

The Semantics of K

Formal Systems Laboratory
University of Illinois

August 8, 2017

Please feel free to contribute to this report in all ways. You could add new contents, remove redundant ones, refactor and organize the texts, and correct typos.

1 The Kore Language

1.1 Preliminary

Let us recall the basic grammar of matching logic. We have a countable set of *variable identifiers* to construct logic variables, denoted as N , by definition. Assume a matching logic signature (S, Σ) , which contains a nonempty finite (or infinite?) set of *sorts* and a countable set of *symbols*. Each symbol $\sigma \in \Sigma$, which has a unique identifier in Σ , has a fixed number of arguments, fixed argument sorts, and a fixed result sort. The well-formed patterns of sort $s \in S$ in generated by the next grammar:

$$\begin{aligned} \varphi_s ::= & x:s \quad \text{where } x \in N \\ & | \varphi_s \wedge \varphi_s \\ & | \neg \varphi_s \\ & | \exists x:s'. \varphi_s \quad \text{where } x \in N \text{ and } s' \in S \\ & | \sigma(\varphi_{s_1}, \dots, \varphi_{s_n}) \quad \text{where } \sigma \in \Sigma \text{ has } n \text{ arguments, and } \dots \end{aligned}$$

Remark 1. The above *is* a formal grammar, whose semantics¹ is well studied and crystal clear. The grammar defines for each sort s exactly one set of well-formed patterns of sort s . We are defining a *set*, that is to say, following the above grammar, one is able to (1) distinguish well-formed patterns from ill-formed ones; and (2) decide whether two well-formed patterns are the same pattern or not. The next remark provides an example of (2).

Remark 2. Assume $x, y \in N$ and $s \in S$, pattern $x:s \wedge y:s$ is a well-formed pattern of sort s , by definition. It is also *distinct* from pattern $y:s \wedge x:s$, by

¹Semantics as a formal grammar, not the matching logic semantics.

definition. The fact that (after introducing equalities as syntactic sugar in the logic) one can use some proof systems of matching logic and establish

$$\vdash x:s \wedge y:s = y:s \wedge x:s,$$

or use the semantics of matching logic and establish

$$\models x:s \wedge y:s = y:s \wedge x:s,$$

has *nothing* to do with the formal grammar itself and does not change the fact that $x:s \wedge y:s$ and $y:s \wedge x:s$ are two distinct patterns in matching logic.

Definition 3 (Matching Logic Theory). A matching logic theory (S, Σ, A) is a triple that contains a nonempty finite set of sorts, a finite or countably infinite set of symbols, and a recursive set of axioms. Two theories are *equal* if they have the same set of sorts and symbols, and they deduce the same set of theorems.

I am trying to capture the meta-level theory in the next definition.

Definition 4 (The Meta-level Theory). The meta-level theory, denoted as U , is a matching logic theory together with a lifting operator $\langle \cdot \rangle$, such that for any theory T and pattern φ ,

$$T \vdash \varphi \quad \text{iff} \quad U \cup \langle T \rangle \vdash \langle \varphi \rangle.$$

This is simply wrong.

1.2 The Kore Language

Definition 5 (The Kore Language). The Kore language is a language to write matching logic theories. The outcomes are called Kore definitions. Kore definitions are mainly served as the interface between a K frontend and a K backend, but a human should be able to read and write Kore definitions of simple theories, too. The Kore language is designed in a way that:

- Every Kore definition defines exactly one matching logic theory;
- Every matching logic theory can be defined as a Kore definition;
- There is no parsing ambiguity.
- The least amount of inferring is needed;
- Symbols are decorated with their argument sorts and result sort;
- There is no polymorphic or overloaded symbols, so every symbol has a unique name (reference).

Definition 6 (Frontend). A K frontend is an artifact that generates Kore definitions.

Definition 7 (Backend). A K backend is an artifact that consumes a Kore definition of a theory T and does some work. Whatever it does can and should be algorithmically reduced to the task of proving $T \vdash \varphi$ where φ “encodes” that work. A K backend should justify its results by generating formal proofs that can be proof-checked by the oracle matching logic proof checker. Examples of K backends include concrete execution engines, symbolic executions engines, matching logic provers, verification tools, etc.

Some discussions. We spent lots of time considering the design of the Kore language, with which we specify matching logic theories, and we decided to go for meta-logic. This paragraph is a summary that serves as a justification of our choice.

