Electronic Notes in Theoretical Computer Science 198 (2008) 37–49 

[www.elsevier.com/locate/entcs](http://www.elsevier.com/locate/entcs)

Model-based Theory Combination

# Leonardo de Moura[1](#_bookmark0) Nikolaj Bjørner[2](#_bookmark0)

*Microsoft Research, One Microsoft Way, Redmond, WA, 98074, USA*

Abstract

Traditional methods for combining theory solvers rely on capabilities of the solvers to produce all implied equalities or a pre-processing step that introduces additional literals into the search space. This paper introduces a combination method that incrementally reconciles models maintained by each theory. We evaluate the practicality and efficiency of this approach.

*Keywords:* Theory Combination, Decision Procedures, SMT.

# Introduction

A core problem of Satisfiability Modulo Theories is combining separate theory solvers for theories T 1 and T 2 to a combined solver for the union T 1 ∪T 2. The Nelson-Oppen combination method identifies sufficient conditions for combin- ing two theories over disjoint signatures: only (disjunctions of) equalities over shared variables that are implied by one of the theories need to be communi- cated. Most existing implementations and optimizations of this method seek to efficiently implement the trigger:

if T *i* ∪ Γ*i* |= *u* *v* then propagate *u* *v*,

to exhaustively enumerating all implied (disjunctions of) equalities for a the- ory T *i* and constraints Γ*i* that are asserted in its context. Another method

[[4](#_bookmark13)] to obtain completeness is by enumerating equalities corresponding to the

1 Email: [leonardo@microsoft.comu](mailto:leonardo@microsoft.com)

2 Email: [nbjorner@microsoft.com](mailto:nbjorner@microsoft.com)

1571-0661 © 2008 Elsevier B.V. Open access under [CC BY-NC-ND license](http://creativecommons.org/licenses/by-nc-nd/3.0/).

doi:10.1016/j.entcs.2008.04.079

cross-product of all shared variable pairs and use the SAT solver for non- deterministically choosing a partition based on the cross-product. Common to these methods is that they are pessimistic about which equalities are propa- gated. A more optimistic approach is by inspecting a candidate model M*i* for one of the theories T *i* and propagate all equalities implied by the candidate model, hedging that other theories will agree. If not, use backtracking to fix the model. Thus, Model-based Theory Combination is based on a trigger of the form:

if M*i* |= T *i* ∪ Γ*i* ∪ {*u* *v*} then propagate *u* *v* .

The rationale for Model-based Theory Combination is practical: It tends to be much cheaper to enumerate equalities that are implied in a particular model than of all models; the number of inter-theory equalities that really matter is small in practice (intra-theory equality propagation on the other hand does matter); backtracking is relatively cheap with modern DPLL solvers; and finally, one may limit the number of equalities implied by a model by model mutation.

# Background

A *signature* Σ is a set of function and predicate symbols. Each symbol is associated with a nonnegative integer, called the *arity*. If *arity*(*g*)= 0, then *g* is a *constant symbol*. We assume that the binary equality predicate to be always present in any signature Σ. We use the standard notion of Σ*-structure* M, that is, a support set endowed with an arity-matching interpretation of the function and predicate symbols from Σ. We use *f* M (*p*M) to denote the interpretation of the function symbol *f* (predicate symbol *p*) in the structure

M. The truth of a Σ-formula in M is defined in the standard ways. A formula *φ* is satisfiable in M iff its *existential closure* is true in M. In this case, we say M is a *model* for *φ*. A *sentence* is a first-order formula with no free variables. A (first-order) *theory* T over a signature Σ is a set of (deductively closed) sentences over Σ. We say two theories T 1 and T 2 have disjoint signatures when Σ1 ∩ Σ2 = { }. A theory T is *stably inﬁnite* if every satisfiable quantifier free formula is satisfiable in an infinite model. A theory T is *convex* [[15](#_bookmark24)] iff for all finite sets Γ of literals and for all non-empty disjunctions *i*∈*I ui* *vi* of variables, Γ |=T *i*∈*I ui* *vi* iff Γ |=T *ui* *vi* for some *i* ∈ *I*. Intuitively, a theory is convex if for every satisfiable set of literals there is a model where variables not implied to be equal have a distinct interpretation. For example, linear integer arithmetic is not convex, because the set of literals {0 ≤ *x*1 ≤ 1*,* 0 ≤ *x*2 ≤ 1*,* 0 ≤ *x*3 ≤ 1} is satisfiable, no equality *xi* *xj* for *i* /= *j* is implied, but there is no model where *x*1, *x*2 and

*x*3 are all distinct.

