Haskell-style Overloading is NP-hard

Dennis M. Volpano †
Department of Computer Science
Naval Postgraduate School
Monterey, California, 93943
volpano@cs.nps.navy.mil

Abstract

Extensions of the ML type system, based on constrained type schemes, have been proposed for languages with overloading. Type inference in these systems requires solving the following satisfiability problem. Given a set of type assumptions $C$ over finite types and a type basis $A$, is there is a substitution $S$ that satisfies $C$ in that $A \vdash C$ is derivable? Under arbitrary overloading, the problem is undecidable.

Haskell limits overloading to a form similar to that proposed by Käes called parametric overloading. We formally characterize parametric overloading in terms of a regular tree language and prove that although decidable, satisfiability is NP-hard when overloading is parametric.

1 Introduction

A practical limitation of the ML type system is that it prohibits global overloading in a programming language by restricting to at most one the number of assumptions per identifier in a type context, a limitation noted by Milner himself [Mil78]. Suppose we wish to assert that a free identifier, say $+$, has precisely finite types $\text{int} \to \text{int} \to \text{int}$ and $\text{real} \to \text{real} \to \text{real}$. Any context in which $+$ has one of the two desired finite types precludes a derivation that it has the other. On the other hand, any context that assigns type scheme $\forall a. a \to a \to a$ to $+$ is one from which too many types can be derived for $+$. There is no type context in system ML from which we can derive all and only the desired finite types for $+$. Even system ML with subtypes is inadequate. From type context

$$A = \{ \text{int} \subseteq \text{real}, \ + : \text{real} \to \text{real} \to \text{real} \}$$

one could derive $A \vdash + : \text{int} \to \text{int} \to \text{real}$ but not $A \vdash + : \text{int} \to \text{int} \to \text{int}$.

Several type disciplines have emerged for programming languages with overloading. Among them are those based on intersection types [CoD78, Sal78, CDV80] and those based on constrained type schemes, the latter being inspired by the design of Haskell [WaB89, CDO91, Smi91, Kae92, CHO92, Jon92]. The type system of Forsythe, an explicitly-typed descendant of Algol, is based on an intersection type discipline, namely $\lambda_\alpha$ [Rey88]. Though useful, $\lambda_\alpha$ remains limited in that it has no type schemes and all intersections are finite [Lie90, Pie91].

A more flexible type discipline for languages with overloading is an extension of the ML type system with constrained type schemes [Kae92, Smi93]. Using the notation of [Smi93], a constrained type scheme has the general form

$$\forall a_1, \ldots, a_n \text{ with } x_1 : \tau_1, \ldots, x_m : \tau_m . \tau$$

where $\tau$ is a finite type. Finite types are defined in the usual way. Every type variable $a$ is a finite type, and if $\tau_1, \ldots, \tau_n$ are finite types then so are $\tau_1 \to \tau_2$ and $\chi(\tau_1, \ldots, \tau_n)$ where $\chi$ is a type constructor of arity $n$. The $x_1 : \tau_1, \ldots, x_m : \tau_m$ are constraints on overloaded free identifiers $x_1, \ldots, x_m$. Quantifier $\forall$ is omitted if there are no quantified variables and the with clause is omitted if there are no constraints, in which case we have an ordinary ML type scheme. Unlike the ML type system, a free identifier may be overloaded, that is, have multiple assumptions in an initial type context, so we refer to this extension as system $ML_c$.

The fact that a free identifier is permitted to have more than one assumption in a type context immediately raises the issue of semantic ambiguity in terms. Care must be taken to ensure that terms with overloaded identifiers have unambiguous meaning. Consider, for instance, type context

$$\left\{ + : \text{real} \to \text{real} \to \text{real}, \quad + : \forall a. \text{set}(a) \to \text{set}(a) \to \text{set}(a) \right\}$$

(1)
**Title:** Haskell-style Overloading is NP-hard

**Abstract:**

Haskell-style overloading is a feature in the Haskell programming language that allows a function to have multiple definitions, each with a different list of type signatures. This paper investigates the computational complexity of deciding whether a given set of type signatures can be overloaded in Haskell.