Suppose we allow users to write infinite axioms to specify theories. In that case, there is no need to go for a meta-logic, since one can always enumerate all axioms in Kore definitions, as long as they are recursively enumerable (r.e.). Theories who do not have a r.e. set of axioms are not considered as of interest of practice.

However, we cannot afford our definitions to run forever. We look for a finite representation of them. This is when the concept of meta-variables comes in and plays a role. And soon one realizes that we do not only need meta-variables, but also some notations in the meta-level, too, serving as methods that help us finitely represent the infinite sets of axioms we want to specify. One typical such notation is the substitution $\varphi[\psi/x]$, where $[-/ -]$ is the mathematical notation, in the meta-level, for substitution, which is not part of the object-logic. Other examples include side-conditions on meta-variables and context.

We look for a generic way that helps us represent infinite axioms in a finite way. And there is a natural one. Since axioms are r.e. sets, by definition there are semi-decision procedures that define them, and semi-decision procedures have finite representation. Therefore, instead of enumerating all the axioms, one simply write down the corresponding semi-decision procedure.

The next grammar of the Kore language is proposed to declare matching logic signatures, to write matching logic patterns, and to specify matching logic theories (as Kore modules). The grammar is supposed to be *minimal* w.r.t. “completeness”, in the sense that one is able to specify any “interesting” theories using the Kore language. Languages such as eKore will be proposed as syntactic sugar of the Kore language, and will (probably) include useful commands such as `import` and logic connectives such as `\forall`.

```
// Namespaces for sorts, variables, metavariables,
// symbols, and Kore modules.
SortId      = ...
VariableId  = ...
MetaVariableId = ...
SymbolId    = ...
ModuleId    = ...
```

```

Variable      = VariableId:SortId
MetaVariable  = MetaVariableId::SortId
// or MetaVariable = MetaVariableId:SortId
// if two namespaces are disjoint

Pattern  = Variable
         | MetaVariable
         | \and(Pattern, Pattern)
         | \not(Pattern)
         | \exists(Variable, Pattern)
         | SymbolId(List{Pattern})
         | #up(Pattern)
         | #down(Pattern)

Signature = syntax SortId
         | syntax SortId ::= SymbolId(List{SortId})
         | Signature Signature

Axioms    = axiom Pattern
         | Axioms Axioms

Module    = module ModuleId
         Signature
         Axioms
         endmodule

```

(1) Is alpha-renaming assumed in Kore? In other words, are `exsits(x, x)` and `exists(y, y)` the same or not? If alpha-renaming is assumed (as in the matching logic paper), then they are *the same thing*.

(2) By “the same thing”, we mean they are the same matching logic pattern, not that they can be proved equal or something like that. For example, an implementation of Kore is free to rename bound variables to prevent free variables capturing.

(3) So far so good until we have `#up`, a monster that lives outside the peaceful land of matching logic, because `exsits(x, x)` and `exists(y, y)` will have different metarepresentations.

(4) This will cause problems. For example, one writes a function `boundVars`, calls it on `exsits(x, x)`, expects seeing `{x}`, but gets surprised by seeing `{y}`, or even `{_fv__$142857}`, simply because of alpha-renaming.

(5) It is not alpha-renaming but `#up` the trouble maker I would say.

(6) I started to consider such problems when I tried to define `isLTerm` that checks lambda terms. Consider the next definition:

1. $\text{isLTerm}(\#up(x)) = \text{true}$
2. $\text{isLTerm}(\#up(\exists x.\lambda_0(x, e))) = \text{isLTerm}(e)$
3. ...

Axiom (1) is just wrong, because $\#up(x)$ is $\#var("x")$, and the axiom becomes $\text{isLTerm}(\#var("x")) = \text{true}$. So instead of writing (1), one should write $\text{isLTerm}(\#var(s:String)) = \text{true}$.

Think of axiom (2), too. The l.h.s. is basically

$\text{isLTerm}(\#exists(\#var("x"), \#app(\#symbol("lambda0"), \#append(\dots, \#up(e)))))$.

Notice how variable x becomes a domain value $\#var("x")$ in the meta-level.

