Lecture Notes on
Subsingleton Logic

15-317: Constructive Logic
Frank Pfenning

Lecture 23
November 28, 2017

1 Introduction

In this lecture we will first define subsingleton logic which is the subset of ordered logic where each judgment has at most one antecedent. Then we provide an operational interpretation of subsingleton logic in which cut reduction drives computation. This is in contrast to what we have been doing so far, where logical inference, that is, proof construction models computation.

The correspondence from this lecture is summarized in the following table.

<table>
<thead>
<tr>
<th>Logic</th>
<th>Programming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propositions</td>
<td>Session types</td>
</tr>
<tr>
<td>Ordered proofs</td>
<td>Concurrent programs</td>
</tr>
<tr>
<td>Cut reduction</td>
<td>Communication</td>
</tr>
</tbody>
</table>

This is an instance of a very general connection between proofs and programs studied in type theory. We can vary the logic and the computational interpretation. The big upside of this form of correspondence is that it helps us design programming languages in concert with the logic for reasoning about its programs.

This analysis was pioneered by Curry [Cur34] who related proofs in axiomatic form with combinatory logic. Late, Howard [How69] made the discovery that the Church’s simply typed λ-calculus was in bijective correspondence with intuitionistic natural deduction. The particular instance of this correspondence for subsingleton logic is a recent discovery by DeYoung and yours truly [DP16].
2 Subsingleton Logic

We can examine the rules for each of the connectives to see which of them are still meaningful if we restrict ourselves to at most one antecedent. For example,

\[
\frac{\Omega \vdash A \quad \vdash B / A}{\Omega \vdash B / A} \quad \text{/R}
\]

would have a premise with two antecedents if the conclusion has only one.

What remains from the connectives we have introduced so far is only \(x \& y\) and \(1\). But we haven’t had a notion of disjunction yet, which is written as \(x \oplus y\). It is a disjunction, which means that \(x \oplus y\) is true if either \(x\) or \(y\) is true. So we have two right rules:

\[
\frac{\Omega \vdash A}{\Omega \vdash A \oplus B} \quad \oplus R_1 \quad \frac{\Omega \vdash B}{\Omega \vdash A \oplus B} \quad \oplus R_2
\]

Knowing that \(x\) or \(y\) is true, but not which one, means that the left rule proceeds by cases.

\[
\frac{\Omega_L A \quad \Omega_R \vdash C \quad \Omega_L B \quad \Omega_R \vdash C}{\Omega_L (A \oplus B) \quad \Omega_R \vdash C} \quad \oplus L
\]

It is straightforward to check the identity expansion and cut reduction, as well as extend the proof of cut elimination accordingly. Disjunction, just like the alternative conjunction, make sense in subsingleton logic.

We summarize the rules of subsingleton logic, with two small notational changes: we write \(\omega\) for zero or one antecedent.

\[
\frac{\vdash A}{A \vdash A} \quad \text{id}_A \quad \frac{\omega \vdash A \quad A \vdash C}{\omega \vdash A \quad A \vdash C} \quad \text{cut}_A
\]

\[
\frac{\omega \vdash A}{\omega \vdash A \oplus B} \quad \oplus_1 \quad \frac{\omega \vdash B}{\omega \vdash A \oplus B} \quad \oplus_2 \quad \frac{A \vdash C \quad B \vdash C}{A \oplus B \vdash C} \quad \oplus L
\]

\[
\frac{\omega \vdash A \quad \omega \vdash B}{\omega \vdash A \& B} \quad \& R \quad \frac{A \vdash C \quad B \vdash C}{A \& B \vdash C} \quad \& L_1 \quad \frac{A \& B \vdash C}{A \& B \vdash C} \quad \& L_2
\]

\[
\frac{}{\vdash 1} \quad 1R \quad \frac{\vdash C}{1 \vdash C} \quad 1L
\]
### 3 Proofs as Programs

We write $\omega \vdash P : A$ with two alternative interpretations:

1. $P$ is a proof of $A$ with antecedent $\omega$.
2. $P$ is a process providing $A$ and using $\omega$.

