

Variability Modeling in Clafer Using SMT

Ed Zulkoski

University of Waterloo, Waterloo, Ontario, Canada
ezulkosk@gsd.uwaterloo.ca
(ezulkosk, 20456819)

Abstract

We present a new backend for Clafer - a variability modeling language - using the Z3 Satisfiability Modulo Theory (SMT) solver. Z3 is well respected for its speed and has been shown to outperform other solvers in the domain of partial modeling – one type of modeling within the scope of Clafer. We show that, by retaining the notion of a *scope*, Clafer can generally be expressed within the logic of **QF_UFNRA** (quantifier-free non-linear real arithmetic), however all Clafer models encountered so far can be expressed in **QF_LIA** (quantifier-free linear integer arithmetic). We are capable of supporting language features not previously available in Clafer, including constraints over real numbers, and string constraints, leveraging Z3-Str: a theory extension to Z3. We conclude with a discussion of other extensions we have made, as well as new directions for future work that would not be possible with other Clafer backends.

Contents

1	Introduction	2
2	Clafer Overview	3
3	Solution Overview	3
3.1	Interpreting Z3 output as a Clafer Model	4
4	Detailed Solution Overview	5
4.1	Hierarchical and Cardinality Constraints	5
4.2	Set Constraints	5
4.3	Quantifiers	5
4.4	Discussion	6
4.5	Bracketed Constraints	6
5	Extensions to Clafer	6
5.1	String Constraints	6
5.2	Isomorphic Model Prevention	7
6	Experimental Results	8
7	Related and Previous Work	8
8	Future Work	9
9	Conclusions	9
		1

1 Introduction

Clafer is a modeling language with first-class support for feature and meta-modeling [1]. In earlier work, Clafer has been translated to two backend solvers 1) Alloy – a bounded relational model checker, and 2) Choco – a library for constraint satisfaction problems. A Clafer specification can be translated to either of these two backends, which produce models of the specification if it is satisfiable, or produce an unsatisfiable core otherwise. Depending on the type of constraints within the Clafer specification, one backend may be more suitable than the other. For example, Alloy does not perform well on arithmetic constraints over large integers, as it deals with them by flattening bounded integer ranges into boolean formulas, however the Choco solver is much more capable in this regard. Still, Choco requires some bounding on integer ranges to facilitate the search process.

Furthermore, some desirable language features, such as constraints over real numbers and strings, are not currently supported by either backend due to restrictions of the solvers. Many domains require real numbers to be modeled naturally. For example, any models involving probabilities or percentages can be modeled using reals. One applicable domain that has previously been modeled in Clafer is that of banking. The work investigated the family of available Scotiabank mortgage options, which include interest rates and monetary amounts, both of which can be naturally modeled with reals¹. However, due to restrictions of previous backends, the specification could not be instantiated. Clafer should be capable of analyzing these models.

In short, the restrictions of Clafer are intrinsically tied to the limitations of its backend solver. In order to address some of these restrictions, we have developed a new translation from Clafer to Z3 [7] – a state-of-the-art SMT solver. Z3 is well known to be a fast solver, motivating our desire to create a new Clafer backend with it. In an experiment by [10], randomly generated partial models were analyzed by four solvers: Alloy, a relational logic solver; Minizinc, a *constraint satisfaction problems* (CSP) solver; Clasp with GrinGo, an *answer set programming* (ASP) solver; and Z3. Z3 was shown to be more efficient (based on solving time) in general, and also scaled better to harder problems. Z3 has also been shown to perform well relative to other SMT solvers, winning the SMTCOMP 2012 competition in the theory categories of QF_UFLIA, QF_UFLRA, and QF_BV, among others². Further, a recent extension to Z3: Z3-Str [11], allows support for some string constraints (*e.g.* length, substring).

