EPiC Series in Computing

Volume 53, 2018, Pages 1–8

Vampire 2017. Proceedings of the 4th Vampire Workshop

Theorem recycling for Theorem Proving

Nikolaj Bjørner and Lev Nachmanson

Microsoft Research

Abstract

In this paper we examine two cases where solutions to one system of constraints can be used or adapted to solutions to others, for free. We first revisit a method by Bromberger for lifting solutions to systems over linear real arithmetic to solutions over integers. We extend it by identifying several scenarios where solutions over reals can be directly used to establish solutions over integers. Our second case discusses *model-based projection*, which was introduced in two different places with different, dual, definitions. It turns out that one can typically use the same underlying engines to compute both versions of model based projection and we characterize when this is the case. We extend projection with *model-based realization*. When used for quantifier reasoning, it serves a complementary purpose than projection. While projection can be used for computing conflict clauses, realizers may be used for forward pruning.

1 Introduction

Z3 [7] has found several applications that involve program analysis, testing and verification. It integrates several theories that are commonly encountered in these domains. While recognized as all round efficient the quest for scale and further efficiency remains. We are currently revising Z3's arithmetic solver addressing long standing limitations: the new arithmetic solver comes with a scalable revised Simplex implementation that can switch between arbitrary precision arithmetic, for certified results, and floating point arithmetic, for efficiency. It includes also a solver based on dual Simplex which remains the engine that is most effective on typical applications from the SMT domain. For linear real arithmetic, the new solver has been used as default in Z3's distribution since spring of 2017 and solves overall 40% more problems that the previous version. We are currently extending the improvements to linear integer arithmetic. Furthermore, in contrast to the previous solver, it now supports an integration with non-linear polynomial arithmetic which is complete for signature disjoint theory combinations. One of the deciding factors in leapfrogging the previous solver in number of benchmarks solved included so far an integration with the method by Bromberger and Weidenbach [3],[4] to detect integer feasible solutions from strengthened inequalities. We observed that the default strengthening proposed by Bromberger and Weidenbach can often be avoided: integer solutions can be guaranteed from weaker systems. We conjecture that polynomial time decidable fragments of integer linear arithmetic are generally amenable to elementary conversions from real solutions to either integer solutions or polynomial size certificates that there are no integer solutions. We prove this conjecture in the cases of bounded variables, difference arithmetic, unit two variables per

inequality (often called the octagon domain), and for unit horn inequalities. We leave the more general cases of (non-unit) two-variable per inequalities and non-unit Horn inequalities open.

2 Cubes

In the following we let A, A' range over integer matrices and a, b, c over integer vectors. The 1-norm $\|A\|_1$ of a matrix is a column vector, such that each entry i is the sum of the absolute values of the elements in the corresponding row A_i. We write $\|A_i\|_1$ to directly access the 1-norm of a row.

A (unit) *cube* is a polyhedron that is a Cartesian product of intervals of length one for each variable. Since each variable therefore contains an integer point, the interior of the polyhedron contains an integer point. The condition for a convex polyhedron to contain a cube can be recast as follows:

Proposition 1 ([3])**.** *If $Ax \leq b - \frac{1}{2}\|A\|_1$ has a solution over the reals, then $Ax \leq b$ has an integer solution.*

Proof. Given a feasible solution to the strengthened system we extract integer values that satisfy the original constraints as follows.

$$\hat{x} \quad = \quad \begin{cases} \lfloor x \rfloor & \text{if } x - \lfloor x \rfloor \leq \frac{1}{2} \\ \lceil x \rceil & \text{otherwise} \end{cases} \tag{1}$$

The original constraints $Ax \leq b$ are satisfied because the value at each row i is shifted by at most $\frac{1}{2}\|A_i\|_1$, that is, $A\hat{x} \leq Ax + \frac{1}{2}\|A\|_1$, and therefore if $Ax \leq b - \frac{1}{2}\|A\|_1$, then $A\hat{x} \leq b$. □