**Keywords:** Haskell, Overloading, NP-hard.
where + denotes real addition and set union. If one can derive from this context that term \( \lambda x. x + x \) has type \( \text{real} \rightarrow \text{real} \) and \( \forall \beta. \text{set}(\beta) \rightarrow \text{set}(\beta) \) then the term can be interpreted in one of two different ways. Its meaning then must be determined by a process called overloading resolution whose outcome depends on the type of \( x \). Thus we say that the overloading of + above is incoherent. Surprisingly, incoherent overloading is pervasive among languages despite its potential for semantic ambiguity. For example, "\( f \)" is often overloaded, as in Ada, to stand for integer and floating-point division.

Coherent overloading, on the other hand, gives rise to discrete polymorphism where the meaning of a term does not depend on overloading resolution. In this setting, a semantics for an operator, say \( f \), is postulated as a set of sentences, or axioms, \( \Delta \) say in first-order logic. A model of \( \Delta \) is any interpretation that satisfies it. So if for a type basis \( A \), one is able to derive \( A \vdash f : \sigma_1 \) and \( A \vdash f : \sigma_2 \), then the overloading of \( f \) within \( A \) is coherent if \( \sigma_1 \) and \( \sigma_2 \) are each models of \( \Delta \). If so, then we may regard \( f \) as belonging to the intersection of \( \sigma_1 \) and \( \sigma_2 \). Coherent overloading then allows the meaning of every term to be uniquely determined by simply appealing to the axioms for the operators in question which, after all, is where semantics should be prescribed.

For instance, suppose \( \Delta = \{ \forall x. x+x = x \} \). Both an interpretation of + as set union and logical disjunction satisfy \( \Delta \), so sets and truth values are models of \( \Delta \). But \( \Delta \) is false under a real number interpretation. So we would regard the sentence in \( \Delta \) as an axiom of set theory and boolean algebra, but not the first-order theory of reals with addition. The overloading of + then in set (1) is incoherent if we adopt the sentence as an axiom of our intended meaning of +. However if the first assumption for + in (1) is replaced by + : \( \text{bool} \rightarrow \text{bool} \rightarrow \text{bool} \) then the overloading is coherent. So although we may be able to derive from (1) that \( \lambda x. x+x \) has type \( \text{bool} \rightarrow \text{bool} \) and \( \forall \beta. \text{set}(\beta) \rightarrow \text{set}(\beta) \), we know the function belongs to the intersection of the two types and its meaning, given uniquely by \( \Delta \), is a function that behaves as the identity function.

### 1.1 Satisfiability

Two new type assignment rules, (\( \forall \)-intro) and (\( \forall \)-elim) given in Figure 1, accompany constrained types. For a constraint set \( C \), the notation \( A \vdash C \) means that for each constraint \( x: \tau \) in \( C \), \( A \vdash x : \tau \) is derivable. The notation \( [\overline{\alpha} := \overline{\tau}] \) denotes a substitution, the application of which is written in postfix form. Observe that when \( C \) is empty the two rules reduce respectively to type generalization and instantiation in system ML [Mil78, DaMS82].

