Contextualized Abstraction for Assertion-Level Theorem Proving

Quoc Bao Vo
FR Informatik, Universität des Saarlandes, 66041 Saarbrücken, Germany
email: bao@ags.uni-sb.de

1 Introduction

In this paper we propose a context-based approach to abstract theorem proving. The challenges stem from the need to identify an abstract level for theorem proving where (less important) information can be temporarily ignored so that a (plan for a) proof of the abstracted problem can be devised to guide the (re)construction of the object-level proof. Contextualization is realized by preserving the logical structures of the formulas of the original representation while pushing the less important subformulas, according to a relevance relation, into the hierarchical subcontexts. This representation allows the problem to be gradually unfolded during the proof search process by hierarchically exploring the subcontexts required to provide support for the hypotheses used in the proof plan.

The underlying inference machinery is also equipped with an assertion application module which allows mathematical assertions such as axioms, definitions, theorems, and even global and local assumptions to be applied directly to a proof situation to obtain their logical consequences (from the applied proof situation) and fill in the gaps opened up by an abstract-level proof step. This guarantees that our achievement is two-fold: on the one hand, we are able to carry out effective techniques to search for and construct proofs for a problem; on the other hand, the constructed proof is readily at a sufficiently high level of abstraction so that it can be communicated directly to human mathematicians without undergoing a proof transformation process as required by most machine-generated proofs.

2 Context-based abstraction

While assertion-level reasoning empowers theorem proving systems with the capability of making conclusions directly from mathematical assertions (see [6]), it can not offer much in terms of mathematical discoveries and proving creativity. Assertion-level reasoning shares with traditional theorem proving the same representation, *viz.* logical formulas, to formulate mathematical theories and problems. On the other hand, many solutions to mathematical problems rely on just one or two key steps which might help unfold the whole problem and a proof of the theorem could then subsequently be found by routine application of standard inference steps. It is this capability of discovering such key steps that is still missing from our assertion-level reasoning mechanism. We also believe that different representations, generally at different levels of abstraction, are required to achieve such capability.

In the rest of this paper, following Gentzen [5], we formulate the problems of theorem proving as sequents $\Gamma \vdash F$ where $\Gamma \cup \{F\}$ is a finite set of wffs. Sequents formulating problems are called **problem theories** in this paper. To simplify the presentation, we further assume that all quantifiers are removed by skolemization, leaving the formulas with only free variables.

Definition 1 Let a problem theory Σ be given, a *context* for Σ is a tuple $\langle$variables, constants, functions, relations, assertions$\rangle$, where:

- variables is the set of free variables occurring in Σ;
- constants is the set of constants occurring in Σ. These include all skolem terms which are possibly parameterized on the variables from variables;
- functions and relations are the sets of functions and relations, respectively, occurring in Σ;
- assertions is the set of (local) assertions which, at least, contains the definitions of all domain-specific functions and relations occurring in Σ.

Definition 2 Let a problem theory Σ be given, a *contextualized problem* of Σ is a triple **Context** : **Body** $\triangleright$ **Head**, where:

- **Context** is a context for Σ;
- **Head** is a formula to be proved by the prover; and
- **Body** consists of two parts:
  (a) **Supports** is a (possibly empty) list of *support lines*. Each support line σ consists of: (i) a formula, called the *support formula* of σ and denoted as $supp(\sigma)$; and (ii) a (possibly empty) list of contextualized (sub)problems, called the *conditions* of σ.
  (b) **Conditions** is a (possibly empty) list of formulas which need to be proved for the problem to be completely solved.

Let π be a contextualized problem for the problem theory $\Gamma \vdash F$, we will use the accessor "." to obtain the appropriate fields in π, e.g. π.**Context**.variables is the set of variables defined in the context of π. A contextualized problem π is *well-defined* if (i) all symbols occurring in $\{\pi.\textbf{Head}\} \cup \{supp(\sigma) : \sigma \in \pi.\textbf{Body}\}$ are declared in its context, and (ii) **Head** is a subformula of F. In this paper, we consider only well-defined contextualized problems and will refer to them simply as contextualized problems unless explicitly stated otherwise.