This paper makes the following contributions:

1. We describe how Clafer models can be reduced to constraints in logics supported by Z3.
2. We have developed a tool called *ClaferZ3* that reflects the translation described in this work, and can be found at <https://github.com/gsdlab/ClaferZ3>.
3. Our tool supports constraints over real numbers and strings, which are not supported by previous Clafer backends, and thus expands the scope of models that Clafer can analyze. Furthermore, integer instances are unbounded.
4. We discuss further extensions to Clafer that are possible with an SMT backend. For example, we have prototyped a new approach for eliminating isomorphic models (Section 5.2).

¹See <http://gsd.uwaterloo.ca/node/356>.

²Results can be found at <http://www.smtexec.org/exec/?jobs=1004>.

2 Clafer Overview

Clafer is a structural modeling language which is designed for variability modeling. It unifies both feature models and meta-models [1]. Clafer specifications are built of components called clafers.

In Listing 1 we show a specification of two mobile phones in Clafer. **Phone** is an example of a top-level (non-nested) abstract clafer. **Abstract clafers** do not get directly instantiated in the resulting model, however concrete clafers, such as **BudgetPhone** and **SmartPhone**, can extend abstract clafers to inherit their sub-clafers. **Sub-clafers** are indicated by indentation, and cannot exist without their parent. Although our example only has two levels of indentation, other specifications may have more. The * after **Phone** indicates that zero or more **Phones** may be included in the resulting model. **Phone** has an optional feature **Wifi**, denoted by the question mark after it. **instApps** is a **reference clafer** (denoted by the -> symbol) that refers to a set of installed **Apps**. We emphasize that this is a set: an implicit constraint is that the same phone cannot have two of the same **App**. However, *different* phones may install the same **App**. A **Phone**, has a final attribute of **cost**, which we indicate is of type real number. Note that clafers that are declared primitive (int/string/real) get *desugared* into reference clafers that point to instances of their respective type. On line 6, **App** is an example of a **concrete clafer**.

On line 9, we introduce the concrete clafer **BudgetPhone**, which inherits all subclafers from **Phone**. The number 2 after it indicates that there must be exactly two **BudgetPhones** in the resulting model. **BudgetPhone** has two constraints associated with it on lines 10-11 (indicated by square brackets). Line 10 consists of a quantified formula (with quantifier *no*), indicating that a **BudgetPhone** cannot have **Apps**. Note that this constraint must be true of *all* **BudgetPhone** instances, due to its level of indentation. Line 11 indicates the price of **BudgetPhones**, constraining the inherited clafer **cost**. Line 14 restricts the cost of **SmartPhones** to be its original cost, plus the sum of all installed **Apps**. The dot character in “instApps.appCost” in essence serves as a navigation operator, by performing a join between the set of **Apps** associated with this individual **SmartPhone** and the **appCosts** associated with them. A model of the specification is given in Listing 2.

This example only illustrates a fragment of the expressions supported by Clafer. Most notably, set operations such as intersection and union allow richer expressions over instances of clafers. We describe the other components of the language in Section 4

3 Solution Overview

We describe the approach of our translation through our example in Section 2. For consistency (and due to large amounts of overlapping terminology), we define the following terms and notations: 1) we use capitalized *Clafer* to denote the language Clafer itself, and lowercase *clafer* to denote individual components of the input (*e.g.* **Phone** in Listing 1); 2) we call the Clafer input the *specification* (*e.g.* Listing 1); 3) an output that conforms to the specification is a *model* (*e.g.* Listing 2); and 4) individual occurrences of a clafer in the model are *instances* (*e.g.* *Phone0* in Listing 2).