* 1. *Nelson-Oppen combination method*

Nelson-Oppen (NO) combination method [[12](#_bookmark21)] provides a rather simple solu- tion for the theory combination problem for theories that are stably infinite and have disjoint theories. More formally, let 7 1 and 7 2 be consistent, stably infinite theories over disjoint (countable) signatures. Assuming satisfiability of conjunction of literals can be decided in 0(7 1(*n*)) and 0(7 2(*n*)) time re- spectively. Then,

1. The combined theory 7 is consistent and stably infinite.
2. Satisfiability of quantifier free conjunction of literals in 7 can be decided in 0(2*n*2 × (7 (*n*)+ 7 (*n*))).

1 2

1. If 7 1 and 7 2 are convex, then so is 7 and satisfiability in 7 is in 0(*n*4 ×

(7 1(*n*)+ 7 2(*n*))).

Let Γ be a set of literals over Σ1 ∪ Σ2. Then, the non-deterministic NO combination method can be described in the following way. First, a satis- fiability preserving transformation called *puriﬁcation* is used to transform Γ

into Γ1 Λ Γ2, such that, the symbols from Γ*i* are in Σ*a*, where Σ*a* = Σ*i* ∪ *a*,

*i* *i*

and *a* (= V(Γ1) ∩ V(Γ2)) denotes the set of shared variables between Γ1 and

Γ2. Then, a partition of *a* into disjoint subsets is guessed and is expressed as a conjunction of literals *φ*. For example, the partition {*x*1}*,* {*x*2*, x*3}*,* {*x*4} is represented as *x*1 / *x*2*, x*1 / *x*4*, x*2 / *x*4*, x*2 *x*3. Then, the individual procedures are used to decide whether Γ*i* Λ *φ* is satisfiable. The combined procedure returns unsatisfiable if one of the procedures returns unsatisfiable. For convex theories, instead of *guessing*, one can *deduce* the equalities to be shared. The key idea is to propagate *x* *y* to Γ2 whenever 7 1 ∪ Γ1 |= *x* *y*, and vice-versa. This process is repeated until no further equations can be propagated. Then, the individual procedures are used to decide whether Γ*i* is satisfiable. Sharing equalities in this case is sufficient, because a theory 7 1 can assume that *x*M2 /= *y*M2 whenever *x* *y* is not implied by 7 2 and vice versa. So, for convex theories, there is an efficient way to construct a partition

of the set of shared variables.

# Related Work

* 1. *Convex theories only*

For convex theories it is sufficient to propagate all implied equalities between shared variables. For instance, theories that admit canonizers solve equality

propagation by rewriting. In general, a theory 7 *i* is canonizing (as coined in [[18](#_bookmark26)]) if it admits a function ↓ , such that:

7 *i* ∪ Γ*i* |= *s* *t* iff *s* ↓Γ*i* = *t* ↓Γ*i .*

Linear rational arithmetic is convex, procedures based on the Fourier- Motzkin algorithm produce all implied equalities in a straight-forward way, but the procedure may require exponential space. For procedures based on the Simplex algorithm, all implied equalities can be deduced using the ap- proaches described in [[16](#_bookmark25),[7](#_bookmark16)].

The main disadvantage of these approaches is poor performance (either of the solver or of the equality propagation) and the inability to deal with non-convex theories.

* 1. *DTC: Delayed Theory Combination*

Several SMT solvers [[3](#_bookmark11)] use the underlying SAT solver to guess a partition of V(Γ1) ∩ V(Γ2), the idea is to create a literal *u* *v* for every pair of shared variables *u* and *v*. One may be concerned that guessing a partition would be exponentially more expensive than deriving it when the theories are convex. However, as shown in [[6](#_bookmark15)], back-jumping and lemma learning allow *simulating* the standard Nelson-Oppen combination method: equalities that are implied by a theory, once learned are not flipped.

