (QE) by cylindrical algebraic decomposition (CAD) is a general purpose symbolic computation tool for solving algebraic and geometric problems. While its many improvements have led to some success with its use in practical applications, there is room for further development of the method. Improvements which better address the requirements of special types of problems and take advantage of any favourable features of such problem types to reduce the amount of computation needed may be particularly beneficial. In this extended abstract we announce two enhancements to CAD based QE for situations in which multiple equational constraints (ECs) are present in the input formula and certain conditions are met. We indicate extensions of, and improvements to, our work which we expect will be achieved in the near future.

Let ϕ^* be a given prenex formula of Tarski algebra which has the form

$$(Q_{n-k+1}x_{n-k+1})\dots(Q_n x_n)\phi(x_1,\dots,x_n)$$

where ϕ is $f_1 = 0 \wedge \dots \wedge f_t = 0 \wedge \psi$, for some quantifier-free formula ψ. We call $\{f_1 = 0,\dots,f_t = 0\}$ the set of ECs of ϕ^*, and denote the number of free variables of ϕ^* by $s = n - k$. We suppose that an initial segment of the n variables of ϕ^* is naturally partitioned into $p \le s$ *parameters* and u *unknowns* thus: $x_1,\dots,x_p,x_{p+1},\dots,x_{p+u}$, with $p + u \le n$.

We suppose that it is of practical interest to express the unknowns in terms of the parameters. Thus, for our first enhancement, we aim to provide as output not just a quantifier-free formula which describes the truth set of ϕ^*, but a cell decomposition $\mathcal{D}_p$ of the parameter space $\mathbf{R}^p$ such that in each open cell of $\mathcal{D}_p$ the number of solutions (i.e. the number of associated vectors of unknowns) is a finite constant or is infinite. Moreover, for each cell of $\mathcal{D}_p$ having a finite constant number of solutions, we want to find an expression for the solutions in terms of the parameters. This extends the work reported in [6]. In the preliminary draft of our manuscript [3], we treat the case $p = s$ and $p + u = n$ in detail. Here it makes sense also to assume that $(Q_j x_j) = (\exists x_j)$, for every j. We plan to extend the cell decomposition framework of [3] to other cases soon.

Our second enhancement to CAD-based QE with multiple ECs is to identify an efficiency gain achievable in certain situations. Specifically, we report progress on the validation of Collins' original, fully reduced CAD equational projection operation beyond its existing validation for the first projection step [7], [4]. Provided certain conditions are met, we show in [3] that the second projection step can be reduced more significantly than existing theory [4] allows. We think there is scope to go further still, as explained in detail in [3].

2 Background material

Where A is a set of integral polynomials in $x_1, \ldots, x_n$, an A-invariant *cylindrical algebraic decomposition (CAD)* is a decomposition of $\mathbf{R}^n$ into cells (connected subsets), each of which is semi-algebraic, that are arranged cylindrically, and such that each element of A is sign-invariant in every cell. The concept is due to Collins [1], who also gave the first algorithm for constructing an A-invariant CAD for a given set A. We can also talk more generally of a *truth-invariant* CAD where the truth of a Boolean combination of polynomial sign conditions is invariant in each cell. See [3, § 2] for a survey of CAD and its variants, and see [7] for the definitions of technical terms used below such as submanifold, analytic delineability and order-invariance.

3 Framework for enhanced CAD-based QE for parametric systems with many ECs

In Section 3 of [3] we present a CAD-based method for finding generic solutions of a parametric system given by a quantified formula ϕ^* as described in the Introduction (recall that $p = s$ and $p + u = n$ in this setting). There are two parts to our presentation of the method: first, we state and prove a foundational result [3, Prop. 2]; and second, we present a formal algorithm description. Our foundational result, in part, is stated as follows.

Proposition 1. *Let $\mathcal{D}$ be a truth-invariant CAD of $\mathbf{R}^n$ for ϕ and let $\mathcal{D}_s$ denote the CAD of $\mathbf{R}^s$ induced by $\mathcal{D}$. Let c be a cell of $\mathcal{D}_s$, and let $\alpha \in c$. Then the total number $\nu_{c,\alpha}$ of distinct solution vectors $\beta \in \mathbf{R}^k$ for ϕ associated with α is an element of $\mathbf{N} \cup \{\infty\}$, constant as α varies in c: hence we can put $\nu_c = \nu_{c,\alpha}$.*

Our formal algorithm description takes as input a formula ϕ^* with $p = s$ and $p + u = n$, and yields as output a description of the cells of the CAD $\mathcal{D}_s$ of $\mathbf{R}^s$ induced by a truth-invariant CAD $\mathcal{D}$ of $\mathbf{R}^n$ for ϕ, and lists $\mathcal{N}$ of numbers ν_c, for each cell c of $\mathcal{D}_s$ (where ν_c is defined by the above proposition), and $\mathcal{F}$ of suitable functional expression lists F_c, for each such cell c.

4 Progress validating fully reduced equational projection

In Section 4 of [3] we present variations of existing theorems relating to delineability. These are of help in justifying the use of the fully reduced equational projection operation beyond the first projection step in certain special situations, consistent with the framework mentioned in the previous section.