Two processes are composed by cut, so that if

$$\omega \vdash P : A \quad A \vdash Q : C$$

then $P$ and $Q$ can run next to each other and exchange messages. Which messages can be exchanged is dictated by the type (= proposition) $A$.

As an example, consider

$$\omega \vdash P : A \oplus B \quad A \oplus B \vdash Q : C$$

The proof $P$ of $A \oplus B$ will contain critical information, namely if $A$ is true or if $B$ is true. Since the proof $Q$ of $C$ must account for both possibilities, we see that $P$ will eventually send some information (inl if $A$ is true, or inr if $B$ is true) and $Q$ will receive it. In a synchronous communication model, the message exchange can only take place if both sides are ready, which correspond to a principal case of cut where $A \oplus B$ is the principal formula in both inferences. Using this intuition to fill in proof terms for one of the cases we arrive at:

$$\begin{array}{c}
\omega \vdash P : A \\
A \vdash Q_1 : C \\
B \vdash Q_2 : C \\
A \oplus B \vdash (\text{caseL (inl } \Rightarrow Q_1 \mid \text{inr } \Rightarrow Q_2)) : C
\end{array} \quad \oplus L$$

This reduces to the new cut at type $A$

$$\omega \vdash P : A \quad A \vdash Q_1 : C$$

So we think of $(\text{R.inl ; } P)$ as sending the label inl to the right and then continuing as $P$, while caseL (inl $\Rightarrow Q_1 \mid$ inr $\Rightarrow Q_2$) receives either inl or inr from the left and continues as $Q_1$ or $Q_2$, respectively. The types $A$ that type the interface between two processes are called session types (see [HHN+14] for a survey). A strong logical foundation for session types in linear logic was discovered by Caires and your lecturer [CP10] and later extended by others [Wad12, CPT13, Ton15].

If $\oplus R_2$ was used in the first proof, then the new cut would be at type $B$. In either case, the communication corresponds exactly to a principal case in cut reduction.
Looking at computation more globally, processes are configured into a linear chain

\[ P_1 \mid P_2 \mid P_3 \mid \cdots \mid P_n \]

Such a configuration is well-typed if we have

\[(\omega_0 \vdash P_1 : A_1) \quad (A_1 \vdash P_2 : A_2) \quad (A_2 \vdash P_3 : A_3) \quad \cdots \quad (A_n \vdash P_n : A_n)\]

where for any two adjacent processes, the type \( A_i \) provided by \( P_i \) has to be the same as the one used by \( P_{i+1} \).

We now go through the rules and connective of ordered logic and develop the operational interpretation of proofs.

**Cut as Composition.** Cut is straightforward, since it just corresponds to parallel composition.

\[
\begin{align*}
\omega \vdash P : A \\
A \vdash Q : C
\end{align*}
\]

\[\frac{}{\omega \vdash (P \mid Q) : C} \text{cut}_A\]

Computationally, a process \( P \mid Q \) will spawn \( P \) and continue as \( Q \) which might written as

\[
\frac{}{(P \mid Q) \mid Q}
\]

\[\frac{}{P \mid Q} \]

Clearly, this rule preserves the typing invariant for a configuration if \((P \mid Q)\) is typed by the cut rule, since the type \( A \) provided by \( P \) is exactly the same as the one as used by \( Q \), and the left and right interfaces \( \omega \) and \( C \), respectively, are preserved.

**Identity as Forwarding.** Cut creates two processes from one, while identity removes one process from the configuration, acting like a “forwarding” between the processes to its sides.

\[\frac{}{A \vdash \leftrightarrow : A} \text{id}_A\]

The computation rule simply removes the process from the configuration.

\[\frac{}{\leftrightarrow} \]
Again, this preserves the typing invariant for configurations since the processes to the left and right of \((\leftrightarrow)\) have the same type \(A\) on the right and left sides, respectively.