Example 1 In this example we consider the challenge problem for automated theorem provers (as proposed by Bledsoe [4]) in elementary analysis to prove that "limit of sum is sum of limits". Following Bledsoe, we will refer to this problem as LIM+. The problem theory for LIM+ can be represented by the following sequent:

$$\vdash \lim_{x \to a} f(x) = L_1 \wedge \lim_{x \to a} g(x) = L_2 \Rightarrow \lim_{x \to a} (f(x) + g(x)) = L_1 + L_2$$

Since the formal definition of the limit of a function F at a cluster point a (see e.g. [2]) is:

$$\lim_{x \to a} F(x) = L \Leftrightarrow$$
$$\forall_\epsilon . 0 < \epsilon \Rightarrow (\exists_\delta . 0 < \delta \wedge (\forall_x . x \neq a \wedge |x - a| < \delta \Rightarrow |F(x) - L| < \epsilon)))$$

we can accordingly expand the above sequent, with the definition of $\lim_{x \to a}$, and perform skolemization and normalization, yielding the expanded problem theory.

$$\begin{array}{l} \vdash 0 < \epsilon_1 \Rightarrow 0 < sko_{\delta_1}(\epsilon_1) \wedge (x_1 \neq a \wedge |x_1 - a| < sko_{\delta_1}(\epsilon_1) \Rightarrow |f(x) - L_1| < \epsilon_1) \wedge \\ \quad 0 < \epsilon_2 \Rightarrow 0 < sko_{\delta_2}(\epsilon_2) \wedge (x_2 \neq a \wedge |x_2 - a| < sko_{\delta_2}(\epsilon_2) \Rightarrow |g(x) - L_2| < \epsilon_2) \\ \quad \Rightarrow (0 < sko_\epsilon \Rightarrow (0 < \delta \wedge (sko_x(\delta) \neq a \wedge |sko_x(\delta) - a| < \delta \Rightarrow \\ \qquad\qquad |(f(sko_x(\delta)) + g(sko_x(\delta))) - (L_1 + L_2)| < sko_\epsilon))) \end{array}$$

This problem theory can now be reformulated in the proposed context-based language as depicted in Figure 1, where SP^i_j's are the

Problem: LIM+		
Context	variables: $\delta : \mathbb{R}$; $\epsilon_1 : \mathbb{R}$; $\epsilon_1 : \mathbb{R}$; ...	
	constants: $sko_\epsilon : \mathbb{R}$; $sko_x(\delta) : \mathbb{R}$; $a, L, L_1, L_2 : \mathbb{R}$; ...	
	functions: $\|.\| : \mathbb{R} \to \mathbb{R}$; $f, g : \mathbb{R} \to \mathbb{R}$; ...	
	relations: $<, \leq : \mathbb{R} \times \mathbb{R}$; ...	
	assertions: Triangle theorem; Definitions of $\|.\|, +, -, 0$; ...	
Head	$\|(f(x) + g(x)) - (L_1 + L_2)| < sko_\epsilon$	
Body	**Supports**	$\sigma_1 : ((0 < sko_\epsilon); [\,])$
		$\sigma_2 : ((sko_x(\delta) \neq a); [\,])$
		$\sigma_3 : ((\|sko_x(\delta) - a| < \delta); [SP^3_1])$
		$\sigma_4 : ((\|f(x_1) - L_1| < \epsilon_1); [SP^4_1, SP^4_2, SP^4_3])$
		$\sigma_5 : ((\|g(x_2) - L_2| < \epsilon_2); [SP^5_1, SP^5_2, SP^5_3])$
	Conditions	

Figure 1. The contextualized problem LIM+.

contextualized subproblems providing the local conditions for the respective supports they belong to. For instance:

$$SP^3_1 = [\,] : [\,] \rhd (0 < \delta)$$

i.e. its context and body are empty[1] and its head is the formula $0 < \delta$. Note that this is the local condition of the support line σ_3. That is, the proof obligation for this subproblem is not necessarily discharged if a proof for the main problem, i.e. LIM+, does not use the support formula $(|sko_x(\delta) - a| < \delta)$. This is particularly useful in e.g. proof by case analysis in which a (conditional) assumption is only needed in one of the cases but not the others. More complex are the cases of the support lines σ_4 and σ_5 which are essentially have the same structure. For instance, when $(|f(x_1) - L_1| < \delta_1)$ is invoked in a proof of $(|(f(x) + g(x)) - (L_1 + L_2)| < sko_\epsilon)$ then the subproof obligations $\boxed{0 < \epsilon_1}$; $\boxed{|x - a| < sko_{\delta_1}(\epsilon_1)}$ (under the support $0 < sko_{\delta_1}(\epsilon_1)$); and $\boxed{x \neq a}$ are required to be discharged. These correspond to the subproblems SP^4_1, SP^4_2, and SP^4_3, respectively.