(7) We need some “formal semantics” of $\#up$, if we want to seriously incorporate our logic with it and not just regard it as an implementation trick. In Maude, the meta-level is a theory U together with a lifting operator $\langle \cdot \rangle$ such that

$$R \vdash t_1 \rightarrow t_2 \quad \text{iff} \quad U \vdash \langle R, t1 \rangle \rightarrow \langle R, t2 \rangle,$$

where $\langle \cdot \rangle$ is not defined in the logic. I am trying to come up with a similar thing in Definition 4 but failed.

Here we provide a list of potential questions and their quick answers. All questions will be addressed again and answered in full details in later sections, so if you do not satisfy the short answers listed below, please read the entire proposal before addressing a comment.

Question A: Why propose a minimal one?

Answer: This is because matching logic and matching logic theories are the foundation of everything we do within the K framework. The Kore language is designed as the universal language to specify all matching logic theories used in the K framework. By having a minimal such language, we require the minimal amount of common knowledge among all K tools, and leave the most amount of flexibility to their developers.

Question B: What are metavariables?

Answer: They are mathematical variables for patterns. Check this.

Question C: Why do we need metavariables? They are not part of the grammar of matching logic.

Answer: Metavariables are not part of the grammar. We need them in the Kore language because some theories have axiom schemata, which contain metavariables, and there is no way to define those schemata as a finite number of (object-level) axioms. If we do not have metavariables, we end up with theories which has an infinite list of axioms, and we cannot afford that.

Question D: What is #up?

Answer: It takes a pattern to its metarepresentation.

Question E: Why do we need #up?

Answer: In some important theories we need restricted metavariables, and we decided to go to meta-level for that, and #up let us go to the meta-level.

Question F: Why does a minimal language have #up?

Answer: This is because #up cannot be defined within the logic, no matter how.

Question G: Does it mean every K tools have to support the meta-level, since #up is in Kore?

Answer: No. K tools are free to support fragment of matching logic. A concrete execution engine will not bother with variables, and a theorem prover for quantifier free theories will not bother with \exsits.

Question H: What is the formal semantics of #up?

Answer: Sounds like a good question.

2 Object-level and Meta-level

It is an aspect of life in mathematical logics to distinguish the *object-level* and *meta-level* concepts. In matching logic, we put more emphasize and care on metavariables and their range, that is, the set of patterns that they stand for. It turns out that having metavariables that range over all well-formed patterns will lead us to inconsistency theories immediately. As an example, consider the (β) axiom in the matching logic theory LAMBDA of lambda calculus:

$$(\lambda x.e)[e'] = e[e'/x].$$

If we do not put any restriction on the range of metavariables e and e' , we have an inconsistency issue as the following reasoning shows:

$$\perp \stackrel{(\mathbf{N})}{=} (\lambda x.\top)[\perp] \stackrel{(\beta)}{=} \top[\perp/x] = \top.$$

Therefore, in matching logic, one should explicitly specify the range of metavariables whenever he uses them.

Definition 8 (Restricted metavariables). Let φ be a metavariable of sort $s \in S$. The range of φ is a set of patterns of sort s . We write $\varphi :: R$ if the range of φ is $R \subseteq \text{Pattern}_s$.

Remark 9 (Metavariables in first-order logic). In first-order logic, one often uses metavariables in axiom schemata, but the inconsistency issue does not arise.

This is because in first-order logic, we do not need to distinguish metavariables for terms from logic variables, thanks to the next (Substitution) rule:

$$\forall x.\varphi(x) \rightarrow \varphi(t).$$

The predicate metavariables are not a problem because there are no object level symbols on top of them.

I don't get the point of predicate metavariables.

Variables and metavariables for variables For any matching logic theory $\mathbb{T} = (S, \Sigma, A)$, it comes for each sort $s \in S$ a countably infinite set V_s of variables. We use $x : s, y : s, z : s, \dots$ for variables in V_s , and omit their sorts when that is clear from the contexts. Different sorts have disjoint sets of variables, so $\text{Var}_s \cap \text{Var}_{s'} = \emptyset$ if $s \neq s'$.

Proposition 10. *Let A be a set of axioms and $\bar{A} = \forall A$ be the universal quantification closure of A , then for any pattern φ , $A \vdash \varphi$ iff $\bar{A} \vdash \varphi$.*

Remark 11 (Free variables in axioms). The free variables appearing in the axioms of a theory can be regarded as implicitly universal quantified, because a theory and its universal quantification closure are equal.