Now we come to the logical connectives. We already foreshadowed the case for disjunction, but we first generalize it to be more amenable for programming without changing its logical meaning.

**Disjunction as Internal Choice.** We generalize disjunction to be an \(n\)-ary connective by writing \(\oplus\{l_i : A_i\}_{i \in I}\) for some finite index set \(I\) and labels \(l_i\). Now the binary disjunction is defined as \(A \oplus B = \oplus\{\text{inl} : A, \text{inr} : B\}\). Disjunction is also called *internal choice* since the proof itself determines which of the alternatives is chosen.

The right rule will send the appropriate label while the left rule will receive it and branch on it.

\[
\frac{\omega \vdash P : A_k \quad (k \in I) \quad A_i \vdash Q_i : C \quad (\text{for all } i \in I)}{\omega \vdash (R.l_k ; P) : \oplus\{l_i : A_i\}_{i \in I} \quad \oplus L}
\]

Again, the computation rule just mirrors the cut reduction and therefore is easily seen to preserve configuration typing.

\[
\frac{(R.l_k ; P) \mid (\text{caseL}(l_i \Rightarrow P_i)_{i \in I})}{P_k \mid Q_k}
\]

The interface type between the two adjacent processes transitions from \(\oplus\{l_i : A_i\}_{i \in I}\) to \(A_k\) for some \(k \in I\).

**Alternative Conjunction as External Choice.** Again, we generalize from \(A \& B\) to \&\{\(l_i : A_i\)\}_{i \in I}\ and defined \(A \& B = \&\{\text{inl} : A, \text{inr} : B\}\). \(A \& B\) is sometimes called *external choice* since its proof must account for both possibilities and the client selects between them. Otherwise, it is the straightforward dual of \(\oplus\), sending to the left and receiving from the right.

\[
\frac{\omega \vdash P_i : A_i \quad (\text{for all } i \in I)}{\omega \vdash \text{caseR}(l_i \Rightarrow P_i)_{i \in I} \quad \& L_k}
\]

Again, the computation rule just mirrors the cut reduction and therefore is easily seen to preserve configuration typing.

\[
\frac{(\text{caseR}(l_i \Rightarrow P_i)_{i \in I}) \mid (L.l_k ; Q)}{P_k \mid Q}
\]
**Unit as Termination.** The unit 1 just corresponds to termination. Since communication is synchronous, the paired process to the right just waits for the termination to occur.

\[
\begin{align*}
    \text{⊢ closeR : } & 1R \\
    \text{⊢ Q : } & C \\
    \text{1 ⊢ waitL ; Q : } & 1L
\end{align*}
\]

The computation rule lets the waiting process proceed while the closing one disappears.

\[
\frac{\text{closeR } | \text{ (waitL ; Q) }}{Q}
\]

This preserves types since there is no left interface to the configuration before and after the step, and the right interface \( C \) is preserved. Again, this can simply be read off from the cut reduction.

This completes the introduction of the computational interpretation of subsingleton logic. We will not discuss the computational metatheory, namely the *progress* and *preservation* theorems guarantee. Briefly, preservation here means that the configuration of process will remain well-typed during the computation, and progress that at least one process in a closed configuration can always take a step unless we are communicating and the right end of the configuration.
4 Example: Subsequential Finite State Transducers

We have already introduced FSTs in Lecture 21, where we provided an implementation using the computation-as-ordered-inference paradigm. Here, we will use the computation-as-ordered-proof-reduction paradigm instead. We begin with the example of an FST that compresses runs of $b$ into a single $b$.