Figure 3 depicts how our translation of Clafer to Z3 fits into the Clafer toolchain. Clafer specifications are first run through the front-end (scanner, parser, type-checker, etc.), and a representation of the input is generated in Python. Using the Z3Py API, ClaferZ3 generates a set of variables and asserts constraints over them. If string constraints are not present, then we can use the standard Z3 implementation to check for satisfiability, else we use Z3-Str. If the solver finds a satisfying assignment over the generated variables and constraints, then the

Listing 1: Clafer specification of two types of phones and apps.

```

1 abstract Phone *
2   Wifi ?
3   instApps -> App *
4   cost : real
5
6 App *
7   appCost : real
8
9 BudgetPhone: Phone 2
10  [ no instApps && no Wifi ]
11  [ cost = 49.99 ]
12
13 SmartPhone: Phone 1
14  [ cost = 99.99 + sum(instApps.appCost)]

```

Listing 2: A generated model of a mobile phone and its apps in Clafer.

```

App0
  appCost = 0.99
App1
  appCost = 2.99
BudgetPhone0 : Phone0
  Wifi0
  cost = 49.99
BudgetPhone1 : Phone1
  cost = 49.99
SmartPhone0 : Phone2
  Wifi1
  instApps0 -> App0
  instApps1 -> App1
  cost = 103.97

```

Listing 3: The variables associated with each clafer in Z3 corresponding to Listing 2.

```

Phone: [0, 0, 0]
Wifi: [0, 2, 3]
instApps: [2, 2, 3]
instApps.ref: [0, 1, 3]
cost: [0, 1, 2]
cost.ref: [49.99, 49.99, 103.97]
App: [0, 0, 1]
appCost.ref: [0.99, 2.99, 0]
BudgetPhone: [0, 0]
SmartPhone: [0]

```

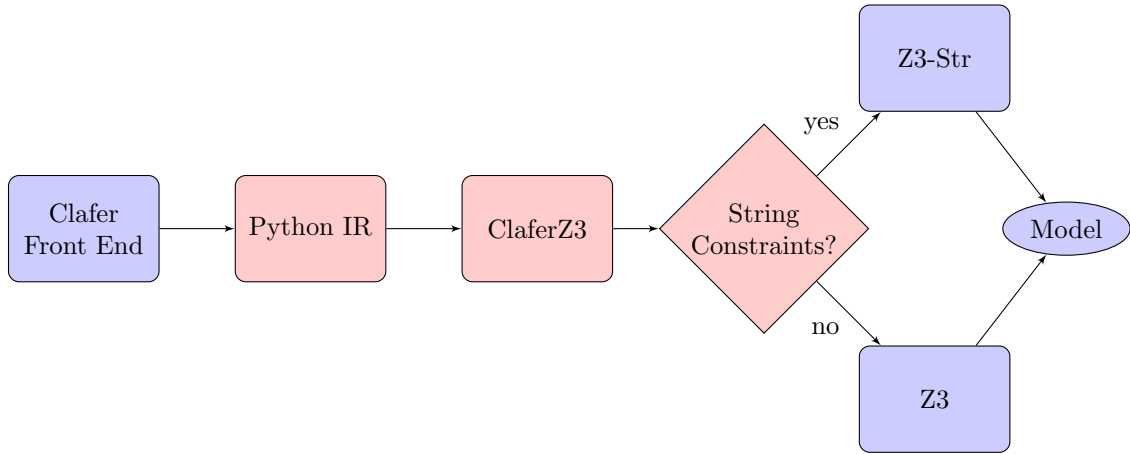


Figure 1: Depicts ClaferZ3 within the Clafer toolchain. Nodes marked red indicate contributions of this work.

values of these variables can be interpreted as a Clafer model.

We devote the remainder of this section to describing the variables generated to express our Clafer specification in Z3, and how their valuations are interpreted back into a Z3 model. The actual constraints over the variables are discussed in Section 4. We hope that by discussing the end result first, the constraint that need to be generated are more intuitive.

3.1 Interpreting Z3 output as a Clafer Model

We borrow two key ideas from a previous translation of Clafer to Choco [5]: 1) clafers are represented as a finite number of integers; and 2) clafers that extend abstract clafers have a direct mapping to their supers (we discuss this point later).