Example 12.

$$\begin{aligned} A_1 &= \{\text{mult}(x, 0) = 0\} \\ A_2 &= \{\forall x.\text{mult}(x, 0) = 0\} \\ A_3 &= \{\forall y.\text{mult}(y, 0) = 0\} \\ A_4 &= \{\text{mult}(x, 0) = 0\} \\ A_5 &= \{\forall x.\text{mult}(x, 0) = 0\} \\ A_6 &= \{\forall y.\text{mult}(y, 0) = 0\} \\ A_7 &= \{\text{mult}(x, 0) = 0, \text{mult}(y, 0) = 0, \text{mult}(z, 0) = 0, \dots\} \\ A_8 &= \{\forall x.\text{mult}(x, 0) = 0, \forall y.\text{mult}(y, 0) = 0, \forall z.\text{mult}(z, 0) = 0, \dots\} \end{aligned}$$

All the eight theories are equal. Theories A_4, A_5, A_6 are finite representations of theories A_7, A_8, A_8 respectively.

Remark 13. There is no need to have metavariables for variables in the Kore language, because (1) if they are used as bound variables, then replacing them with any (matching logic) variables will result in the same theories, thanks to alpha-renaming; and (2) if they are used as free variables, then it makes no difference to consider the universal quantification closure of them and we get to the case (1).

~~Given said that, there are cases when metavariables for variables make sense. In those cases we often want our metavariables to range over all variables of all sorts, in order to make our Kore definitions compact. No, we do not need metavariables over variables. I was~~

thinking of the definedness symbols. We might want to write only one axiom schema of $[x]$ instead many $[x:s]_s^{s'}$'s, but we cannot do that unless we allow polymorphic and overloaded symbols in Kore definitions.

Patterns and metavariables for patterns It is in practice more common to use metavariables that range over all patterns. One typical example is axiom schemata. For example, $\vdash \varphi \rightarrow \varphi$ in which φ is the metavariable that ranges all well-formed patterns.

There has been an argument on whether metavariables for patterns should be sorted or not. Here are some observations. Firstly, since all symbols are decorated and not overloaded, in most cases, the sort of a metavariable for patterns can be inferred from its context. Secondly, the only counterexample against the first point that I can think of is when they appear alone, which is not an interesting case anyway. Thirdly, we do want the least amount of reasoning and inferring in using Kore definitions, so it breaks nothing if not helping things to have metavariables for patterns carrying their sorts.

Example 14.

$$\begin{aligned} A_1 &= \{\text{merge}(h1, h2) = \text{merge}(h2, h1)\} \\ A_2 &= \{\forall h1 \forall h2. \text{merge}(h1, h2) = \text{merge}(h2, h1)\} \\ A_3 &= \{\text{merge}(\varphi, \psi) = \text{merge}(\psi, \varphi)\} \end{aligned}$$

All three theories are equal. It is easier to see that fact from a model theoretic point of view, since all theories require that the interpretation of `merge` is commutative and nothing more. On the other hand, it is not straightforward to obtain that conclusion from a proof theoretic point of view. For example, to deduce $\text{merge}(\text{list}(\text{one}, \text{cons}(\text{two}, \text{epsilon})), \text{top}) = \text{merge}(\text{top}, \text{list}(\text{one}, \text{cons}(\text{two}, \text{epsilon})))$ needs only one step in A_3 , but will need a lot more in either A_1 or A_2 , because one cannot simply substitute any patterns for universal quantified variables in matching logic.

2.1 The module META – LEVEL

The theory of meta-level in matching logic provides a universe of metarepresentation (abstract syntax trees) of object-level patterns. The theory of meta-level helps us specify the range of metavariables and much more. One important observation is that the connection between object-level modules and the meta-level module cannot be defined in the logic itself. More specifically, the operator `#up` that takes object-level patterns to their metarepresentation in the meta-level module cannot be defined in the logic no matter how. Consider the next simple example where one defines a symbol `isGround` that checks whether a pattern is

a ground pattern or not, using the meta-level module:

```
isGround(#up[X]) = false
isGround(#up[σ]) = true
isGround(#up[σ(φ1, ..., φn)]) =
  andBool(isGround(#up[φ1]), ..., isGround(#up[φn]))
isGround(#up[φ ∧ ψ]) =
  andBool(isGround(#up[φ]), isGround(#up[ψ]))
...
```

Unfortunately, the first two axioms lead us to inconsistency, as shown in the following:

```
isGround(#up[X - X]) = false
isGround(#up[zero]) = true
```

The only way to prevent such inconsistency issue is to prevent equations propagating through `#up`, more specifically, to forbid the next inference rule:

From $\varphi = \psi$ deduce $\#up[\varphi] = \#up[\psi]$,

which is a strong evidence that `#up` is not part of the logic.