We would like to represent the transducer as a process $T$ that receives the input string, symbol by symbol, from the left and sends the output string, again symbol by symbol, to the right.

$$\text{string} \vdash T : \text{string}$$

The first problem is how to represent the type $\text{string}$. It is easy to represent symbols as labels and a choice between symbols $a$, $b$, and the endmarker $\$$. As an internal choice

$$\oplus\{a : A_a, b : A_b, \$ : A_\$\} \vdash T : \text{string}$$

Clearly, $T$ can proceed with a $\oplus L$ rule, which means it can branch on whether it receives an $a$, $b$, or a $\$$. After receiving an $a$, for example, what should the type on the left be? We can receive further symbols, so it should be again string. This leads us to

$$\text{string} = \oplus\{a : \text{string}, b : \text{string}, \$ : A_\$\}$$

which is an example of a recursive type since $\text{string}$ is defined in terms of itself. What should the remaining unspecified type $A_\$ be? Once we receive
the endmarker we can receive no further symbols (or anything else) from the left, we can only wait for the process to our left (that produced the string) to terminate. So $A_8 = 1$ and we have

$$\text{string} = \oplus \{ a : \text{string}, b : \text{string}, \$: 1 \}$$

It is convenient in this setting to think of the string as being equal to the type on the right. If every type definition is contractive [GH05] in the sense that it starts with a type constructor ($\oplus, \&$, 1) then we do not need any explicit right or left rules since we can “silently” replace a type by its definition and apply the appropriate rule. This is the idea behind equirecursive treatment of recursive types. One should be worried that they could destroy all the good properties of the logic, but with some care this does not have to be the case.

Here is a simple program that produces the string babb:

$$1 \vdash [\text{babb}] : \text{string}$$

$$\llbracket \text{babb} \rrbracket = \text{R.b}; \text{R.a}; \text{R.b}; \text{R.b}; \text{R.}$;$ \leftrightarrow$$

To deal with recursive types, the program will have to be similarly recursive. At the level of proofs, this can be analyzed as circular proofs [FS13], fixed points [Bae12], or corecursive proofs [TCP14]. We will just freely use recursion. Each state of the FST becomes a process definition that captures how the FST behaves with the corresponding input. Output is handled simply by sending the appropriate label to the right, and the new state is handled by invoking this state.

$$Q_0 = \text{caseL (a ⇒ R.a ; Q_0)}$$

$$| b ⇒ R.b ; Q_1$$

$$| \$: ⇒ R.$ ; Q_f)$$

$$Q_1 = \text{caseL (a ⇒ R.a ; Q_0)}$$

$$| b ⇒ Q_1$$

$$| \$: ⇒ R.$ ; Q_f)$$

$$Q_f = \leftrightarrow$$

The type of the final state $Q_f$ is a bit different, since we know input and output have completed by the time this state is reached. We have

$$\text{string} \vdash Q_0 : \text{string}$$

$$\text{string} \vdash Q_1 : \text{string}$$

$$1 \vdash Q_f : 1$$
We also note an alternative definition for $Q_f$

$$Q_f = \text{waitL} \; ; \; \text{closeR}$$

These two definitions are equivalent in the sense that $(\text{waitL} \; ; \; \text{closeR})$ is the identity expansion of $\leftrightarrow : 1$. We will not go into detail, but this means that those two processes are observationally equivalent and can be used interchangeably [PCPT14].

At this point we could almost formulate a conjecture such as

$$\langle w \rangle \cdot Q_0\cdot \cdot \cdot \langle v \rangle$$

where $Q_0$ is the process representing the initial state of the machine that transforms input $w$ to output $v$. Before reading on, consider why this may not hold.\(^1\)

\(^1\)We did not discuss this find point regarding the operational semantics in lecture.
Yes: the problem is that when \( T \) attempts to send an output symbol to the right, there is no consumer so the process will actually block and the computation will come to a halt. There are at least two ways to solve this problem. One is to make communication *asynchronous* so that output (sending a label to the left of right) can always take place. This has two advantages: (1) it is more realistic from the implementation perspective, and (2) it increases the available parallelism.

Another solution is to create a client that will accept the expected output string. This client could be written in the form of a finite automaton, which we discuss in the next section.

## 5 Finite-State Automata

A (deterministic) finite-state automaton works almost exactly like a sub-sequential transducer, but it will output only either *acc* or *rej*, not a whole string. This is easy to model:

\[
answer = \oplus\{acc : 1, rej : 1\}
\]

It generalizes the grammar for strings by allowing two different endmarkers (instead of just \( $ \)), and has otherwise no symbols.

