Session-Typed Concurrent Programming
Frank Pfenning
OPLSS 2019

Date Performed:	June 17th 2019
Students:	J.W.N. Paulus
	R. Gurdeep Singh
	H. C. A. Tavante

Motivation and intro

There are two ways to look at a program. From an operational standpoint and form a logical standpoint. Let us look at an example program the *presumably* gets the smallest element form *presumably* a list.
Operational reasoning: *How* a program works.

```
sort(A)
x = A[0]
```

Here `sort` *presumably* sorts the list `A` inplace. We assume here that `A` is a list because we use the `[]` operator on it to *presumably* fetch the first element of the sorted list.
Logical reasoning: *What* does the program do?

```
hd ∘ sort
```

Here we use function composition ∘ to capture that we sort the list and then take the first element. Here, `hd` is a function that takes the first element of something, and `sort` is a function that sorts its input and returns it. Note that we do not specify how `sort` or `hd` is implemented. And it from a logical reasoning point of view, we don't care.
Designing abstractions
When we design abstractions we aim to capture some computational phenomenon such that:

a. We can reason about it operationally

b. We can reason about it logically

c. (1) and (2) are coherent

1 Lecture 1: Sequent Calculus for Singleton logic

Logic is:

- The process of **deduction**
- About what you can **infer** from some axioms rather then what you know as truth.
- Wikipedia: the systematic study of the form of valid inference, and the most general laws of truth
- A rapper according to Wikipedia

1.1 Form and inference rules

A sequent has following form:

$$\underbrace{A}_{\text{Antecedent or Assumption}} \vdash \underbrace{B}_{\text{succedent}}$$

Where the antecedent contains the assumption, and succedent contains the "conclusion". In the case of the *singleton* logic, both A and B must be a singleton, i.e. exactly one antecedent and one succedent (and they should both be propositions). The $\vdash$ symbol should be read as "entails".

1.1.1 Connectors

We use the "&" for conjunction (and) and the "$\oplus$" for disjunction (simple logical or, not to be confused with exclusive or).

1.1.2 Base inference rules

The fist rule we introduce is the states that we can derive that A entails A without needing anything.

$$\frac{}{A \vdash A}\ \text{ID}_A$$

The second rule we introduce is the CUT rule. It encodes the transitivity of entailment. To derive C from A (that is $A \vdash C$) we first derive $A \vdash B$ and $B \vdash C$ and then we conclude $A \vdash C$. One could informally say that "B is a lemma".

$$\frac{A \vdash B \quad B \vdash C}{A \vdash C}\ \text{CUT}_B$$

1.1.3 Connectors.

So far the propositions in our . Let's introduce some connectors. Each

Disjunction / or operator $\oplus$ One of the most basic connectors is the "or" connector. We will write it as $\oplus$ here[1]. Its rules are:

$$\frac{A \vdash C \quad B \vdash C}{A \oplus B \vdash C}\ \oplus\text{L} \qquad \frac{A \vdash B}{A \vdash B \oplus C}\ \oplus\text{R}_1 \qquad \frac{A \vdash C}{A \vdash B \oplus C}\ \oplus\text{R}_2$$

Assume that we made a mistake when defining $\oplus$, and we used the following for $\oplus L$ instead:

$$\frac{A \vdash C}{A \oplus B \vdash C}\ \oplus\text{L?}$$

Our slight oversight allows us to make following derivation:

$$\dfrac{\dfrac{\dfrac{}{B \vdash B}\ \text{ID}_B}{B \vdash A \oplus B}\ \oplus R_2 \quad \dfrac{\dfrac{}{A \vdash A}\ \text{ID}_A}{A \oplus B \vdash A}\ \oplus L}{B \vdash A}\ \text{CUT}_{A \oplus B}$$

It states that anything is able to entail anything, which makes no sense.