We provide the Kore definition of the META – LEVEL module.

```
module META-LEVEL
  import STRING

  syntax Sort
  syntax SortList
  syntax Symbol
  syntax Name

  syntax Sort ::= #sort(String)
  syntax Name ::= #name(String)
  syntax Symbol ::= #symbol(Name, SortList, Sort)
  syntax SortList ::= #nilSortList()
                        | SortListAsSort(Sort)
                        | #appendSortList(SortList, SortList)

  syntax Pattern
  syntax Pattern ::= #variable(Name, Sort)
                    | #and(Pattern, Pattern)
                    | #not(Pattern)
                    | #exists(Name, Sort, Pattern)
                    | #application(Symbol, PatternList)

  syntax PatternList
```

```

syntax PatternList ::= #nil()
                    | #PatternListAsPattern(Pattern)
                    | #append(PatternList, PatternList)

syntax SortSet SymbolSet PatternSet // defined in the usual way

syntax Module
syntax Module ::= #module(SortSet, SymbolSet, PatternSet)

syntax Bool ::= #wellFormed(Pattern)
syntax Sort ::= #getSort(Pattern)
// more to go

endmodule

```

Using the `META – LEVEL` module, we can easily define the ranges of metavariables using *side conditions*. The next section illustrates that.

3 Binders

In matching logic there is a unified representation of binders. We will be using the theory of lambda calculus `LAMBDA` as an example in this section. Recall that the syntax for untyped lambda calculus is

$$\Lambda ::= V \mid \lambda V. \Lambda \mid \Lambda \Lambda$$

where V is a countably infinite set of atomic λ -terms, a.k.a. variables in lambda calculus. The set of all λ -terms, denoted as Λ , is the smallest set satisfying the above grammar.

The matching logic theory `LAMBDA` has one sort `Exp` for lambda expressions. It also has in its signature a binary symbol `lambda0` that builds a λ -terms, and a binary symbol `app` for lambda applications. To mimic the binding behavior of λ in lambda calculus, we define syntactic sugar $\lambda x.e = \exists x.\text{lambda}_0(x, e)$ and $e_1 e_2 = \text{app}(e_1, e_2)$ in theory `LAMBDA`. Notice that by defining λ as a syntactic sugar using the existential quantifier $\exists x$, we get alpha-renaming for free. The β -reduction is captured by the next axiom:

$$(\lambda x.e)e' = e[e'/x] \quad , \text{ where } e \text{ and } e' \text{ are metavariables for } \lambda\text{-terms.}$$

Two important observations are made about the (β) axiom. Firstly, e and e' cannot be replaced by logic variables, because λ -terms in matching logic are (often) not functional patterns. Secondly, metavariables e and e' cannot range over all patterns of sort `Exp`, but only those which are (syntactic sugar of) λ -terms. Allowing e and e' to range over all patterns of `Exp` will quickly lead to an inconsistent theory, because of the next contradiction:

$$\perp \stackrel{(N)}{=} (\lambda x.\top)[\perp] \stackrel{(\beta)}{=} \top.$$

Therefore, when defining the lambda calculus, we need a way

Theorem 15 (Consistency). *Consider a theory of a binder α , with a sort S and two binary symbols α_0 and $-..$. Define $\alpha x.e$ as syntactic sugar of $\exists x.\alpha(x, e)$ where x is a variable and e is a pattern. Define α -terms be patterns satisfying the next grammar*

$$T_\alpha ::= V_s \mid \alpha x.T_\alpha \mid T_\alpha T_\alpha.$$

If a theory contains only axioms of the form $e = e'$ where e and e' are α -terms, then the theory is consistent.

Proof. The final model M exists, in which the carrier set is a singleton set, and the two symbols are interpreted as the total function over the singleton set. One can then prove that all α -terms interpret to the total set, so all axioms hold in the final model. \square

Corollary 16. *The theory LAMBDA is consistent.*

Definition 17 (Common ranges of metavariables).