The antecedent of (\( \forall \)-intro) requires \( C \) be satisfiable with respect to \( A \). That is, for some finite types \( \overline{\tau} \), \( A \vdash C[\overline{\alpha} := \overline{\tau}] \) must be derivable. Operators that are constrained in \( C \) and interact share a type variable which in essence hypothesizes a model common to their semantics. Satisfiability of \( C \) then ensures the existence of such a model assuming overloading is coherent. If a model exists (there may be more than one), then the meaning of \( M \) is uniquely determined by the axioms of the operators, otherwise \( M \) has no meaning and consequently should be and is untypable. For example, suppose

\[
\begin{align*}
&\{ x + : \text{bool} \rightarrow \text{bool} \rightarrow \text{bool}, \\
&\quad \forall a. \text{set}(a) \rightarrow \text{set}(a) \rightarrow \text{set}(a) \}
\end{align*}
\]

is a coherent overloading with respect to semantics \( \Delta_1 = \{ \forall x. x+x = x \} \) and suppose

\[
\begin{align*}
&\{ x \leq : \text{int} \rightarrow \text{int} \rightarrow \text{bool}, \\
&\quad \forall a. \text{set}(a) \rightarrow \text{set}(a) \rightarrow \text{bool} \}
\end{align*}
\]

is a coherent overloading relative to an axiomatization, say \( \Delta_2 \), of a partial order. We can derive from (2) \( 1 \sqcup (3) \) that \( \lambda x. x+x \leq x \) has type \( \forall a. \text{set}(a) \rightarrow \text{bool} \) since \( \Delta_1 \) and \( \Delta_2 \) have sets as a common model. So the meaning of the term is given by \( \Delta_1 \) and \( \Delta_2 \) and is a constant function mapping sets into \text{true}. If there were no common model then the axioms could not be applied and the term would be meaningless.

So rules (\( \forall \)-intro) and (\( \forall \)-elim) give rise to the following satisfiability problem.

**Definition 1.1** The problem of constraint-set satisfiability CS-SAT is deciding for a given set of type assumptions \( C \), involving only finite types (constraints), and an assumption set \( A \), whether there is a substitution \( S \) such that \( A \vdash CS \) is derivable.

Without any restrictions on the kind of overloading in \( A \), CS-SAT is undecidable [Sm91]. Constrained type schemes permit recursive overloading where an
+ : real → real → real
+ : ∀α with + : α → α → α.
  matrix(α) → matrix(α) → matrix(α)
∗ : int → int → int
∗ : real → real → real
∗ : ∀α with + : α → α → α, ∗ : α → α → α.
  matrix(α) → matrix(α) → matrix(α)

Figure 2: A recursive overloading

assumption for an overloaded identifier has a constraint whose satisfiability may depend on the assumption itself. This permits type assumptions to be very expressive. For example, + and ∗ are overloaded recursively in Figure 2 due to constraints on + and ∗. Eliminating recursion altogether makes CS-SAT decidable but this is unacceptable because it arises naturally in practice as Figure 2 shows. Smith gives a restriction called overloading by constructors that allows CS-SAT to be solved in polynomial time [Smi91]. But it prohibits the kind of recursion given in Figure 2. The functional language Haskell adopts another restriction similar to that proposed by Käes called parametric overloading [Kae88].

2 Parametric Overloading

Assumption sets that arise in practice often follow a very simple pattern of overloading called parametric overloading [Kae88]. This form of overloading allows natural recursive overloading and makes CS-SAT decidable. To define it, we introduce the notion of the least common generalization (LCG) of a set of finite types which captures common structure among type assumptions for overloaded identifiers [Rey70, McC84].

Definition 2.1 A finite type τ is a common generalization of finite types τ₁, . . . , τₙ if there are n substitutions $S₁, . . . , Sₙ$ such that $τS_i = τ_i$ for all i; τ is the least common generalization of these types if in addition there is a substitution $S$ such that $τS = τ$ for any other generalization $τ'$. It is useful to extend this definition to identifiers. If identifier x is overloaded with constrained type schemes $∀j_1 with C_1 ∗ τ_1, . . . , ∀j_n with C_n ∗ τ_n$, such that τ₁, . . . , τₙ has τ as LCG with free variables $\bar{a}$, then $∀\bar{a}, τ$ is the LCG of x.

For example, if + is overloaded with assumptions $+ : int → real → real$ and $+ : real → complex → complex$ then its LCG is $∀α, β. α → β → β$.