Example 1. *Suppose we have $3x + y \leq 9 \wedge -3y \leq -2$ and wish to find an integer solution. By solving $3x + y \leq 9 - \frac{1}{2}(3 + 1) = 7, -3y \leq -2 - \frac{1}{2}3 = -3.5$ we find a model where $y = \frac{7}{6}, x = 0$. After rounding y to 1 and maintaining x at 0 we obtain an integer solution to the original inequalities.*

2.1 Special Inequalities

Definition 1 (Difference Matrix)**.** *We say that D is* difference matrix *if it comprises of entries over $-1, 0, 1$ and every row contains at most one entry with value -1 and at most one entry with value 1.*

Proposition 2. *If $Ax \leq b - \frac{1}{2}\|A\|_1, Dx \leq c$ has a solution over the reals, then $Ax \leq b, Dx \leq c$ has a solution over the integers.*

Proof. Given values for x that satisfy the inequalities $Ax \leq b - \frac{1}{2}\|A\|_1, Dx \leq c$ we use the same rounding as in the proof of Proposition 1. The updated values to x satisfy the difference constraints because for each row d_i in D, the difference between $d_i x$ and $d_i \hat{x}$, that is $|d_i \cdot (x - \hat{x})|$, is strictly less than 1 (to achieve a maximal value, one coordinate has to be rounded down, while the other is rounded up, their net difference is below 1). As the result of rounding is integral, the same integral inequalities with c are satisfied. □

We can extend the result from difference constraints to Horn constraints.

Definition 2 (Integer Horn Matrix)**.** *An integer matrix H is said to be* Horn *if every row contains at most one negative entry. The only legal value to negative entries is the value -1.*

Example 2. $3x+3y-z \leq 7$ *and* $3x+y \leq 7$ *are Horn, but* $3x+3y-z-u \leq 7$ *and* $3x+3y-2z \leq 7$ *are not.*

Proposition 3. *If* $Ax \leq b - \|A\|_1, Hx \leq c$ *has a solution over the reals, then* $Ax \leq b, Hx \leq c$ *has a solution over the integers.*

Proof. We have tightened bounds on non-Horn constraints as our proof requires adapting a strategy of always rounding non-integral values down. By consistently rounding down, the contributions from non-negative coefficients in H are reduced. The contribution from the negative coefficients in H may be increased, but only by values strictly below 1. As the result of rounding is integral, and is shifted by a value less than 1 upwards, the integral bounds c, remain upper bounds. Formally, we have $H\lfloor x \rfloor < Hx+1$ and since $Hx \leq c$, where c is integral, it follows that $H\lfloor x \rfloor < c+1$ and therefore $H\lfloor x \rfloor \leq c$. □

A minimal scenario where the difference $|a_i x - a_i \hat{x}|$ is not strictly less than 1 is the case where a_i contains two entries that are 1 and all other are 0. For example $x + y \geq 1$ is satisfied by $x = y = \frac{1}{2}$, but rounding x and y produces values for x and y that no longer satisfy the inequality. We will establish that this minimal case can also be saved, but this time requires to sometimes round up instead of down from values that are at the mid-point between two integers.

Definition 3 (Octagon Matrix)**.** *We say that O is an* octagon matrix *if it comprises of entries over $-1, 0, 1$ and every row has at most two non-zero entries.*

Example 3. $x - y \leq 2, z + u \leq 4, -x - z \leq -2$ *are octagon inequalities.*

Definition 4 (Alternating rounding)**.** *An alternating rounding justification is an inequality $\pm x + \pm y \leq k$, such that both x and y have values at the midpoint 0.5 and rounding x up requires rounding y down and conversely.*

A notation that suggests the dependencies is as follows: $\underline{x} \xrightarrow{-x+y\leq k} \underline{y}$ is used to track when rounding x down forced y to be rounded down. Similarly, $\overline{y} \xrightarrow{-x+y\leq k} \overline{x}$, and $\overline{x} \xrightarrow{x+y\leq k} \underline{y}$, etc.