With the correct rules we can prove the commutativity of $\oplus$ like this:

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\ ID_A}{A \vdash B \oplus A}\ \oplus R_2 \quad \dfrac{\dfrac{}{B \vdash B}\ ID_B}{B \vdash B \oplus A}\ \oplus R_1}{A \oplus B \vdash B \oplus A}\ \oplus L$$

Conjunction / and / with operator & The next connector we tackle is the and operator, denoted by &. Its rules are defined below.

$$\frac{A \vdash B \quad A \vdash C}{A \& B \vdash C}\ \& R \qquad \frac{A \vdash C}{A \& B \vdash C}\ \& L_1 \qquad \frac{B \vdash C}{A \& B \vdash C}\ \& L_2$$

Things we cannot have

a. Implication
   The problem with implication is that to use it, we need to allow more than one assumption in the proofs. This does not fit in our singleton logic model.

b. Negation $A \vdash \neg B$

[1] The $\oplus$ is simple or, and should not be confused with the exclusive or operator

Wise words of Pfenning:

I'm not interested in success, only in failure

I once needed to do a proof with 64 cases, you can guess which 63 I did first. The last one did not work out and I had to switch topics.

1.2 Examples of Proofs

It is typical to expect some form of distribution law between & and $\oplus$. Our goal is to prove the following

$$(A\&B) \oplus (A\&C) \vdash\dashv A\&(B \oplus C) \text{ and } (A\&B) \oplus (A\&C) \vdash\dashv A\&(B \oplus C)$$

We are only able to prove in one direction of the entailment at a time as we have no concept that $A \vdash B \Rightarrow B \vdash A$. So we will first start with $(A\&B) \oplus (A\&C) \vdash A\&(B \oplus C)$. It is sufficient to show that all branches deviation consist of axioms in order to prove this.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ID_A}{A\&B \vdash A}\,\&L_1 \quad \dfrac{\dfrac{}{A \vdash A}\,ID_A}{A\&C \vdash A}\,\&L_1}{(A\&B) \oplus (A\&C) \vdash A}\,\oplus L \quad \dfrac{\dfrac{\dfrac{}{B \vdash B}\,ID_B}{B \vdash B \oplus C}\,\oplus R_1}{A\&B \vdash B \oplus C}\,\&L_2 \quad \dfrac{\dfrac{\dfrac{}{C \vdash C}\,ID_C}{C \vdash B \oplus C}\,\oplus R_2}{A\&C \vdash B \oplus C}\,\&L_2}{(A\&B) \oplus (A\&C) \vdash B \oplus C}\,\oplus L}{(A\&B) \oplus (A\&C) \vdash A\&(B \oplus C)}\,\&R$$

Next we will attempt to prove $(A\&B) \oplus (A\&C) \dashv A\&(B \oplus C)$. Using the inference rules yields the following

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ID_A}{A\&(B \oplus C) \vdash A}\,\&L_1 \quad \dfrac{\dfrac{\dfrac{}{B \vdash B}\,ID_B \quad \dfrac{(1)}{C \vdash B}}{B \oplus C \vdash B}\,\oplus L}{A\&(B \oplus C) \vdash B}\,\&L_2}{A\&(B \oplus C) \vdash A\&B}\,\&R}{A\&(B \oplus C) \vdash\dashv (A\&B) \oplus (A\&C)}\,\oplus R_1$$

Notice however we have that for some (1) we can infer $C \vdash B$. This may lead you to believe that no inference rule can be made however that is not the case as you are always able to create some new M and perform the CUT rule.

$$\dfrac{C \vdash M \quad M \vdash B}{C \vdash B}\,CUT_M$$

now let us consider three cases. $M = C, M = B, M \neq B$ or C. In the first case we get ID_C on the left branch and exactly what we started with on the right so we are able to recursively call cut. In the second case we have the same situation however we ID_B is on the right branch. In the finally case we are able to generate a new M_1 and M_2 and call CUT on both the left and the right.
Similarly for $(A\&B) \oplus (A\&C) \vdash\dashv A\&(B \oplus C)$
We are first able to prove $(A\&B) \oplus (A\&C) \vdash A\&(B \oplus C)$ by :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ID_A}{A\&B \vdash A}\,\&L_1 \quad \dfrac{\dfrac{}{B \vdash B}\,ID_B}{B \vdash B \oplus C}\,\oplus R_1}{A\&B \vdash B \oplus C}\,\&L_2}{A\&B \vdash A\&(B \oplus C)}\,\&R \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ID_A}{A\&C \vdash A}\,\&L_1 \quad \dfrac{\dfrac{}{C \vdash C}\,ID_C}{C \vdash B \oplus C}\,\&L_2}{A\&C \vdash B \oplus C}\,\oplus L_2}{A\&C \vdash A\&(B \oplus C)}\,\&R}{(A\&B) \oplus (A\&C) \vdash A\&(B \oplus C)}\,\oplus L$$