$f, g : χ₁$
$f : ∀α with g : α. χ₂(α)$
$g : ∀α with f : α. χ(α)$

Figure 3: A mutually-recursive overloading

Definition 2.2 Parametric assumption sets are defined inductively.
The empty set is parametric.
If A is parametric with no assumption for x and σ is a constrained type scheme ∀α with C : τ such that for each $z : ρ ∈ C$, z is overloaded in A and ρ is a generic instance of its LCG then $A \cup \{x : σ\}$ is parametric.
If A is parametric with no assumption for x and B is the set

$$\begin{align*}
  &\{ x : ∀j_1 with C_1. τ[a := χ(\bar{a})] \\
  &\vdots \\
  &\{ x : ∀j_n with C_n. τ[a := χ(\bar{a})] \\
\end{align*}$$

such that

• $x$ has $LCG \forall a. τ$,
• $χ_i \neq χ_j$ for $i \neq j$, and
• $z : ρ ∈ C_i$ implies that z has $LCG \forall τ. ρ$, for some $τ ∈ \bar{a}$, and either z is overloaded in A or $z = x$,

then $A \cup B$ is parametric.

Examples of parametric assumption sets are given below and in Figure 2.

$$\begin{align*}
  &= : int → int → bool \\
  &= : ∀α, β with = : α → α → bool. \\
  &\quad pair(α, β) → pair(α, β) → bool \\
  &= : ∀a, ref(α) → ref(α) → bool
\end{align*}$$

The last assumption above specifies a polymorphic instance for $=,$ reflecting that equality is meaningful for references (pointers).

Parametric assumption sets allow a limited form of recursion. If we define a dependency relation among identifiers in a type assumption set that says identifier f depends on g if and only if f has an assumption with a constraint on g, then we see that parametricity ensures that the transitive closure of the relation is antisymmetric and consequently mutual recursion is prohibited. For instance, the set in Figure 3 is mutually recursive and therefore is not parametric. Neither the assumptions for f nor g can be introduced because each requires the introduction of the other.
2.1 Regular Tree Languages

Problem CS-SAT has two inputs, $A$ and $C$. In practice $A$ usually varies little if at all across different instances of type inference. Thus we can benefit from suitably representing $A$ and reusing its representation for different inputs $C$. A realistic measure of CS-SAT’s complexity should not ignore this fact. So although $A$ is an assumption set, we assume that as an instance of CS-SAT, it is suitably represented. If $A$ is parametric then every overloaded identifier $x$ has an LCG of the form $\forall \alpha. \tau$ and the set of finite types $\tau$ to which $\alpha$ can be instantiated, meaning one can derive $A \vdash x : \tau[\alpha := \pi]$, form a regular tree language.

Given an alphabet $A$, an $A$-valued tree $t$ is specified by its set of nodes, or domain, $\text{dom}(t)$, and a valuation of the nodes in $A$. Formally, a $k$-ary, $A$-valued tree is a mapping $t : \text{dom}(t) \rightarrow A$ where $\text{dom}(t) \subseteq \{0, \ldots, k-1\}^*$ is a nonempty set and closed under prefixes. The frontier of $t$ is the set of nodes $\{w \in \text{dom}(t) \mid \exists \delta w \in \text{dom}(t)\}$. We assume that $A$ is partitioned into a ranked alphabet $\Sigma$, and a frontier alphabet $X$. For any $\Sigma$ and $X$, we denote the set of all finite $\Sigma X$-trees by $F_{\Sigma}(X)$.

Regular tree languages, or forests, can be characterized in different ways using tree recognizers (automata) [GeS84] or familiar operations of regular sets, like concatenation and closure, extended to finite sets of trees [Tho90]. To simplify our proofs, we choose to characterize them as forests generated by a class of context-free grammars called the regular tree grammars [GeS84].