We represent a clafer as a finite list of integers. Consider the **BudgetPhone** clafer in Listing

1. Since a model will have at most two **BudgetPhone** clafer, we can represent it with a list of two integer variables, say $[BudgetPhone_0, BudgetPhone_1]$.

For star-cardinalities (as in the reference clafer **App**), we place a finite *scope* s on the clafer, indicating that only s instances can occur in the model. For the sake of example, let us assume that the scope of all unbounded clafers is 3. Then we can represent the clafer **App** with the list $[App_0, App_1, App_2]$.

Listing 3 depicts a possible Z3 output for our model. Note that, for example, “Wifi: [0,2,3]” is shorthand for $Wifi_0 = 0, Wifi_1 = 2, Wifi_2 = 3$. Semantically, the values of these integer variables represent *parent pointers*, indicating where the clafer should be placed in the model. For example, if the variable App_0 is set to 0 by the solver, then it should fall directly beneath $Phone_0$ in the hierarchy of the model. Likewise, if $App_0 = 1$, then App_0 would be placed under $Phone_1$.

A clafer instance is *excluded* from the model if its integer variable is set to a pre-defined *sentinel* value, which equals the total number of instance variables of the clafer’s parent. For example, since the **cost** clafer is directly underneath **Phone**, and **Phone** has three instances variables, any **cost** instance set to 3 will not be included in the model. For *top-level clafers* that do not have a parent, the instance is included if its corresponding variable is set to 0, and not included if set to 1. For simplicity in the remainder of the paper, given a clafer x , an instance x_i is excluded if $x_i = x_{off}$ ($Wifi_2 = Wifi_{off}$ in our example).

Reference clafers (e.g. **instApps**) require an additional variable associated with each instance, which corresponds to where the reference points. For a reference clafer instance x_i , we label its reference $x_i.ref$. In Listing 3, since $instApps_0.ref = 0$, $instApps_0$ points to App_0 . The *sentinel* value for a reference variable is equal to the number of instances of the referenced clafer (e.g. $instApps_{off} = App_{off}$).

Integer and real number clafers (e.g. **cost**) are treated similarly to reference clafers, however their references have unbounded ranges. Also, if an integer clafer is not present in the model, we set its reference to 0 to facilitate other set operations, such as summation.

4 Detailed Solution Overview

This section describes the Z3 constraints that are generated to represent a Clafer specification in Z3. We begin with our representation of a clafer in Section ???. The remaining sections constrain this representation to conform to all restrictions of the specification (e.g. cardinality constraints, bracketed constraints, etc.).

4.1 Hierarchical and Cardinality Constraints

asdf A reference exists *iff* its corresponding clafer exists (e.g. $Apps_0 \neq Apps_{sentinel} \Leftrightarrow Apps_0.ref \neq SwApps_{sentinel}$).

4.2 Set Constraints

a[4] asdf

4.3 Quantifiers

Quantified expressions.

4.4 Discussion

Due to space restrictions, we do not discuss the full set of expressions available in Clafer. Most expressions follow patterns analogous to those previously presented. We also did not discuss arithmetic constraints, however they translate naturally into Z3.

Although we have not formally proven it, we believe our approach is sound, in that it will only produce models that satisfy the specification. However, our approach is incomplete for multiple reasons. Most notably, since we bound our specifications, we may miss larger models. Further, Clafer technically allows non-linear arithmetic, although we have not seen any specifications so far that require it. With that in mind, our approach of translating bounded Clafer specifications can generally be expressed within the logic of **QF_UFNRA** (quantifier-free non-linear real arithmetic), however all Clafer models encountered so far can be expressed in **QF_LIA** (quantifier-free linear integer arithmetic).