The obvious disadvantage of this approach is that the number of additional equality literals is quadratic in the number of shared variables. There is an additional assumption that may be tool specific to MathSat, but are pervasive in the results from [[6](#_bookmark15)]: all literals used by the SAT solver must be present in the input to the SAT solver. At the current time of writing CVC3 [[2](#_bookmark12)], Verifun [[10](#_bookmark19)], Yices [[9](#_bookmark18)], and our tool Z3 all support dynamically added literals. Our approach, presented later, appeals to an SMT solver that allows in- troducing literals on the fly. If this is not possible, the approach boils down

to a branching heuristic on top of DTC.

* 1. *Ackermannization*

When combining two theories 7 1 and 7 2, where 7 1 is the theory of unin- terpreted functions, one can eliminate 7 1 by creating all ground instances of Leibniz’s rule [[1](#_bookmark10)]:

*ni* *mi* → *f* (*n*) *f* (*m*) (1)

Thus, we can eliminate a function symbol *f* from a set of formulas *F* by applying the procedure ackermannize:

ackermannize(*f, F* ):

foreach *f* (*n*) ∈ *F* where *n* do not contain *f*

create a fresh constant *af*(*n*)

replace *f* (*n*) by *af*(*n*) in *F*

foreach *af*(*n*)*, af*(*m*)

add the clause *ni* *mi* → *af*(*n*) *af*(*m*) to *F*

A partial Ackermann’s reduction heuristic is proposed and investigated in [[5](#_bookmark14)]. Functions are only eliminated when the number of distinct occurrences is smaller than the set of shared variables in the function arguments.

Ackermannization has the same disadvantage as DTC in that the number of additional literals is quadratic in the size of the input. It is furthermore problematic to use Ackermannization in the context of several theories and when combining SMT solvers with quantifier instantiation.

* + 1. *Dynamic Ackermannization*

Congruence closure algorithms for deduction in equational theories are ubiq- uitous. Efficient and incremental congruence closure based procedures are described in [[7](#_bookmark16),[13](#_bookmark22)]. However, these algorithms miss the following propagation rule:

*f* (*n*) / *f* (*m*) =⇒ *ni* / *mi .* (2)

This propagation rule (which is a contrapositive of ([1](#_bookmark1))) has a dramatic per- formance benefit in some benchmarks, and Ackermann’s reduction gives this rule for free. For example, the following simple formula takes 0(2*N* ) time to be solved using the algorithms presented in [[7](#_bookmark16),[13](#_bookmark22)]. In contrast the formula can be solved in polynomial time if either 0(*N*2) axioms are added up front by ackermannize or the above propagation rule is used resulting in “only” 0(*N*) space and time overhead.

*N*

(*pi* V *xi* *v*0) Λ (ч*pi* V *xi* *v*1) Λ (*pi* V *yi* *v*0) Λ (ч*pi* V *yi* *v*1)*,*

*i*=1

*f* (*xN ,... ,f* (*x*2*, x*1) *.. .*) / *f* (*yN,... ,f* (*y*2*, y*1) *. .*(*.*3))

This performance problem reflects a limitation in the current congruence clo- sure algorithms used in SMT solvers, and it is not related with the theory combination problem. In fact, the formula above uses only one theory. In [[9](#_bookmark18)], an approach, called *Dynamic Ackermannization*, is proposed to cope with this problem. There, clauses corresponding to Ackermann’s reduction are added when a congruence rule participates in a conflict.

# Model-based Theory Combination

Our approach minimizes the number of produced shared equalities. It is based on the fact that, in practice, the number of local inconsistencies is much bigger than the number of global (cross theory) inconsistencies. It works for convex and non-convex theories alike.

1. Each theory 7 *i* maintains a model M*i* for Γ*i*, or at times only for a subset of Γ*i*.
2. From time to time, if *u*M*i* = *v*M*i* , then the theory creates the case-split

*u* *v*, the positive case is tried first.