The new theory relies upon the notion of the order of a real analytic function $g(x_1, \ldots, x_n)$ relative to the real variety V_f of another real analytic function $f(x_1, \ldots, x_n)$ at a non-singular point p of V_f. This notion is defined informally as follows. Since p is assumed to be non-singular for V_f, some first order partial derivative $\partial f/\partial x_i$ does not vanish at p. Then, by the implicit function theorem, V_f is represented near p by the graph of a real analytic function $x_i = \phi(x_1, \ldots, \hat{x}_i, \ldots, x_n)$ (where $\hat{x}_i$ denotes omission of the variable x_i). The reader is alerted that this is a new use of the symbol ϕ compared with its usage in previous sections. We say that g has order $k \in \mathbf{N} \cup \{\infty\}$ relative to V_f at p if the order of the real analytic function,

$$g(x_1, \ldots, x_{i-1}, \phi(x_1, \ldots, \hat{x}_i, \ldots, x_n), x_{i+1}, \ldots, x_n), \tag{1}$$

at $(p_1, \ldots, \hat{p}_i, \ldots, p_n)$ is k. We shall denote the order of g relative to V_f at p by $\mathrm{ord}_p g|_{f=0}$. In [3], it is argued that this notion is well-defined.

In Section 4.2 of [3], we state and prove a trilogy of theorems relating to delineability which use the concept of relative order introduced above. Here we state the first theorem of the trilogy [3, Thm. 2].

Theorem 1. *Let $f(x_1, \ldots, x_n) \in \mathbf{R}[x_1, \ldots, x_n]$ be a real polynomial of positive degree in x_n, and let $e(x_1, \ldots, x_{n-1}) \in \mathbf{R}[x_1, \ldots, x_{n-1}]$ be a real polynomial of positive degree in x_{n-1}. Let $d(x_1, \ldots, x_{n-1})$ and $a(x_1, \ldots, x_{n-1})$ be the discriminant and the leading coefficient of f, respectively, both with respect to x_n, suppose that d is a non-zero polynomial, and suppose that e and d are relatively prime. Let σ be a connected submanifold of $\mathbf{R}^{n-1}$ contained in the real hypersurface (variety) defined by $e = 0$ in which a is sign-invariant and f vanishes identically at no point. Suppose that σ contains no singular point of the real hypersurface defined by $e = 0$ and that the order of $d|_{e=0}$ is invariant in σ.*

Then f is analytic delineable on σ.

The other two theorems referred to above involve small though significant changes to the hypotheses and conclusions. A separate detailed proof is provided for each theorem in [3].

Finally, in Section 4.3 of [3], we state and prove a result ([3, Thm. 5]), combining the trilogy of theorems mentioned, which states conditions under which the fully restricted projection operation for e can be used for the second projection step, as it can for$f$ in the first projection step [7]. The key conditions are: (1) f and e are well-placed [3], (2) codim $S \leq 1$ [3], and (3) V_e is non-singular.

Section 5 of [3] provides detailed discussions of two relevant worked examples: the solution of a parametric system first introduced in [5], and Solotareff's approximation problem [2]. We observe that the new theory described in Section 4 above validates the intuitive approach used to solve Solotareff's problem in [2].

5 Summary

In summary, we have announced two enhancements to CAD-based QE when multiple ECs are present, given in full detail in [3]. In the future we will explore further enhacements, and comparison with the work on border polynomial in [8] and C.W. Brown's work on *restricted order* presented at SYNASC 2023, which is similar to, but more general than, the concept of relative order defined above.

Acknowledgments. JHD and ME were supported by the EPSRC DEWCAD Project, "*Pushing Back the Doubly-Exponential Wall of Cylindrical Algebraic Decomposition* (grant EP/T015713/1 and EP/T015748/1), as was SMcC's visit to the UK.

Disclosure of Interests. The authors have no competing interests to declare.

References

1. Collins, G.E.: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Brakhage, H. (ed.) Proceedings of 2nd GI Conference on Automata Theory and Formal Languages. Lecture Notes in Computer Science, vol. 33, pp. 134–183. Springer-Verlag (1975), `https://doi.org/10.1007/3-540-07407-4_17`
2. Collins, G.E.: Application of quantifier elimination to Solotareff's approximation problem. In: Jeltsch, R., Mansour, M. (eds.) Stability Theory. ISNM International Series of Numerical Mathematics, vol. 121, pp. 181–190. Birkhäuser Basel (1996), `https://doi.org/10.1007/978-3-0348-9208-7_19`
3. Davenport, J., England, M., McCallum, S.: Enhanced CAD-based quantifier elimination with multiple equational constraints – preliminary draft. Preprint: arXiv 2604.23873 (2026), `https://doi.org/10.48550/arXiv.2604.23873`
4. England, M., Bradford, R., Davenport, J.H.: Cylindrical algebraic decomposition with equational constraints. J. Symbolic Computation **100**, 38–71 (2020), `https://doi.org/10.1016/j.jsc.2019.07.019`
5. Fortuna, E., Gianni, P., Trager., B.: Degree reduction under specialization. J. Pure and Applied Algebra **164**, 153–163 (2001), `https://doi.org/10.1016/S0022-4049(00)00151-1`
6. Lazard, D., Rouillier, F.: Solving parametric polynomial systems. J. Symbolic Computation **42**(6), 636–667 (2007), `https://doi.org/10.1016/j.jsc.2007.01.007`
7. McCallum, S.: On projection in CAD-based quantifier elimination with equational constraint. In: Dooley, S. (ed.) Proceedings of ISSAC'99. pp. 145–149. ACM Press (1999), `https://doi.org/10.1145/309831.309892`
8. Moreno Maza, M., Xia, B., Xiao, R.: On solving parametric polynomial systems. Mathematics in Computer Science **6**(4), 457–473 (2012), `https://doi.org/10.1007/s11786-012-0136-3`