Definition 5 (Infeasible Cycle)**.** *Given an octagon matrix O and a valuation of v satisfying $Ov \leq c$, we say v certifies an infeasible cycle if*

1. *v satisfies all inequalities.*
2. *There is a subset of tight inequalities where both values are at the midpoint 0.5.*
3. *The subset labels a cycle that contain vertices labeled by both $\underline{x}$ and $\overline{x}$ for some x.*

Example 4. *Suppose we have inequalities $0 \leq x-y \leq 0, 1 \leq x+y \leq 1$. They have the rational solution $x = y = \frac{1}{2}$, but no integer solution. The corresponding dependencies are*

$$\overline{x} \xrightarrow{x-y\leq 0} \overline{y} \quad \overline{x} \xrightarrow{x+y\leq 1} \underline{y} \quad \underline{y} \xrightarrow{x-y\leq 0} \underline{x} \quad \overline{y} \xrightarrow{x+y\leq 1} \underline{x} \quad \underline{x} \xrightarrow{0\leq x-y} \underline{y} \quad \underline{x} \xrightarrow{1\leq x+y} \overline{y} \quad \overline{y} \xrightarrow{0\leq x-y} \overline{x} \quad \underline{y} \xrightarrow{1\leq x+y} \overline{x}$$

and we see they contain an infeasible cycle as follows:

$$\overline{x} \xrightarrow{x+y\leq 1} \underline{y} \xrightarrow{x-y\leq 0} \underline{x} \xrightarrow{1\leq x+y} \overline{y} \xrightarrow{0\leq x-y} \overline{x}$$

Example 5. *Let us weaken the inequalities by removing* $1 \leq x + y$. *That is, we are given the inequalities* $0 \leq x - y \leq 0, x + y \leq 1$ *and dependencies*

$$\overline{x} \xrightarrow{x-y\leq 0} \overline{y} \quad \overline{x} \xrightarrow{x+y\leq 1} \underline{y} \quad \underline{y} \xrightarrow{x-y\leq 0} \underline{x} \quad \overline{y} \xrightarrow{x+y\leq 1} \underline{x} \quad \underline{x} \xrightarrow{0\leq x-y} \underline{y} \quad \overline{y} \xrightarrow{0\leq x-y} \overline{x}$$

There is a path from $\overline{x}$ *to* $\underline{x}$, *but no path in the reverse direction.*

$$\overline{x} \xrightarrow{x+y\leq 1} \underline{y} \xrightarrow{x-y\leq 0} \underline{x}$$

Suppose we are given the values $x = y = \frac{1}{2}$. *We can round both* x *and* y *down to* 0 *and still satisfy the inequalities.*

Proposition 4. *If* $Ax \leq b - \frac{1}{2}\|A\|_1, Ox \leq c$ *has a solution over the reals, then* $Ax \leq b, Ox \leq c$ *has a solution over the integers, or the real solution to* $Ox \leq c$ *contains an integer infeasible cycle.*

Proof. To prove the proposition we describe a procedure that computes a rounding for x or fails with an integer infeasible cycle. We start with an evaluation $\hat{x}$ that rounds down when $x - \lfloor x \rfloor = \frac{1}{2}$. If there is an octagon inequality in $Ox \leq c$ that is not satisfied by this assignment, it must necessarily be due to two values that are at the mid-point. Choose one of the two variables and round it up instead and record the inequality where it occurred as the justification for this change in rounding strategy. Perform these flips repeatedly. Every time a choice has to be taken between two variables to flip, choose the least recently flipped variable; the justification for flipping the least recently used variable includes the inequality and the justification for flipping the other variable. An infeasible cycle establishes integer infeasibility. □

Note that our procedure is naïve as it does not provide a small bound on the number of flips. We can do better by flipping variables along a topological sort. We omit the details.

There are several other classes of linear arithmetic that would merit examination: can one extract, cheaply, an integral solution from a rational solution without strengthening bounds? The class of non-unit two-variable per inequality (TVPI) was solved in a low order polynomial time in [5]. While their result speaks for the case where variables range over reals, the same phenomena that are crucial for the algorithm are replicated for integers: upper and lower bounds on variables can be computed from loops (and it is not necessary to examine all exponentially bounded number of loops). We also leave extracting integer solutions for the related class of non-unit Horn inequalities open.

2.2 On the complexity of solving linear integer arithmetic

The original argument that establishes NP membership of ILP shows directly that every solvable set of inequalities have a small (polynomial size) solution. We can use bound strengthening as a tool to establish NP membership by guessing a solution of bounded polynomial size or creating an LP problem.