1. At the discresion of the theory solver, change a model M*i* to M' to

*i*

satisfy newly assigned literals, or to imply fewer equalities.

It is fairly straight-forward to integrate this approach in a DPLL(7 ) frame- work, that we rename DPLL(7 M), as the search is now model-guided. Bor- rowing notation from [[11](#_bookmark20),[14](#_bookmark23)], the relevant new rules are presented in Fig. [1](#_bookmark3). The full set of rules are repeated from [[14](#_bookmark23)] in Fig. [A.1](#_bookmark27). The transition rules modify triplets of the form M*,* Γ || *F* , where M is a set of models for theories 7 1*,... ,* 7 *n*, Γ is a set of asserted literals, and *F* is a set of clauses. The rule M-Propagate creates a fresh equality literal (*u* *v*)*d* when a model associated with one of the theories imply it, but the equality is not present in the context Γ. The equality literal is pushed on Γ, thus propagating the equality to all theories sharing variables *u* and *v*. The tag *d* on the literal indicates that the literal may be negated during backtracking. The M-Mutate rule allows changing models during backtracking search. For instance, after applying De- cide, a newly assigned literal *ld* may not be satisfied in the existing models. We do not need to specify when M-Mutate is applied. In particular, theory solvers are not required to maintain models for their contexts at all times during a search. Models are only required when other case splits have been attempted. For example, when using linear programming for an integer linear programming problem, a simplex tableau may choose to delay introducing Gomory cuts to obtain an integer interpretation until other constraints have been propagated.

We use the following optimizations to minimize even further the number of necessary case splits. Let *R*M be an equivalence relation on V such that *R*M(*u, v*) iff *u*M = *v*M. Let *classes*(*R*) be the set of equivalence classes induced by *R*.

1. Opportunistic equality propagation: Equalities that can be inferred with- out additional expense to the theory solver are always propagated eagerly. Section [5](#_bookmark4) gives an example of opportunistic equality propagation.

M-Propagate

M*,* Γ || *F* =⇒ M*,* Γ(*u* *v*)*d* || *F* if

M-Mutate

⎧ *u, v* ∈ V*,* (*u* *v*) /∈ L

*u*M*i* = *v*M*i*

⎪⎪⎨

⎪⎪⎩ add (*u* *v*) to L

M*,* Γ || *F* =⇒ M'*,* Γ || *F* if M' is some variant of M

Fig. 1. Model-based propagation

1. Postponing model-based equality propagation: we delay applying the rule M-Propagate until case splits on already existing literals have been performed.
2. Model mutators, the idea is to use a function *δ*(M*k*) that returns a more

*diverse* model. More formally, |*classes*(*R*M*k* )| ≤ |*classes*(*Rδ*(M*k* ))|

# Simplex: An example model-producing theory solver

Following [[8](#_bookmark17)], a theory solver for linear arithmetic, and integer linear arith- metic, can be based on a Simplex Tableau of the form:

*xi* Σ

*xj*∈N

*aijxj xi* ∈ B*,*

where B and N denote the set of basic and nonbasic variables, respectively. In addition to this tableau, the solver state stores upper and lower bounds *li* and *ui* for every variable *xi* and a mapping *β* that assigns a rational value *β*(*xi*) to every variable *xi*. The bounds on nonbasic variables are always satisfied by *β*, that is, the following invariant is maintained

∀*xj* ∈ N *, lj* ≤ *β*(*xj*) ≤ *uj.*

Bounds constraints for basic variables are not necessarily satisfied by *β*, so for instance, it may be the case that *li > β*(*xi*) for some basic variable *xi*, but pivoting steps can be used to fix bounds violations, or detect an infeasible tableau. We hope it does not come as a total surprise that the current model for the simplex solver is given by *β*. Enumerating the equalities implied by *β* is simple: enumerate all the values of *β*(*xi*), inserting each value into a hash table. The expected time of enumerating all equalities is then 0(|B ∪ N |).