4.5 Bracketed Constraints

We must also support Clafer’s bracketed constraints (as in $[sum\ Apps.ref.memory \leq 100]$ from Listing 1), which we only discuss at a very high-level. To generate this constraint, we must first compute each of the joins in $Apps.ref.memory$. which is intuitively the set of **memory** clafers that are beneath any **SwApp** referenced by an **Apps** instance. We must then ensure that the sum of this set of **memory** instances is less than 100. Note that this is indeed the case in our example, since $memory0 + memory1 = 41 \leq 100$.

Although this example is not too difficult to convert to Z3 constraints, more complicated expressions and language features make set constraints challenging. Consider the specification in Listing ???. Both **iPhoneApps** and **AndroidApps** reference **SwApps**, however when considering the summation on the last line, we must only consider instances of **SwApps** referenced by instances of **AndroidApps**. As another example, two previously unmentioned Clafer keywords are **this** and **parent**, which essentially allows one to consider each instance of a claffer individually. For example, the constraint: $[this.ref.memory = 15]$ in Listing ??? essentially states that the **memory** field of any **SwApp** referenced by an **iPhoneApp** must be equal to 15. This requires us to generate constraints corresponding to *all* individual instances of **iPhoneApp**.

5 Extensions to Clafer

A notable difference of using Z3, as opposed to previous backends of Clafer, is its ability to handle constraints on real numbers³. Z3 handles real numbers naturally, so incorporating constraints over them into our translation required minimal effort. We therefore do not discuss further details.

We next briefly describe our extensions allowing string constraints. We also propose a new algorithm to prevent the generation of models that are isomorphic to previously generated models.

5.1 String Constraints

String constraints are supported through Z3-Str [11], an extension to Z3 allowing the string expressions, such as concatenation, substring, and cardinality. If the given specification contains

³Due to complications with the Clafer frontend grammar, we have only been able to prototype these constraints with small hand-generated models. This also applies to string constraints. These restrictions will be addressed in the near future.

Listing 4: A specification with 6 isomorphic models. Below are two example models.

```
AddsToSix 1
  Digit -> int 3
  [this.ref > 0]
  [sum(Digit.ref) = 6]

//example model
AddsToSix0
  Digit0 = 1
  Digit1 = 2
  Digit2 = 3

//isomorphic to first model
AddsToSix0
  Digit0 = 2
  Digit1 = 1
  Digit2 = 3
```

Listing 5: The Clafer constraint restricting all models isomorphic to Listing 4.

```
[ //note the negation here
  !( #AddsToSix = 1 &&
    (some Digit0 ; Digit1 ; Digit2 : Digit |
      (some c0_AddsToSix_sort_0 : AddsToSix |
        #c0_AddsToSix_sort_0.Digit = 3 &&

          Digit0 in AddsToSix0.Digit &&
          Digit1 in AddsToSix0.Digit &&
          Digit2 in AddsToSix0.Digit &&

          "Digit uniqueness constraints" &&

          Digit0.ref = 1 &&
          Digit1.ref = 2 &&
          Digit2.ref = 3
        ))) ]
```

string constraints, we translate to Z3-Str instead of Z3.

Since we are using the Z3 Python API (which does not support strings), we need to modify our translation to conform to the Z3-Str input format. Our approach is to first purify any strings and string operations present in the AST of the specification. String variables are temporarily replaced with fresh Int variables, and string expressions are replaced with either fresh Int or fresh Boolean variables, depending on the operation (e.g. cardinality is replaced with an Int, whereas substring is replaced with a Boolean). After all other components of the translation finish, the constraints constructed during translation are converted into Z3-Str format, reintroducing strings and string expressions where necessary.

5.2 Isomorphic Model Prevention

Clafer can produce many models for a given specification, however many models may have the same structure, that is, they are *isomorphic*. While we do not formally define isomorphism of models, intuitively two models are isomorphic if they have the same number of instances of each clafer, the same tree structure, and the graph formed by reference clafers is isomorphic. From a user's viewpoint, these *redundant* models are not as useful, and should be excluded if possible. Consider Listing 4. Essentially, this specification requires three unique positive integers, such that their sum is six. There are six unique models (one for each permutation of the numbers 1, 2, and 3), however they are all isomorphic to each other.