1. Given a set of inequalities $Ax \leq b$, guess a subset A', b', and constants k such that $A'x = b' - k$. We bound the size of the constants to $(\|A\|_1)^n$, where n are the number of variables.

2. The selected equalities are solved by computing a matrix H in Hermite normal form and totally uni-modular matrix U, such that $H = A'U^{-1}$, thus $Hx = U^{-1}b'$.

3. The lower triangular matrix H provides solutions for a subset of variables from x. The coefficients in H's diagonal need not be integral, for example it may solve for x_0 as $3x_0 = 5x_1 + 8x_2 + 2$. We can remove the non-unit coefficient to x_0 by replacing x_1 by $3x'_1 + k_1$ and x_2 by $3x'_2 + k_2$, where $0 \leq k_1, k_2 \leq 2$ are guessed. This transformation increases the coefficients in the linear system by $(\|A\|_1)^n$.

4. The remaining linear system is a set of inequalities $A''x \leq b''$. For those we check for a solution to $A''x \leq b - \frac{1}{2}\|A''\|_1$.

Note that the approach splits solutions to inequalities into two camps: those that are between $b - \frac{1}{2}\|A''\|_1$ and b and those that are below.

3 Universal and Existential Model-based projection

We will now switch gears and examine procedures for computing quantifier free formulas, or as we will say, projecting variables. We are interested in compute under-approximations of projections for both universally and existentially quantified formulas. Projections of universal formulas correspond to half-interpolants and are instrumental for model-based search techniques where it is convenient to extract conflict clauses based on a subset of variables. Existential projection is useful when checking satisfiability of quantified formulas [1] and satisfiability of Horn clauses, or more generally, when constructing a sequence of resolutions. Both scenarios engage in a model construction search and have a candidate partial model available to focus the search for relevant under-approximations.

Example 6. *In the following we will introduce the function $Mbp(M, x, L)$ by example, where M is an interpretation, x a variable and L a conjunction of literals containing x. Want to compute small formula that implies $\exists x \,.\, (2y \leq x \wedge y - z \leq x \wedge x \leq z)$. First note that the formula is equivalent to the quantifier-free version as follows:*

$$\exists x \,.\, (2y \leq x \wedge y - z \leq x \wedge x \leq z) \quad \equiv \quad (y - z \leq 2y \leq z) \vee (2y \leq y - z \leq z)$$

Suppose we have a model $M = [x \mapsto 3, y \mapsto 1, z \mapsto 6]$ and we wish to compute

$$Mbp(M, x, 2y \leq x \wedge y - z \leq x \wedge x \leq z)$$

In this case $2y^M = 2$, $(y - z)^M = -5$. So $2y > y - z$ is true under M. Then

$$Mbp(M, x, 2y \leq x \wedge y - z \leq x \wedge x \leq z) \quad = \quad y - z \leq 2y \leq z$$

Note that the result satisfies our desired property

$$y - z \leq 2y \leq z \;\Rightarrow\; \exists x \,.\, (2y \leq x \wedge y - z \leq x \wedge x \leq z)$$

3.1 Model-based Projection for Linear Real Arithmetic

MBP is particularly easy to define for linear real arithmetic. It works as a specialization of the Loos-Weispfenning [9] quantifier elimination procedure by selecting a conjunction that is satisfied under M. It can be defined by cases:

Eliminate $\simeq, \not\simeq$ from conjunction of literals L:

$$\begin{array}{lcll} Mbp(M, x, x \simeq t \wedge L) & = & L[t/x] & \text{if } x \notin FV(t) \\ Mbp(M, x, x \not\simeq t \wedge L) & = & Mbp(M, x, x > t \wedge L) & \text{where} \quad M(x) > M(t) \end{array}$$

We can use infinitesimals, ϵ, to turn $>$ into $\geq$.

$$Mbp(M, x, x > t \wedge L) \quad = \quad Mbp(M, x, (x \geq t + \epsilon) \wedge L)$$