* 1. *Opportunistic equality propagation*

In a Simplex tableau, some equalities can be inferred using the following inex- pensive rules. We say that a variable *xi* is *ﬁxed* iff *li* = *ui*, a linear polynomial *xj* ∈V *aijxj* is fixed iff for every *xj* ∈ V, *xj* is fixed or *aij* = 0. Given a linear

Σ

Σ Σ

polynomial *P* = *xj* ∈V *aijxj*, we use *β*(*P* ) to denote *xj* ∈V *aijβ*(*xj*).

FixedEq

*li* ≤ *xi* ≤ *ui, lj* ≤ *xj* ≤ *uj* =⇒ *xi* *xj* if *li* = *ui* = *lj* = *uj*

EqRow

*xi* *xj* + *P* =⇒ *xi* *xj* if *P* is fixed, and *β*(*P* )= 0

EqOffsetRows

*xi* *xk* + *P*1 *xj* *xk* + *P*2

EqRows

*xi* *P* + *P*1 *xj* *P* + *P*2

=⇒ *xi*

=⇒ *xi*

*xj*

*xj*

if ,⎨ *P*1 and *P*2 are fixed,

, and *β*(*P*1)= *β*(*P*2)

if ,⎨ *P*1 and *P*2 are fixed,

, and *β*(*P*1)= *β*(*P*2)

The first rule can be implemented using a mapping from values to fixed variables, the second rule can be easily checked when a row is updated during a pivoting step. The rule EqOffsetRows is a simpler and less expensive version of EqRows. It can be implemented using a mapping (*xk, v*) '→ *xi*, where *xk* and *xi* are variables, and *v* is a value. In our implementation, the first three rules are eagerly applied, and the last one is only applied before M-Propagate. We also aggressively remove fixed variables from the basis.

These rules can miss some implied equalities. For instance, from the con- straints ([4](#_bookmark5)), the rules detect the implied equality *z* *w*, but miss the equality *x* *y*, because *z* is not a fixed variable. Fortunately, the bound propagation technique described in [[8](#_bookmark17)] can be used imply the bound 0 ≤ *w*, making *w* a fixed variable, and enabling the application of the rule EqRow.

*x* *y* + *w* + *s, z* *w* + *s,* 0 ≤ *z, w* ≤ 0*,* 0 ≤ *s* ≤ 0 (4)

* 1. *Mutation using* freedom intervals

The *freedom* of a non-basic variable *xj* is defined as the interval [*Lj, Uj*], where:

*L* = max „j*β*(*x* )+ *li* − *β*(*xi*) | *a*

*j*

*j*

*a*

*ij*

*>* 0ﬀ ∪ j*β*(*x* )+ *ui* − *β*(*xi*) | *a*

*ij*

*<* 0ﬀ ∪ {*l* }«

*U* = min „j*β*(*x* )+ *ui* − *β*(*xi*) | *a*

*ij*

*j*

*a*

*ij*

*j*

*j*

*j*

*a*

*ij*

*j*

*a*

*ij*

*j*

*ij*

*>* 0ﬀ ∪ j*β*(*x* )+ *li* − *β*(*xi*) | *a*

*ij*

*<* 0ﬀ ∪ {*u* }«

Intuitively, if *β* satisfies all rows and bound constraints, then *β* will also satisfy them after executing update(*xj, v*) for any value *v* in the interval [*Lj, Uj*], where the update procedure is defined as:

update(*xj, v*)

foreach *xi* ∈ B*, β*(*xi*) := *β*(*xi*)+ *aij*(*v* − *β*(*xj*)) *β*(*xj*) := *v*

Freedom intervals can be used to produce a more diverse *β* without performing any pivoting operation. A simple *greedy* heuristic seems to be quite effective: for each non-basic variable *xj*, execute update(*xj, v*), if there is a value *v* ∈

'

[*Lj, Uj*] such that |*classes*(*Rβ*)| *<* |*classes*(*Rβ*' )|, where *β*

update operation.