Definition 2.3 A regular $\Sigma X$-grammar $G$ consists of

- a finite nonempty set $N$ of nonterminal symbols,
- a finite set $P$ of productions $A \rightarrow r$ where $A \in N$ and $r \in F_{\Sigma}(N \cup X)$, and
- an initial symbol $S \in N$.

Definition 2.4 If $G = (N, \Sigma, X, P, S)$ is a regular $\Sigma X$-grammar then the $\Sigma X$-forest generated by $G$ is $T(G) = \{t \in F_{\Sigma}(X) \mid S \Rightarrow^*_t t\}$.

From a given parametric assumption set $A$, the idea is to construct for each overloaded identifier $x$ a regular tree grammar $G_x$ such that if $x$ has LCG $\forall \alpha. \tau$ then for any closed (variable-free) finite type $\tau$, $A \vdash x : \tau[\alpha := \pi]$ is derivable if and only if $\pi \in T(G_x)$. So determining whether constraint $x : \tau[\alpha := \pi]$ is satisfiable with respect to $A$ amounts to parsing $\pi$. $G_x$ always has a nonempty ranked alphabet of type constructors $\chi_1, \ldots, \chi_n$ and an empty frontier alphabet.

So we drop the frontier alphabet from discussion and speak of just $\Sigma$-trees from now on, the collection of which is $F_{\Sigma}$ for a given $\Sigma$.

Critical to our representation of a parametric overloading is the property that regular forests are effectively closed under intersection. This implies they are properly contained within the context-free languages since the latter are not closed under intersection.

Theorem 2.1 If $G_1$ and $G_2$ are regular tree grammars then $T(G_1) \cap T(G_2)$ is generated by a regular tree grammar.

Proof. Suppose $G_1 = (N_1, \Sigma, P_1, S_1)$ and $G_2 = (N_2, \Sigma, P_2, S_2)$ are regular $\Sigma$-grammars. Let $\Sigma$-grammar $G = (N_1 \times N_2, \Sigma, P, [S_1, S_2])$ where

$[A, B] \rightarrow a([Y_1, Z_1], \ldots, [Y_n, Z_n]) \in P$, for $n \geq 0$

if and only if $A = a(Y_1, \ldots, Y_n) \in P_1$, $B = a(Z_1, \ldots, Z_n) \in P_2$, and $a \in \Sigma$. Then $T(G) = T(G_1) \cap T(G_2)$.

Suppose $x$ is overloaded in an initial parametric assumption set $A$ with $LCG \forall \alpha. \tau$ and that $\Sigma$ contains all type constructors of $A$. We construct $G_x$ as follows. Since the overloading for $x$ may be recursive, we first factor all assumptions on $x$ into two sets, one containing its assumptions without any constraints on $x$ and the other having its assumptions with only constraints on $x$ if any. $G_x$ then is the intersection of the regular $\Sigma$-grammars representing the two sets. These two tree grammars cannot depend on $G_x$ since the transitive closure of the dependency relation is antisymmetric.

A regular $\Sigma$-grammar is constructed for each set as follows. For each assumption

$x : \forall \gamma_1, \ldots, \gamma_n$ with $C. \tau[\alpha := \chi(\gamma_1, \ldots, \gamma_n)]$

introduce $n$ nonterminals $A_1, \ldots, A_n$ and create a production $S \rightarrow \chi(A_1, \ldots, A_n)$ such that $A_i$ derives exactly $\bigcap_{k=1}^m T(G_{z_k})$ if $\gamma_i$ appears in constraints on $z_1, \ldots, z_m$ in $C$ and derives $F_{\Sigma}$ otherwise. By Theorem 2.1, the intersection can be described by a regular $\Sigma$-grammar. Nonterminal $S$ is the start symbol of the grammar. The finite types derivable from $A_i$ correspond precisely to those types that satisfy all constraints in $C$ involving $\gamma_i$.