Then we would write

\[
\begin{align*}
\text{string} &\vdash \text{reject} : \text{answer} \\
\text{reject} &= \text{caseL} (a \Rightarrow \text{reject} | b \Rightarrow \text{reject} | $ \Rightarrow R.\text{rej} ; \leftrightarrow) \\
\text{string} &\vdash \text{accept} : \text{answer} \\
\text{accept} &= \text{caseL} (a \Rightarrow \text{accept} | b \Rightarrow \text{accept} | $ \Rightarrow R.\text{acc} ; \leftrightarrow) \\
\text{string} &\vdash bab^\rightarrow : \text{answer} \\
\downarrow bab^\rightarrow &= \text{caseL} (a \Rightarrow \text{reject} \\
&| \quad $ \Rightarrow R.\text{rej} ; \leftrightarrow \\
&| \quad b \Rightarrow \text{caseL} (b \Rightarrow \text{reject} \\
&\quad | \quad $ \Rightarrow R.\text{rej} ; \leftrightarrow \\
&\quad | \quad a \Rightarrow \text{caseL} (a \Rightarrow \text{reject} \\
&\quad \quad | \quad $ \Rightarrow R.\text{rej} ; \leftrightarrow \\
&\quad \quad | \quad b \Rightarrow \text{accept}))
\end{align*}
\]

We can then test our machine with

\[
\begin{align*}
\langle bab \rangle | Q_0 &\vdash bab^\rightarrow \\
\vdots &
\end{align*}
\]

\[
(R.\text{acc} ; \leftrightarrow)
\]
Now we can state more generally that

\[ \Gamma \vdash w \downarrow | Q_0 | \downarrow v \downarrow \]

\[ \vdash \]

\[ (R, \text{acc} ; \leftrightarrow) \]

if and only of the FST with initial state \( Q_0 \) transduces input \( w \) to output \( v \).

The proof of essentially this theorem is sketched in a recent paper [DP16].

The transitions of the transducer here are not exactly in one-to-one correspondence with the steps of proof construction, since the sequence of reading the input and writing the output are usually seen as a single step. Except for this potential minor difference regarding what counts as a step (depending on the precise formulation of the finite-state transducer), automata transitions are modeled precisely a logical inference steps.

In fact, the opposite is also true. If we have a cut-free proof

\[ \text{string} \vdash P : \text{string} \]

then \( P \) will behave like a finite state transducer. The proof is essentially by inversion: Since the proof is cut-free, \( P \) can proceed only by forwarding, receiving from the left, sending to the right, or recursing. From this we can easily construct an FST with the same behavior, again allowing for some minor discrepancies in how steps are counted.

Taken together, this means we have an isomorphism between proofs in subsingleton logic containing only \( \oplus \) and \( 1 \) and inductively defined types and subsequential finite state transducers. A recent paper [DP16] slightly generalized FSTs so that they encompass finite-state automata as well by allowing multiple distinct endmarkers, as we have done for the representation of string acceptors.

As a last remark, we notice that composition of transducers is logically trivial, namely just cut. If we have

\[ \text{string} \vdash T_1 : \text{string} \quad \text{and} \quad \text{string} \vdash T_2 : \text{string} \]

then

\[ \text{string} \vdash (T_1 \mid T_2) : \text{string} \]

Here, the two transducers will run in parallel, similarly to our earlier modeling of transducers via ordered inference. \( T_1 \) will pass its output to \( T_2 \), which will in turn pass its output to a consumer on the right. We can also just perform cut elimination to obtain a cut-free \( T' \) equivalent to \( (T_1 \mid T_2) \),
but a word of caution: in the presence of corecursive (circular) proofs, the usual cut elimination algorithms has to work somewhat differently [FS13]. Nevertheless, it is an illustration how logical tools such as cut elimination can be used in programming languages, this time in program transformation.