# Experimental Evaluation

denotes *β* after the

The experiments were conducted using a 32bit Pentium 4 processor running at 3.6Ghz, 2Gb of memory, and 2Mb of cache. The timeout was set to 10 minutes. We compared our approach against other SMT solvers and against different strategies within our solver Z3. We used the same benchmarks used in [[5](#_bookmark14)]. The benchmarks were translated to the SMT-LIB format, and are available for download in our website [3](#_bookmark7) . We also included, for *N* ∈ [1*,* 99] the examples from ([3](#_bookmark2)) and the following simple family of satisfiable formulas in the comparison for *N* ∈ [2*,* 99]:

*N*

*ϕ* = *f* (*xi*) ≥ 0 Λ *xi* ≥ 0 Λ *xi* / *xi*+1 (5)

*i*=1

All benchmarks but the Ackermann suite use the theories of uninterpreted functions and linear arithmetic. Tables [1](#_bookmark8) and [2](#_bookmark9) summarize the results ob- tained in our experiments. Each cell has the accumulated time, in seconds, used by each solver to solve a family of benchmarks. It does not include the time spent in instances where the solver produced the *unknown* result. A solver is considered to have produced the *unknown* result when it times out

3 [http://research.microsoft.com/∼leonardo/SMT07](http://research.microsoft.com/~leonardo/SMT07)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | # | MathSAT | MathSAT-dtc | Yices | Z3 |
| EufLaArithmetic | 52 | 1851.50 (11) | 785.87 (1) | 10.45 | 17.34 |
| Hash | 199 | 520.90 | 19.39 | 11.48 | 6.54 |
| Wisa | 256 | 886.36 (1) | 6916.18 | 4.37 | 2.78 |
| RandomCoupled | 400 | 517.05 | 518.15 | 9516.11 (51) | 56.16 |
| RandomDecoupled | 500 | 11989.60 (1) | 97.07 | 19362.40 (51) | 41.95 |
| Simple ([5](#_bookmark6)) | 98 | 1366.33 | 7053.98 (29) | 2328.63 (53) | 1.00 |
| Ackermann ([3](#_bookmark2)) | 99 | 228.49 (82) | 344.00 (82) | 2.99 | 1.72 |
| Total | 1604 | 17360.23 (95) | 15734.64 (112) | 31236.43 (155) | 127.49 |

Table 1 Experimental results

or crashes. The number of *unknown* results is displayed using parenthesis. MathSAT-dtc denotes the MathSAT solver with the command line option -DTC that forces it to use Delayed Theory Combination. We used Yices version 1.0.8 in the experiments. Yices is also based on DTC, but the shared equalities are lazily generated, and it uses a filtering mechanism to avoid the generation of unnecessary shared equalities [[9](#_bookmark18)]. Yices and Z3 implement Dynamic Ackerm- annization suggested in [[9](#_bookmark18)]. Six different versions of our Z3 solver were used: Z3-dtc uses delayed theory combination and the additional equalities between shared variables are eagerly generated; Z3-dtc\* is similar to Z3-dtc but uses the current model to implement a branching heuristic for the generated equalities; Z3-ack uses Ackermann’s reduction as a pre-processing step; Z3-neq, Z3-ndack and Z3 all use Model Based Theory Combination, but Z3-neq does not use opportunistic equality propagation, and Z3-ndack does not use Dynamic Ack- ermannization. Notice that our implementation of Z3-dtc does not include several optimizations that may be useful for a DTC framework. It does not take advantage of theory propagation for arithmetic.

The benchmarks in the EufLaArithmetic family are trivial if the linear arith- metic solver performs some form of opportunistic equality propagation. The Simple family described above was used to demonstrate that DTC is not ro- bust. Yices performs poorly on most satisfiable instances in the RandomCou- pled and RandomDecoupled families.

Model based theory combination seems to be more robust than DTC or Ackermann’s reduction. In these benchmarks, the average number of shared equalities propagated by Z3 using M-Propagate was 2*.*46. The maximum was 57.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Z3-dtc | Z3-dtc\* | Z3-ack | Z3-neq | Z3-ndack | Z3 |
| EufLaArithmetic | 796.71 (11) | 2830.38 (4) | 1094.47 (1) | 786.15 | 11.56 | 17.34 |
| Hash | 310.10 | 305.75 | 23.68 | 5.89 | 6.02 | 6.54 |
| Wisa | 364.71 | 385.06 | 12.31 | 4.89 | 2.40 | 2.78 |
| RandomCoupled | 8122.45 (166) | 12451.82 (103) | 101.24 | 56.45 | 56.65 | 56.16 |
| RandomDecoupled | 12421.30 (85) | 15316.60 (71) | 56.54 | 51.23 | 48.39 | 41.95 |
| Simple ([5](#_bookmark6)) | 7.26 | 7.34 | 33.89 | 0.45 | 1.00 | 1.00 |
| Ackermann ([3](#_bookmark2)) | 728.22 (77) | 733.58 (77) | 37.99 | 1.74 | 874.21 (77) | 1.72 |
| Total | 22750.75 (339) | 32030.53 (255) | 1360.12 (1) | 906.78 | 1000.23 (77) | 127.49 |