For example, we construct regular $\Sigma$-grammars $G_+$ and $G_*$ for the parametric assumption set in Figure 2. Let $\Sigma_0 = \{\text{int, real}\}$ and $\Sigma_1 = \{\text{matrix}\}$. Due to the constraint on $+$ needed to assert that $*$ may stand for matrix multiplication, construction of $G_*$ depends on $G_+$. So we begin by factoring the assumptions for
+), leading to two regular tree grammars $G_1$ and $G_2$ where $G_1$ is

$$
S_1 \rightarrow \text{real} \mid \text{matrix}(U) \\
U \rightarrow \text{int} \mid \text{real} \mid \text{matrix}(U)
$$

and $G_2$ is

$$
S_2 \rightarrow \text{real} \mid \text{matrix}(S_3)
$$

$G_1$ arises from the assumptions for $+$ with the lone constraint on $+$ deleted. Therefore $U$ derives $F_\Sigma$. $G_2$ on the other hand is constructed from the assumptions with only constraints on $+$ which in this example is the same as the original set. The regular $\Sigma$-grammar $G_4$ for $T(G_1) \cap T(G_2)$ becomes

$$
[S_1, S_2] \rightarrow \text{real} \mid \text{matrix}([U, S_2]) \\
[U, S_3] \rightarrow \text{real} \mid \text{matrix}([U, S_2])
$$

Next we construct $G_4$. Corresponding to assumptions for $\ast$ without any constraints on $\ast$ is the grammar

$$
S_3 \rightarrow \text{int} \mid \text{real} \mid \text{matrix}([S_1, S_2])
$$

and to the assumptions with only constraints on $\ast$,

$$
S_4 \rightarrow \text{int} \mid \text{real} \mid \text{matrix}(S_4)
$$

$G_4$ then represents their intersection and is given by

$$
[S_3, S_4] \rightarrow \text{int} \mid \text{real} \mid \text{matrix}([S_1, S_2, S_3]) \\
[[S_1, S_2], S_4] \rightarrow \text{real} \mid \text{matrix}([U, S_3, S_4]) \\
[[U, S_2], S_4] \rightarrow \text{real} \mid \text{matrix}([U, S_3, S_4])
$$

Now if $A$ denotes the set of Figure 2, then for any closed finite type $\tau$, $A \vdash + : \tau \rightarrow \tau \rightarrow \tau$ is derivable if and only if $\tau \in T(G_4)$, likewise for $T(G_4)$. This actually follows from the next theorem which establishes the correctness of the representation.

**Theorem 2.2** If $A$ is parametric and $x$ is overloaded in $A$ with $LCG \forall \alpha. \tau$ and regular $\Sigma$-grammar $G_x = (N, \Sigma, P, S)$ then $A \vdash x : \tau[\alpha := \pi]$ iff $\pi \in T(G_x)$.

**Proof.** We use a normalized version of $ML_\alpha$, replacing $(\forall\text{-elim})$ with rule $(\forall\text{-elim'})$:

$$
x : \forall \bar{\alpha} \text{ with } C. \tau[\alpha := \bar{\alpha}] A \vdash C[\bar{\alpha} := \bar{\pi}]
$$

The normalized version and $ML_\alpha$ are proved equivalent in [Sm91]. We prove $\pi \in T(G_x)$ implies $A \vdash x : \tau[\alpha := \pi]$ by induction on the structure of $\pi$:

$(\tau = \chi)$. If $\chi \in T(G_x)$ then $S \vdash \chi \in P$ which implies $x : \tau[\alpha := \chi] \in A$. By rule (hypoth) then $A \vdash x : \tau[\alpha := \chi]$.