Having applied the previous steps exhaustively we can now assume x occurs only as upper or lower bounds:

$$Mbp(M, x, \bigwedge_i t_i^m \leq x \wedge \bigwedge_j^n x \leq s_j) \quad = \quad \bigwedge_i t_i \leq t_0 \wedge \bigwedge_j t_0 \leq s_j \quad \text{where} \quad m \leq n,\ M(t_0) \geq M(t_i) \forall i$$

3.2 Model-based projections, two lenses

The formal requirements for MBP are provided in the following. Sat based (existential) MBP [8] requires:

- Given: $M \models \ell_1[x] \wedge \ldots \wedge \ell_n[x]$
- Find: $M \models s_1 \wedge \ldots \wedge s_m$, free for x
- Such that: $\models (s_1 \wedge \ldots \wedge s_m) \rightarrow \exists x \ . \ \ell_1[x] \wedge \ldots \wedge \ell_n[x]$

Contrast this with Core-based (universal) MBP [6], where the requirements are:

- Given: $M \models \forall x \ . \ \ell_1[x] \vee \ldots \vee \ell_n[x]$.
- Find: $M \models s_1 \wedge \ldots \wedge s_m$, free for x
- Such that: $\models (s_1 \wedge \ldots \wedge s_m) \rightarrow \forall x \ . \ \ell_1[x] \vee \ldots \vee \ell_n[x]$

Sat- and core-based MBP are not vacuously interchangeable. For example $\forall x \ . \ y \leq x \ \vee \ u \leq x \ \vee \ y < z$ has the projection $y < z$ (which does not contain x), but a related existential projection would need a relation between y and u. The condition for when one can use the same projection method for both cases is spelled out in the proof of the following (easy) proposition.

Proposition 5. *The same projection operator can be used in both cases if x occurs in all literals and the operator is stable under changes to the value of x.*

Proof. We can assume a quantifier elimination procedure that takes a conjunction and eliminates variables producing a DNF as follows

$$\exists x \ . \ \bigwedge_i \ell_i \quad \equiv \quad \bigvee_i \bigwedge_j s_{ij} \tag{2}$$

thus, equivalently

$$\forall x \,.\, \bigvee_i \neg \ell_i \quad \equiv \quad \bigwedge_i \bigvee_j \neg s_{ij} \tag{3}$$

In the existential case, model-based projection selects a conjunction i, such that $\wedge_j s_{ij}$ is true. In the universal case, model-based projection selects one disjunct from every conjunct i, such that $\neg s_{ij}$ is true under the model. The resulting selections imply the existential, respectively, universal formulas. □

Could conversely extract consequences true in M by selecting s_{ij}, respectively $\neg s_{ij}$ from (3), that are true under M.

3.3 Model-based Realization

In addition to projection, a closely related concept of *realization* can be used to solve quantified formulas. It was proposed under the guise of strategies in [1, 2], and a clever and performant method for extracting strategies was developed for 2-QBF in [10]. The starting point for realization is a setting where we are faced with solving a formula with alternating quantifiers

$$\forall x \,.\, \exists y \,.\, F[x,y] \quad \text{or} \quad \exists x \,.\, \forall y \,.\, G[x,y] \;.$$

When establishing satisfiability, a solver produces in the limit a realizer function $f(x)$ such that $\forall x \,.\, F[x, f(x)]$, or a function $g(x)$ such that $\forall x \,.\, \neg G[x, g(x)]$. We will show how portions of a realizer can be extracted using models.

Define model-based realizer Mbr similar to Mbp, but with the main case as follows:

$$Mbr(M, x, \bigwedge_i^m t_i \leq x \wedge \bigwedge_j^n x \leq s_j) \quad = \quad \begin{cases} t_0 & \text{where} \quad m \leq n,\ M(t_0) \geq M(t_i) \quad \forall i \\ s_0 & \text{where} \quad m > n,\ M(s_0) \leq M(s_j) \quad \forall j \end{cases}$$

alternatively to take into account strict inequalities,

$$Mbr(M, x, \bigwedge_i^m t_i \leq x \wedge \bigwedge_j^n x \leq s_j) \quad = \quad \frac{t_0 + s_0}{2} \quad M(t_0) \geq M(t_i) \forall i, \quad M(s_0) \leq M(s_j) \forall j$$

and alternatively, a stronger realizer is given by:

$$Mbr(M, x, \bigwedge_i^m t_i \leq x \wedge \bigwedge_j^n x \leq s_j) \quad = \quad \frac{\max_i t_i + \min_j s_j}{2}$$

As with quantifier elimination, the size of the such a realizer grows proportional to the product of number of inequalities and variables. The realizer that projects either t_0 or s_0 does not incur this overhead.