Table 2 Experimental results (only Z3)

# Conclusions

This paper introduced a new approach for dealing with equality propagation in the context of convex theories where equality deduction is expensive and more generally, in the context of non-convex theories. Both in theory, and as we validated experimentally, the approach solves a number of practical deficiencies with other known solutions to integrating theories.

Model-based Theory Combination requires that a decidable theory main- tains a notion of a model that supports efficiently answering queries of the form *u*M = *v*M.

* 1. *On the signiﬁcance of Ackermann’s reduction*

The Wisa benchmark set is used in [[5](#_bookmark14)] to illustrate the usefulness of Acker- mann’s reduction in contrast with DTC. With Model-based Theory Combi- nation, Ackermann’s reduction does not help on these set of benchmarks. We therefore believe they reflect more the problems with DTC than the advan- tages of Ackermann’s reduction. On the other hand, the synthetic Ackermann benchmarks, one can observe the utility of the reduction. Dynamic Acker- mann reduction is not without an overhead: new literals are added to the search space, and the new literals cause T-Propagate to spend additional over- head of walking use-lists. Future work includes investigating whether it is a practical advantage to build in the propagation directly into a congruence closure algorithm.

* 1. *Are theories amenable to Model-based combinations?*

Our main example of a model producing theory solver was a classical Sim- plex solver. We are experimenting with adding model-based solvers to other theories, and we hope to be reporting on our findings in future work.

# Acknowledgment

The authors would like to thank Alberto Griggio for providing the latest ver- sion of MathSAT and adding a command line option for enabling Delayed Theory Combination.

# References

1. Ackermann, W., *Solvable cases of the decision problem*, Studies in Logic and the Foundation of Mathematics (1954).
2. Barrett, C. and C. Tinelli, *CVC3*, in: W. Damm and H. Hermanns, editors, *CAV’07, Berlin, Germany*, LNCS 4590 (2007).
3. Bozzano, M., R. Bruttomesso, A. Cimatti, T. A. Junttila, S. Ranise, P. van Rossum and

R. Sebastiani, *Efficient theory combination via boolean search.*, Inf. Comput. 204 (2006),

pp. 1493–1525.

1. Bozzano, M., R. Bruttomesso, A. Cimatti, T. A. Junttila, P. van Rossum, S. Schulz and

R. Sebastiani, *The MathSAT 3 System*, in: R. Nieuwenhuis, editor, *CADE*, LNCS 3632 (2005),

pp. 315–321.

1. Bruttomesso, R., A. Cimatti, A. Franz´en, A. Griggio, A. Santuari and R. Sebastiani, *To* *Ackermann-ize or Not to Ackermann-ize? On Efficiently Handling Uninterpreted Function Symbols in UF(*E*)*, in: *LPAR*, 2006, pp. 557–571.
2. Bruttomesso, R., A. Cimatti, A. Franz´en, A. Griggio and R. Sebastiani, *Delayed Theory Combination vs. Nelson-Oppen for Satisﬁability Modulo Theories: A Comparative Analysis.*, in: *LPAR*, 2006, pp. 527–541.
3. Detlefs, D., G. Nelson and J. B. Saxe, *Simplify: a theorem prover for program checking*, J. ACM 52 (2005), pp. 365–473.
4. Dutertre, B. and L. de Moura, *A Fast Linear-Arithmetic Solver for DPLL(T)*, in: *CAV’06*, LNCS 4144 (2006), pp. 81–94.
5. Dutertre, B. and L. de Moura, *The Yices SMT Solver*, <http://yices.csl.sri.com/tool-paper.pdf> (2006).
6. Flanagan, C., R. Joshi and J. B. Saxe, *An explicating theorem prover for quantiﬁed formulas*, Technical Report HPL-2004-199, HP Laboratories, Palo Alto (2004).
7. Ganzinger, H., G. Hagen, R. Nieuwenhuis, A. Oliveras and C. Tinelli, *DPLL(T): Fast decision procedures.*, in: *CAV’04*, LNCS 3144, 2004, pp. 175–188.
8. Nelson, G. and D. C. Oppen, *Simpliﬁcation by cooperating decision procedures*, ACM Transactions on Programming Languages and Systems 1 (1979), pp. 245–257.
9. Nieuwenhuis, R. and A. Oliveras, *Fast Congruence Closure and Extensions*, Inf. Comput. 2005