3 The main algorithm

In the connection method (see [3, 1]), first-order formulas are represented as two-dimensional objects (i.e. matrices). This representation enables powerful proof methods and procedures. By taking the relevance relation between formulas into account, we can add the third dimension to the above representation. By pushing the given problem theory along this dimension, we are able to contextualize our problem, e.g. as illustrated in Figure 1 for the problem theory presented in Example 1.

The idea behind algorithm CONTEXTUALIZATION, whose details are described in the full version of this paper, is to identify the role of a subformula occurring in the problem theory in relation to the formulas in focus. To that end, we first reformulate the problem theory $\{A_1, \ldots, A_n\} \vdash F$ into the goal formula $\gamma \equiv A_1 \wedge \ldots \wedge A_n \Rightarrow F$. Every subformula of γ is then assigned a polarity which is either $+$ or $-$ as follows:[2]

- γ is assigned the polarity $+$;
- If a formula $F \equiv \neg G$ is assigned the polarity π then G is assigned the negation of π;
- If a formula $F \equiv G \vee H$, or $F \equiv G \wedge H$, is assigned the polarity π then so are G and H.

Now, provided the polarity of a formula ϕ and the connective linking its immediate subformulas we can identify the role of a subformula of ϕ to the other, e.g. if $\phi \equiv \phi_1 \to \phi_2$ and is assigned the polarity $-$ then ϕ_1 provides the condition for ϕ_2 (equivalently, $\neg\phi_2$ provides the condition for $\neg\phi_1$), or if $\phi \equiv \phi_1 \wedge \phi_2$ and is assigned the polarity $+$ then ϕ_1 and ϕ_2 are independent of each other and can be considered separately (e.g. as different supports for a goal formula), etc.

4 Discussion

Our approach for context-based abstraction aims at reformulating the problem to (hopefully) provide the connection to the key steps required to unfold and solve the original problem. However, the contextualization process still critically depends on the relevance relation, *viz.* Rel, and the focus of the problem, *viz.* F, around which the problem is contextualized.

Relevance has long been recognized as one of the more important research areas of AI. For instance, a special issue devoted to the topic of Relevance was published by *AI Journal* in 1997. As has been mentioned earlier in this paper, one way to define a relevance relation for contextualization is to consider only atomic formulas sharing at least one problem-specific (vs. domain-specific and general) symbol as being relevant.

Finding the right part of the problem to place the focus on and center all activities for solving the problem around the focus also plays an essential part in the process of tackling mathematical problems. For instance, a standard representation for the proof of the problem in Example 1 was presented by Bartle and Sherbert [2], called the "ϵ-δ game". Using this representation, the focus formula of the problem can be identified immediately.

REFERENCES

[1] Peter B. Andrews, 'Theorem proving via general matings', *Journal of the ACM*, **28**(2), 193–214, (1981).

[2] Robert G. Bartle and Donald R. Sherbert, *Introduction to Real Analysis (Second Edition)*, John Wiley & Sons, Inc, 1982.

[3] Wolfgang Bibel, *Automate Theorem Proving*, Friedr. Vieweg, 1983.

[4] Woodrow W. Bledsoe, 'Challenge problems in elementary calculus', *Journal of Automated Reasoning*, **6 (1)**, 341–359, (1990).

[5] G. Gentzen, 'Untersuchungen über das logische schliessen', *Mathematische Zeitschrift*, **39**(176–210), 405–431, (1935).

[6] Quoc Bao Vo, Christoph Benzmüller, and Serge Autexier, 'Assertion application in theorem proving and proof planning', in *IJCAI-03*, pp. 1343–1344. IJCAI/Morgan Kaufmann, (2003).

[1] Observe that SP^3_1 inherits the super-context for problem LIM+ in which the variable δ and the constants $<$ and 0 are declared.

[2] The negation of $+$ is $-$ and the negation of $-$ is $+$.