Suppose $M \models F[x_0, y]$ for some fixed x_0 and let $L[x, y]$ be an implicant (conjunction) that implies $F[x, y]$ for $x = x_0$. Set $f(x) := Mbr(M, y, L)$. The universal player will have to solve $\neg F[x, f(x)]$ instead of the easier to satisfy formula $\neg F[x, y]$.

On the other hand, suppose $M \models \neg G[x_0, y]$ for some fixed x_0. Then let $L[x, y]$ be an implicant for $\neg G[x, y]$ for $x = x_0$. Set $g(x) := Mbr(M, y, L)$ and the existential player will have to solve $G[x, g(x)]$ instead of the easier $G[x, y]$.

4 Summary

We examined two topics in decision procedures that involve integer linear arithmetic and quantifier reasoning, respectively. They shared a common theme of having transfer properties: theorems established in one setting were applicable in a wider scope. We demonstrated how conditions for integer feasibility from [3] could be relaxed for inequalities coming from special fragments of arithmetic. We examined two related notions of model-based projection and characterized the case where they coincide. Finally, a first attempt was outlined for formulating model-based realization with an example in the context of linear real arithmetic. As demonstrated in the case of 2-QBF in [10], model-based realizers have a potential to advance scalability of quantifier reasoning.

References

[1] Nikolaj Bjørner and Mikolás Janota. Playing with alternating quantifier satisfaction. In *LPAR Short presentation papers*, 2015.

[2] Nikolaj Bjørner, Mikolás Janota, and William Klieber. On conflicts and strategies in QBF. In *20th International Conferences on Logic for Programming, Artificial Intelligence and Reasoning - Short Presentations, LPAR 2015, Suva, Fiji, November 24-28, 2015.*, pages 28–41, 2015.

[3] Martin Bromberger and Christoph Weidenbach. Fast cube tests for LIA constraint solving. In Nicola Olivetti and Ashish Tiwari, editors, *Automated Reasoning - 8th International Joint Conference, IJCAR 2016, Coimbra, Portugal, June 27 - July 2, 2016, Proceedings*, volume 9706 of *Lecture Notes in Computer Science*, pages 116–132. Springer, 2016.

[4] Martin Bromberger and Christoph Weidenbach. New techniques for linear arithmetic: cubes and equalities. *Formal Methods in System Design*, 51(3):433–461, 2017.

[5] Edith Cohen and Nimrod Megiddo. Improved algorithms for linear inequalities with two variables per inequality (extended abstract). In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 145–155. ACM, 1991.

[6] Leonardo Mendonça de Moura and Dejan Jovanovic. A model-constructing satisfiability calculus. In *Verification, Model Checking, and Abstract Interpretation, 14th International Conference, VMCAI 2013, Rome, Italy, January 20-22, 2013. Proceedings*, pages 1–12, 2013.

[7] Leonardo Mendonça de Moura and Nikolaj Bjørner. Z3: An Efficient SMT Solver. In *TACAS*, 2008.

[8] Anvesh Komuravelli, Arie Gurfinkel, and Sagar Chaki. Smt-based model checking for recursive programs. In *CAV*, pages 17–34, 2014.

[9] Rüdiger Loos and Volker Weispfenning. Applying linear quantifier elimination. *Comput. J.*, 36(5):450–462, 1993.

[10] Markus N. Rabe and Sanjit A. Seshia. Incremental determinization. In Nadia Creignou and Daniel Le Berre, editors, *Theory and Applications of Satisfiability Testing - SAT 2016 - 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings*, volume 9710 of *Lecture Notes in Computer Science*, pages 375–392. Springer, 2016.