Suppose the first example model from Listing 4 has been generated. Listing 5 is the constraint (in Clafer syntax) that is added to the specification to prevent future models isomorphic to the first. Essentially, each future model either have a different number of clafers (which is not possible due to cardinality constraints), or must have a digit not equal 1, 2, or 3. Note that by using the *some* quantifier, the order of the *Digits* is ignored.

Although we have only shown a simple example with integers, the approach extends naturally to larger models and reference clafers. This improves upon previous approaches that only

Specification	Translation Time(s)	Solving Time(s)
Clafer Test Suite	10.55	0.88
Audi Configurator	0.13	0.01
PHP Script	N/A	N/A
Zoo	0.84	0.15

Figure 2: Translation and solving time for each experiment. Note that the Clafer test suite consists of 41 individual specifications. Times are in seconds.

look at the tree structure of the model, and cannot detect isomorphism over reference clafers. We note that this approach is possible as Z3 allows pushing new constraints after a solution has been found. Unfortunately, our approach may add an exponential number of constraints, making it infeasible for many specifications. We are still investigating optimizations for this approach.

6 Experimental Results

We provide initial experimental results from four sources: 1) the Audi Car Configurator model from [6]; 2) a simple Clafer specification of a zoo from [5]; 3) a PHP script involving string and integer constraints from [11]; and 4) the Clafer test suite. The Clafer test suite contains mostly small specifications, however it was useful for checking the proper functionality of our tool. The test suite contains 43 specifications, and we evaluated all but two. The two excluded specifications did not adhere to small design restrictions of our approach, which are reserved for future work⁴.

Currently, we do not have any larger models in our evaluation, and we plan to address this limitation of our results in the future. However, our evaluation does demonstrate that our tool can properly analyze specifications from a variety of domains, even outside of what would typically be considered variability models (e.g. the PHP script).

All tests were run on a dual core (2.4GHz) laptop with 8GB of RAM, running 64-bit Linux Mint 14. We used Z3 4.3.2 along with Python 3.2 in our experiments. We specified a global scope of 6 for each test, with the exception of the zoo specification, which requires a scope of 9.

Table 6 shows the translation and solving time for our set of specifications. Translation time indicates the time required to convert a Clafer specification to a set of Z3 constraints. Solving time indicates how long Z3 takes to find the first satisfying model for each specification. Although the translation is currently a large bottleneck for our approach, it can certainly be optimized. We find that the low solving times for all specifications indicates that our approach is promising.

7 Related and Previous Work

The work of Michel et. al. [6] discusses how configuration problems can be encoded in SMT using TVL [2] – a text based feature modeling language similar to Clafer. TVL supports many of the components of feature modeling, including hierarchy, group cardinality, attributes, enums, and cross-tree constraints. However, several aspects of Clafer require extensions to this work.

⁴Essentially, these specifications require instances of abstract clafers to be part of the concrete model.

Most notably, set constraints and quantified expressions.

A previous project [9] within the GSD lab was capable of translating a small subset of Clafer to Z3, in order to support attributed feature models for multi-objective optimization. The primary components of Clafer necessary for this domain include hierarchical constraints, fixed-size cardinalities (e.g. $[0..1]$), and basic arithmetic constraints. This project subsumes that translation by allowing arbitrary Clafer constraints.

This work most closely resembles that of [5]. Their work translates Clafer to Choco, a CSP language. We have borrowed components from that work, particularly in our representation of clafer and inherited clafer. We are able to extend Clafer with constraints over strings and real numbers, which neither the Choco nor Alloy backend currently support. Z3 also allows us to handle arbitrarily larger integers, which neither of the other backends support. In addition, in the future we intend to extend this project in order to eliminate the need for scopes on unbounded clafer. We discuss this in Section 8.