- Full range Pattern_s ;
- Syntactic terms range (variables plus symbols without logic connectives);
- Ground syntactic terms range (symbols only);
- Variable range Var_s (metavariables for variables).

Remark 18. Syntactic terms (and ground syntactic terms) are purely defined syntactically and not equal to terms or functional patterns. When all symbols are functional symbols, the set of syntactic terms equals the set of terms, and both of them are included in the set of all functional patterns.

Remark 19. We need to design a syntax for specifying ranges of metavariables in the Kore language.

Remark 20. We have not proved that matching logic is a conservative extension of untyped lambda calculus, which bothers me a lot. I will remain skeptical about everything we do in this section until we prove that conservative extension result.

The benefit of such a unified theory of binders and binding structures in matching logic is more of theoretical interest. In practice (K backends), one will never want to implement the lambda calculus by desugaring $\lambda x.e$ as $\exists x.\lambda_0(x, \varphi)$ but rather dealing with $\lambda x.\varphi$ directly.

Example 21 (Lambda calculus in Kore).

```
module LAMBDA
  import BOOL
  import META-LEVEL
```

```

syntax Exp
syntax Exp ::= app(Exp, Exp)
              | lambda0(Exp, Exp)

axiom \implies(true = andBool(#isLTerm(#up(E:Exp)),
                              #isLTerm(#up(E':Exp))),
              app(\exists(x:Exp, lambda0(x:Exp, E:Exp)), E':Exp)
                = E:Exp(E':Exp / x:Exp)

// Q1: what is substitution?
// Q2: we know #up is not a part of the logic, so what does
//      it mean?

syntax Bool ::= #isLTerm(Pattern)
axiom #isLTerm(#variable(x:Name, s:Sort)) = true
axiom #isLTerm(#application(
  #symbol(#name("app"), #appendSortList(...), #sort("Exp"))),
  #appendPatternList(#PatternListAsPattern(#P),
                    #PatternListAsPattern(#P')))))
= andBool(#isLTerm(#P), #isLTerm(#P'))
...
endmodule

```

Rewriting logic

4 Contexts

Introduce a binder γ together with its application symbol which we write as $[-]$. Binding variables of the binder γ are often written as \square , but in this proposal and hopefully in future work we will use regular variables x, y, z, \dots instead of \square , in order to show that there is nothing special about contexts but simply a theory in matching logic. Patterns of the form $\gamma x. \varphi$ are often called *contexts*, denoted by metavariables C, C_0, C_1, \dots . Patterns of the form $\varphi[\psi]$ are often called *applications*.

Definition 22. The context $\gamma x.x$ is called the identity context, denoted as \mathbf{l} . Identity context has the axiom schema $\mathbf{l}[\varphi] = \varphi$ where φ is any pattern.

Example 23. $\mathbf{l}[\mathbf{l}] = \mathbf{l}$.

Definition 24. Let $\sigma \in \Sigma_{s_1 \dots s_n, s}$ is an n -arity symbol. We say σ is *active* on its i th argument ($1 \leq i \leq n$), if

$$\sigma(\varphi_1, \dots, C[\varphi_i], \dots, \varphi_n) = (\gamma x. \sigma(\varphi_1, \dots, C[x], \dots, \varphi_n))[\varphi_i],$$

where $\varphi_1, \dots, \varphi_n$, and C are any patterns. Orienting the equation from the left to the right is often called *heating*, while orienting it from the right to the left is called *cooling*.

Example 25. Assume the next theory of IMP.

$$\begin{aligned}
A = \{ & \text{ite}(C[\varphi], \psi_1, \psi_2) = (\gamma x. \text{ite}(C[x], \psi_1, \psi_2))[\varphi], \\
& \text{while}(C[\varphi], \psi) = (\gamma x. \text{while}(C[x], \psi))[\varphi], \\
& \text{seq}(C[\varphi], \psi) = (\gamma x. \text{seq}(C[x], \psi))[\varphi], \\
& C[\text{ite}(\text{tt}, \psi_1, \psi_2)] \Rightarrow C[\psi_1], \\
& C[\text{ite}(\text{ff}, \psi_1, \psi_2)] \Rightarrow C[\psi_2], \\
& C[\text{while}(\varphi, \psi)] \Rightarrow C[\text{ite}(\varphi, \text{seq}(\psi, \text{while}(\varphi, \psi)), \text{skip})], \\
& C[\text{seq}(\text{skip}, \psi)] \Rightarrow C[\psi] \}.
\end{aligned}$$

We can simply require that ψ_1, ψ_2, ψ_3 , and C are any patterns. That will allow us to do any reasoning that we need, but will that lead to inconsistency?