(2007), pp. 557–580.

1. Nieuwenhuis, R., A. Oliveras and C. Tinelli, *Solving SAT and SAT Modulo Theories: From* *an abstract Davis–Putnam–Logemann–Loveland procedure to DPLL(T).*, J. ACM 53 (2006),

pp. 937–977.

1. Oppen, D. C., *Complexity, convexity and combinations of theories.*, Theor. Comput. Sci. 12

(1980), pp. 291–302.

1. Rueß, H. and N. Shankar, *Solving linear arithmetic constraints*, Technical Report SRI-CSL-04- 01, SRI International (2004).
2. Sheini, H. M. and K. A. Sakallah, *SMT(LU): a step toward scalability in system veriﬁcation.*, in: S. Hassoun, editor, *ICCAD* (2006), pp. 844–851.
3. Shostak, R. E., *Deciding combinations of theories.*, J. ACM 31 (1984), pp. 1–12.

# A A presentation of DPLL(7 M)

Fig. [A.1](#_bookmark27) repeats from [[14](#_bookmark23)] the presentation of DPLL(7 ) as an abstract transi- tion system. We have added M to each sequent to emphasize that the current state during proof-search also carries a model. In contrast to [[14](#_bookmark23)], we use a set L of literals to choose case split candidates from. We assume L is a super-set of the literals occurring in the set of clauses *F* . Besides the fresh equality liter- als introduced by the rule M-Propagate, non-convex theory implementations, such as an integer linear solver may introduce fresh literals as a side-effect of performing branch-and bound search.

UnitPropagate

(

M*,* Γ || *I, C* ∨ *l* =⇒ M*,* Γ*l* || *I, C* ∨ *l* if Γ |= ¬*C*

*l* is undefined in Γ

Decide

(

M*,* Γ || *I* =⇒ M*,* Γ*ld* || *I* if *l* occurs in L

*l* is undefined in Γ

Fail

(

M*,* Γ || *I, C* =⇒ *fail* if Γ |= ¬*C*

Γ contains no decision variables

Γ*ld*Γ' |= ¬*C,*

8>

|  |  |  |  |
| --- | --- | --- | --- |
| Backjump |  | | |
| M*,* Γ*ld*Γ' || *I,* | *C* =⇒ | M*,* Γ*l*' || *I, C* | if |
| T-Propagate |  |  |  |
| M*,* Γ || *I*  Learn | =⇒ | M*,* Γ*l* || *I* | if |
| M*,* Γ || *I* =⇒ | | M*,* Γ || *I, C* | if |
| Forget  M*,* Γ || *I, C* =⇒ | | M*,* Γ || *I, C* | if |
| Restart  M*,* Γ || *I* =⇒ | | M*,* ∅ || *I* |  |

there is a clause *C*' ∨ *l*' such that

><

*I, C* |= *C*' ∨ *l*' and Γ |= ¬*C*';

>>:

8><

*l*' is undefined in Γ;

*l*' or ¬*l*' occurs in *I* or in *ld*Γ'

Γ |=T *l*

*l* occurs in L

>: *l* is undefined in Γ

all atoms of *C* occur in L

(

*I* |=T *C*

n *I* |=T *C*

Fig. A.1. DPLL with exhaustive theory propagation