8 Future Work

This project utilized only a small subset of the available features of Z3. For example, Z3 has support for uninterpreted functions and data types. We would like to modify our translation to take advantage of these features. With this approach, we may be able to eliminate the need for scopes in our implementation. The work in [3], which translates components of Alloy to SMT, and that of [8], which discusses some set theoretic operations using the theory of arrays, may be useful starting points for this extension.

One particular reason we did not take this approach yet is due to translation efficiency. As an example, in an early version of this project we used an uninterpreted function to represent cardinality constraints. Given a clafer, the function would restrict its instances to conform to the cardinality constraints. By blasting this function into simple arithmetic constraints (which we can do since we have a bounded number of instances), our translation times were significantly decreased⁵, even for small models. We emphasize that here we are referring to *translation time*; Z3 took approximately the same time to solve models whether or not functions were used.

A proper evaluation is necessary to compare the three Clafer backends that are now available. Since each backend was developed independently and contain unique optimizations, this comparison cannot properly evaluate the effectiveness of Alloy/Choco/Z3 as a backend. However, it would be useful to users of Clafer who wish to choose the ideal backend for their application.

Finally, we intend to further evaluate our extensions for string and real number constraints. Although we currently have models with these constraints, they cannot be properly compiled by Clafer, due to lack of support in the Clafer frontend (see footnote 3). These issues will be addressed in the near future.

9 Conclusions

We have developed a translation from Clafer to Z3. We extend capabilities of Clafer with string constraints using Z3-Str, as well as constraints over real numbers and unbounded integers. Z3's capability to push new constraints to existing specifications allows a new approach to isomorphism detection of Clafer models. Initial results indicate that our approach seems reasonably

⁵Although time differences were not recorded, some relatively small specifications required 2-3 additional seconds.

fast over a variety of specifications, however larger inputs will be needed to validate our results. With the expressive power of Clafer, coupled with the support for new data types, our approach supports the analysis of new domains of models that previous tools are incapable of handling.

References

- [1] K. Bk, K. Czarnecki, and A. Wsowski. Feature and meta-models in Clafer: mixed, specialized, and coupled. *Software Language Engineering*, 2011.
- [2] A. Classen, Q. Boucher, and P. Heymans. A text-based approach to feature modelling: Syntax and semantics of TVL. *Science of Computer Programming*, 76(12):1130–1143, Dec. 2011.
- [3] A. E. Ghazi and M. Taghdiri. Relational reasoning via SMT solving. *FM 2011: Formal Methods*, 2011.
- [4] D. Jackson. *Software Abstractions: Logic, Language, and Analysis*. The MIT Press, 2011.
- [5] J. Liang. Solving Clafer Models with Choco. Technical report.
- [6] R. Michel, A. Hubaux, V. Ganesh, and P. Heymans. An SMT-based Approach to Automated Configuration. *SMT Workshop 2012 10th ...*, pages 107–117, 2012.
- [7] L. D. Moura and N. Bjørner. Z3: An efficient SMT solver. *Tools and Algorithms for the Construction and ...*, 2008.
- [8] L. D. Moura and N. Bjørner. Generalized, efficient array decision procedures. *Formal Methods in Computer-Aided ...*, pages 1–10, 2009.
- [9] R. Olacchia. *Comparison of Exact and Approximate Multi-Objective Optimization for Software Product Lines*. PhD thesis, 2013.
- [10] P. Saadatpanah, M. Famelis, J. Gorzny, N. Robinson, M. Chechik, and R. Salay. Comparing the effectiveness of reasoning formalisms for partial models. *Proceedings of the Workshop on Model-Driven Engineering, Verification and Validation - MoDeVVA '12*, 1(c):41–46, 2012.
- [11] Y. Zheng, X. Zhang, and V. Ganesh. Z3-str: a z3-based string solver for web application analysis. *Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering - ESEC/FSE 2013*, page 114, 2013.