Example 25(a).

$$\begin{aligned}
\text{seq}(\text{skip}, \text{skip}) &= \text{I}[\text{seq}(\text{skip}, \text{skip})] \\
&\Rightarrow \text{I}[\text{skip}] \\
&= \text{skip}.
\end{aligned}$$

Example 25(b).

$$\begin{aligned}
\text{seq}(\text{ite}(\text{tt}, \psi_1, \psi_2), \psi_3) &= \text{seq}(\text{I}[\text{ite}(\text{tt}, \psi_1, \psi_2)], \psi_3) \\
&= (\gamma x. \text{seq}(\text{I}[x], \psi_3))[\text{ite}(\text{tt}, \psi_1, \psi_2)] \\
&\Rightarrow (\gamma x. \text{seq}(\text{I}[x], \psi_3))[\psi_1] \\
&= \text{seq}(\text{I}[\psi_1], \psi_3) \\
&= \text{seq}(\psi_1, \psi_3).
\end{aligned}$$

Example 26. Consider the following theory written in the Kore language:

```

module IMP
  import ...
  syntax AExp
  syntax AExp ::= plusAExp(AExp, AExp)
  syntax AExp ::= minusAExp(AExp, AExp)
  syntax AExp ::= AExpAsNat(Nat)
  syntax BExp
  syntax BExp ::= geBExp(AExp, AExp)
  syntax BExp ::= BExpAsBool(Bool)
  syntax Pgm
  syntax Pgm ::= skip()
  syntax Pgm ::= seq(Pgm Pgm)
  syntax Pgm ::=

```

```

syntax Heap
syntax Cfg

endmodule

```

Example 27. Following the above example, extend A with the next axioms:

$$\begin{aligned}
&\{C[x][\text{mapsto}(x, v)] \Rightarrow C[v][\text{mapsto}(x, v)], \\
&C[\text{asgn}(x, v)][\text{mapsto}(x, v')] \Rightarrow C[\text{skip}][\text{mapsto}(x, v)], \\
&C[\text{asgn}(x, v)][\varphi] \Rightarrow C[\text{skip}][\text{merge}(\varphi, \text{mapsto}(x, v))]\}
\end{aligned}$$

The above example is meant to show the loopup rule, but it does not work because the third axiom is incorrect. Instead of simply writing φ , we should say that φ does not assign any value to x . One solution (that is used in the current K backend) is to introduce a strategy language and to extend theories with strategies.

Example 28. Suppose f and g are binary symbols who are active on their first argument. Suppose a, b are constants, and x is a variable. Let \square_1 and \square_2 be two hole variables. Define two contexts $C_1 = \gamma\square_1.f(\square_1, a)$ and $C_2 = \gamma\square_2.g(\square_2, b)$.

Because f is active on the first argument,

$$\begin{aligned}
C_1[\varphi] &= (\gamma\square_1.f(\square_1, a))[\varphi] \\
&= (\gamma\square_1.f(\text{!}[\square_1], a))[\varphi] \\
&= f(\text{!}[\varphi], a) \\
&= f(\varphi, a), \text{ for any pattern } \varphi.
\end{aligned}$$

And for the same reason, $C_2[\varphi] = g(\varphi, b)$. Then we have

$$\begin{aligned}
C_1[C_2[x]] &= C_1[f(x, a)] \\
&= g(f(x, a), b).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
g(f(x, a), b) &= g(C_1[x], b) \\
&= (\gamma\square.g(C_1[\square], b))[x] \\
&= (\gamma\square.g(f(\square, a), b))[x].
\end{aligned}$$

Therefore, the context $\gamma\square.g(f(\square, a), b)$ is often called the *composition* of C_1 and C_2 , denoted as $C_1 \circ C_2$.