$(\pi = \chi(\bar{\tau}))$. If $\chi(\bar{\tau}) \in T(G_x)$ then $S \vdash \chi(\bar{\tau}) \in P, \bar{\tau} \in T(G_i)$, where $G_i = (N, \Sigma, P, \gamma_i)$, and $x : \forall \bar{\gamma} \text{ with } C. \tau[\alpha := \chi(\bar{\tau})] \in A$. Suppose $z_1, \ldots, z_m$ are all identifiers constrained in $C$ by $\gamma_i$. Since $A$ is parametric, $z_k : \rho_k \in C$ implies $z_k$ has $LCG \forall \gamma_i. \rho_k$ and $z_k$ is overloaded in $A$. By the construction of $G_x$ we have $T(G_i) = \bigcap_{k=1}^m T(G_{z_k})$ so $\pi \in T(G_{z_k})$ for $k = 1, \ldots, m$. By the inductive hypothesis, $A \vdash z_k : \rho_k[\gamma_i := \pi_i]$. So by rule $(\forall\text{-elim'})$, $A \vdash x : \tau[\alpha := \chi(\bar{\tau})]$.

Next we prove that $A \vdash x : \tau[\alpha := \pi]$ implies $\pi \in T(G_x)$ by induction on the length of the derivation of $A \vdash x : \tau[\alpha := \pi]$. The derivation ends with an application of rule (hypoth) or rule $(\forall\text{-elim'})$.

$(\forall\text{-elim'}).$ The derivation ends with

$$
x : \forall \bar{\alpha} \text{ with } C. \tau[\alpha := \chi(\bar{\tau})] A \vdash C[\bar{\alpha} := \bar{\pi}] \\
A \vdash x : \tau[\alpha := \chi(\bar{\tau})]
$$

Suppose $z_1, \ldots, z_m$ are all identifiers constrained in $C$ by $\gamma_i$. Since $A$ is parametric, $z_k : \rho_k \in C$ implies $z_k$ has $LCG \forall \gamma_i. \rho_k$ and $z_k$ is overloaded in $A$. Then $A \vdash C[\bar{\alpha} := \bar{\pi}]$ implies $A \vdash z_k : \rho_k[\gamma_i := \pi_i]$ so by the inductive hypothesis $\pi_i \in T(G_{z_k})$ for $k = 1, \ldots, m$, or $\pi \in \bigcap_{k=1}^m T(G_{z_k})$. Now $x : \forall \bar{\alpha} \text{ with } C. \tau[\alpha := \chi(\bar{\tau})] \in A$ implies $S \vdash \chi(\bar{\tau}) \in P$. By virtue of the construction of $G_x$, we have $\pi_i \in T(G_i)$ and therefore $\chi(\bar{\tau}) \in T(G_x)$. $\square$

3 CS-SAT is NP-hard for Parametric Overloading

The NP lower bound is proved by factoring a reduction from 3CNF-SAT through the problem of computing the intersection of a sequence of regular forests. Though this is unnecessary and a simpler proof is possible, it is done in order to isolate the source of the hardness which lies in computing this intersection.

**Theorem 3.1** Given a parametric assumption set $A$ with overloaded identifiers $x_1, \ldots, x_n$ whose assumptions are represented by regular tree grammars and a constraint set $C$ over $x_1, \ldots, x_n$ such that $x : p \in C$ implies $p$ is a generic instance of the LCG of $x$ in $A$, deciding whether $C$ is satisfiable under $A$ is NP-hard.

**Proof.** We give a P-time reduction from 3CNF-SAT. Given a 3CNF formula $E$, consisting of clauses
$d_1, \ldots, d_n$, we construct a parametric assumption set $A_E$, with all overloading represented by regular tree grammars, and a constraint set $C$ such that $C$ is satisfiable under $A_E$ if and only if $E$ is satisfiable.