For example, we can write a program `flip` that turns a’s into b’s and vice versa:

```plaintext
string ⊢ flip : string
flip = caseL (a ⇒ R.b ; flip
         | b ⇒ R.a ; flip
         | $ ⇒ R.$ ; ↔)
```

Now we can write a program that compresses runs of a’s instead of b’s (renaming $Q_0$ to `compress_b` for consistency):

```plaintext
string ⊢ compress_a : string
string ⊢ compress_b : string
compress_a = flip | compress_b | flip
compress_b = Q_0
```

Note that in the process configuration

```
flip | compress_b | flip
```

the three processes will actually work concurrently, passing through the letters $a$ and $b$ in the form of a pipeline.
Exercises

Exercise 1 Write a transducer over the alphabet $a, b$ which produces $ab$ for every occurrence of $ab$ in the input and erases all other symbols.

1. Present it in the form of ordered inference rules.

2. Present it in the form of a well-typed program.

Exercise 2 Rewrite your parity-computing inference rules from Exercise L2.2 as a transducer, replacing $\text{eps}$ with the endmarker $\$$.

1. Present the transducer in the form of ordered inference rules, for reference. You may freely change your solution of Exercise L2.2 in order to prepare it for part 2.

2. Rewrite it in the form of a well-typed ordered concurrent program.

Exercise 3 Rewrite the program below as a finite state transducer, expressed as a set of ordered inference rules. Describe the function on strings that $Q_0$ computes.

\[
Q_0 = \text{caseL} (a \Rightarrow Q_1 \\
| b \Rightarrow Q_2 \\
| $ \Rightarrow R.$ ; $ \leftrightarrow )
\]

\[
Q_1 = \text{caseL} (a \Rightarrow Q_1 \\
| b \Rightarrow R.b ; Q_2 \\
| $ \Rightarrow R.$ ; $ \leftrightarrow )
\]

\[
Q_2 = \text{caseL} (a \Rightarrow R.a ; Q_1 \\
| b \Rightarrow Q_2 \\
| $ \Rightarrow R.$ ; $ \leftrightarrow )
\]

Exercise 4 Reconsider the transducers for compressing runs of $b$'s, given here as a set of ordered inference rules. We present here the version without an explicit final state.

\[
\begin{array}{c c c}
  a & q_0 & b \\
  q_0 & a & q_1 \\
  b & q_0 & \$ \\
  q_0 & a & q_1 \\
  a & q_1 & b \\
  q_1 & \$ \\
  \$ & \$ \\
\end{array}
\]
In our encoding as a program \( Q_0 \) of type \( \text{string} \vdash Q_0 : \text{string} \) we treated letters as messages and states as processes. No explicit representation of the final state is necessary with the rules above.

Define a dual encoding where symbols of the alphabet and endmarkers are represented processes and states as messages.

1. Define an appropriate type \( \text{state} \) so that \( \text{state} \vdash P_a : \text{state} \) where \( P_a \) is the process representation for the alphabet symbol \( a \).

2. For each symbol \( a \) of the transducer alphabet, define the process \( P_a \).

3. Give the type of the process \( P_\$ \) representing the endmarker \( \$ \). You may choose whether to represent a final state as an explicit message of some form or not.

4. Define the process \( P_\$ \) for the endmarker.

5. Define the initial configuration for the string \( babb \) and initial state \( q_0 \). Then describe it in general for the machine under consideration here.

6. Define the final configuration for the given example string and initial state. Then describe it in general for the machine under consideration here.

7. Do you foresee any difficulties for encoding subsequential finite state transducers in general in this style? Note that FSTs read one symbol at a time but may output any number of symbols (including none) in one transition. Describe how this could be handled, or explain why a dual construction may only work for a restricted class of FSTs.

8. Consider how to compose transducers and compare to the composition in the original encoding given in lecture.
References


[PCPT14] Jorge A. Pérez, Luís Caires, Frank Pfenning, and Bernardo Toninho. Linear logical relations and observational equivalences