Example 29. Suppose f is a binary symbol with all its two arguments active. Suppose C_1 and C_2 are two contexts and a, b are constants. Then easily we get

$$\begin{aligned}
f(C_1[a], C_2[b]) &= (\gamma\square_2.f(C_1[a], C_2[\square_2]))[b] \\
&= (\gamma\square_2.((\gamma\square_1.f(C_1[\square_1], C_2[\square_2]))[a]))[b].
\end{aligned}$$

What happens above is similar to *currying* a function that takes two arguments. It says that there exists a context C_a , related with C_1, C_2, f and a of course, such that $C_a[b]$ returns $f(C_1[a], C_2[b])$. The context C_a has a binding hole \square_2 , and a body that itself is another context C'_a applied to a . In other words, there exists C_a and C'_a such that

- $f(C_1[a], C_2[b]) = C_a[b]$,
- $C_a = \gamma \square_2. (C'_a[a])$,
- $C'_a = \gamma \square_1. f(C_1[\square_1], C_2[\square_2])$.

A natural question is whether there is a context C such that $C[a][b] = f(C_1[a], C_2[b])$.

Proposition 30. $C_1[C_2[\varphi]] = C[\varphi]$, where $C = \gamma \square. C_1[C_2[\square]]$.

4.0.1 Normal forms

In this section, we consider *decomposition* of patterns. A decomposition of a pattern P is a pair $\langle C, R \rangle$ such that $C[R] = P$. Let us now consider patterns that do not have logical connectives.

Fixed points

5 The Kore language

The next grammar is the firstly-proposed Kore language at [here](#).

```

Definition = Attributes
Set{Module}

Module = module ModuleName
Set{Sentence}
endmodule
Attributes

Sentence = import ModuleName Attributes
| syntax Sort Attributes // sort declarations
| syntax Sort ::= Symbol(List{Sort}) Attributes // symbol declarations
| rule Pattern Attributes
| axiom Pattern Attributes

Attributes = [ List{Pattern} ]

Pattern = Variable
| Symbol(List{Pattern}) // symbol applications
| Symbol(Value) // domain values
| \top()

```

```

| \bottom()
| \and(Pattern, Pattern)
| \or(Pattern, Pattern)
| \not(Pattern)
| \implies(Pattern, Pattern)
| \exists(Variable, Pattern)
| \forall(Variable, Pattern)
| \next(Pattern)
| \rewrite(Pattern, Pattern)
| \equals(Pattern, Pattern)

Variable = Name:Sort                                // variables

ModuleName = RegEx1
Sort       = RegEx2
Name       = RegEx2
Symbol     = RegEx2
Value      = RegEx3

RegEx1 == [A-Z][A-Z0-9-]*
RegEx2 == [a-zA-Z0-9.@#%~_-]+ | ' [^']* '
RegEx3 == <Strings>    // Java-style string literals, enclosed in quotes

```

In the grammar above, `List{X}` is a special non-terminal corresponding to possibly empty comma-separated lists of `X` words (trivial to define in any syntax formalism). `Set{X}`, on the other hand, is a special non-terminal corresponding to possibly empty space-separated sets of `X` words. Syntactically, there is no difference between the two (except for the separator), but Kore tools may choose to implement them differently.

5.1 Builtin theories

```

module BOOL
syntax Bool
syntax Bool ::= true | false | notBool(Bool)
| andBool(Bool, Bool) | orBool(Bool, Bool)

// axioms for functional symbols
axiom \exists(T:Bool, \equals(T:Bool, true))
axiom \exists(T:Bool, \equals(T:Bool, false))
axiom \exists(T:Bool, \equals(T:Bool, \notBool(X:Bool)))
axiom \exists(T:Bool, \equals(T:Bool, andBool(X:Bool, Y:Bool)))
axiom \exists(T:Bool, \equals(T:Bool, orBool(X:Bool, Y:Bool)))

// axioms for commutativity
axiom \equals(andBool(X:Bool, Y:Bool), andBool(Y:Bool, X:Bool))
axiom \equals(orBool(X:Bool, Y:Bool), orBool(Y:Bool, X:Bool))

```



```

// the no-junk axiom for constructors
axiom \or(true, false)

axiom \equals(notBool(true), false)
axiom \equals(notBool(false), true)
axiom \equals(andBool(true, T:Bool), T:Bool)
axiom \equals(andBool(false, T:Bool), false)
axiom \equals(orBool(true, T:Bool), true)
axiom \equals(orBool(false, T:Bool), T:Bool)
endmodule

module META-LEVEL
syntax
endmodule

module LAMBDA
syntax Exp
syntax Exp ::= lambda0(Exp, Exp) | app(Exp, Exp)

endmodule

```