Suppose $E$ has $m$ distinct variables $x_1, \ldots, x_m$ and let the ranked terminal alphabet $\Sigma = \Sigma_0 \cup \Sigma_1$ where $\Sigma_0 = \{\varepsilon\}$ and $\Sigma_1 = \{T, F\}$. Construct a regular $\Sigma$-grammar $G_d_i$ for each clause $d_i$ so that $\sigma \in T(G_d_i)$ if and only if

$$\sigma = B_1(B_2(\cdots B_m(\varepsilon)\cdots))$$

and the assignment of truth values $B_1, \ldots, B_m$ to $x_1, \ldots, x_m$ respectively satisfies $d_i$. If $d_i$ contains variables $x_j$, $x_k$, and $x_l$, with $j < k < l$, and $x_j \rightarrow B_j$, $x_k \rightarrow B_k$, and $x_l \rightarrow B_l$ is a truth assignment satisfying $d_i$, then construct a regular $\Sigma$-grammar with start symbol $x_1$ and productions

$$x_j \rightarrow B_j(x_{j+1}) \quad x_k \rightarrow B_k(x_{k+1}) \quad x_l \rightarrow B_l(x_{l+1})$$

and for $1 \leq i \leq m$ with $i \neq j, i \neq k$, and $i \neq l$,

$$x_i \rightarrow T(x_{i+1}) \mid F(x_{i+1})$$

and finally $x_{m+1} \rightarrow \varepsilon$. There is one such regular $\Sigma$-grammar for each of the 7 truth assignments satisfying $d_i$, call them $G_1, \ldots, G_7$. Then let

$$T(G_{d_i}) = \bigcup_{k=1}^{7} T(G_k)$$

$G_{d_i}$ can be constructed in $O(m)$ steps so that for each nonterminal $Y$ and truth value $B$, there is at most one production of the form $Y \rightarrow B(Z)$. For $1 \leq i \leq n$, add to $A_E$ assumption $X_i : \varepsilon$ if $X \rightarrow \varepsilon$ is a production of $G_{d_i}$ and assumption

$$Y_i : \forall \alpha \text{ with } Z_i : \alpha \cdot B(\alpha)$$

if $Y \rightarrow B(Z)$ is a production of $G_{d_i}$. If $G_{d_i}$ has start symbol $S_i$, then with

$$C = \{S_i : \alpha_1, \ldots, S_n : \alpha\}$$

$E$ is satisfiable if and only if $\bigcap_{i=1}^{n} T(G_{d_i})$ is nonempty, or if and only if $C$ is satisfiable under $A_E$. \[\square\]

As is the case for deciding whether a sequence of finite automata accept a common string, the source for the hardness of $CS$-$SAT$ lies not in deciding emptiness but rather in computing the intersection, in this case, of a sequence of regular forests $T(G_1), \ldots, T(G_m)$. The emptiness of $T(G)$ for a regular tree grammar $G$ is decidable in time $O(\mid G \mid^2)$ in the usual way.

From the proof of Theorem 3.1 then every problem in NP is P-time Turing reducible to the problem of constructing the intersection of a sequence of regular tree grammars, so the construction is NP-hard. This helps to explain why the worst-case time complexity of an improved algorithm for computing the intersection of regular forests is still exponential [AiM91]. Actually computing the intersection is much harder. A weak PSPACE-hard lower bound follows immediately from the finite automaton intersection problem, treating strings as unary trees. A tighter exponential time lower bound follows from the complexity of the intersection problem for tree automata [FSV91]. For a fixed $m$, it can be computed in polynomial time.

## 4 Conclusion

Some might argue that given that ML typability is complete for DEXPTIME [KTU90], the fact that $CS$-$SAT$ is NP-hard is insignificant. If we were concerned only about the worst-case time complexities of type inference algorithms then this might be true. But experience has shown that the DEXPTIME lower bound is not an issue in practice and type inference algorithms whose worst-case time complexities are exponential perform quite well on practical programs. In fact it was folklore for many years that ML typability could be decided in polynomial time. So the complexity of $CS$-$SAT$ could very well be the dominating complexity in practice. More experience is needed though in using systems like ML to determine whether the NP lower bound for $CS$-$SAT$ is a practical limitation.

## References