However we run into the same problem when we try to entail $(A\&B) \oplus (A\&C) \dashv A\&(B \oplus C)$ as seen by (2)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ID_A \quad \dfrac{(2)}{A \vdash B}}{A \vdash A\&B}\,\&R \qquad B\&C \vdash A\&B}{A \oplus (B\&C) \vdash A\&B}\,\oplus L}{A \oplus (B\&C) \vdash (A\&B) \oplus (A\&C)}\,\oplus R_1$$

So what is it that we can conclude from this? We are easily able to prove what is true by applying the correct sequence of derivation rules and reaching axioms however for something that we suspect to be false we are always able to perform the cut inference rule upon it. We need some form of notation saying that if there is a derivation proving truth then we are able to write that derivation omitting the CUT rule entirely.

2 Cut-Elimination

The cut rule is not absolutely necessary. It is possible to write proof without using it. Cut-elimination helps us to show that our logic is consistent (our logic is decidable and we can test all the possibilities).
How can we eliminate a cut? For example:

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\text{ID}}{A \vdash A \oplus B}\,\oplus R_1 \qquad \dfrac{\dfrac{\dfrac{}{A \vdash A}\,\text{ID}}{A \vdash B \oplus A}\,\oplus R_2 \quad \dfrac{\dfrac{}{B \vdash B}\,\text{ID}}{B \vdash B \oplus A}\,\oplus R_1}{A \oplus B \vdash B \oplus A}\,\oplus L}{A \vdash B \oplus A}\,\text{CUT}$$

It is possible to "push up the cut". We focus on A and split the proof in two steps:
Step 1:

$$\dfrac{\dfrac{}{A \vdash A}\ \text{ID} \qquad \dfrac{\dfrac{}{A \vdash A}\ \text{ID}}{A \vdash B \oplus A}\ \oplus R_2}{A \vdash B \oplus A}$$

Step 2:

$$\dfrac{\dfrac{}{A \vdash A}\ \text{ID}}{A \vdash B \oplus A}\ \oplus R_2$$

We then introduce a new judgement to indicate that A entails B without cut:

$$A \ \triangleright \ B$$

We will then have similar left and right rules:

$$\dfrac{A \triangleright C \quad B \triangleright C}{A \oplus B \triangleright C}\ \oplus L^{\triangleright}$$

$$\dfrac{A \triangleright B}{A \triangleright B \oplus C}\ \oplus R_1^{\triangleright}$$

$$\dfrac{A \triangleright C}{A \triangleright B \oplus C}\ \oplus R_2^{\triangleright}$$

2.0.1 Proofs by induction

We shall assume all the possible cases. [TODO - complete all the possible cases; showing two]
Case 1

$$\dfrac{A \oplus B \vdash C}{A \vdash C \quad B \vdash C}$$

By inductive hypothesis (I.H.) :

$$\dfrac{A \triangleright C \qquad B \triangleright C}{A \oplus B \triangleright C}\ \oplus L^{\triangleright}$$

Case 2

$$\dfrac{A \vdash B \qquad B \vdash C}{A \vdash C}\ \text{CUT}$$

By inductive hypothesis (I.H.) :

$$\dfrac{A \triangleright B \qquad B \triangleright C}{A \triangleright C}$$

2.0.2 Lemma: Admissibility of Cut

If

$$A \triangleright B$$

and

$$B \triangleright C$$

then

$$A \triangleright C$$

Using constructive proofs, we shall come up with the proof. We shall assume all possible cases: [TODO - complete all the possible cases; showing three; 4 missing]
Case 1:

$$\dfrac{\dfrac{}{A \vdash A}\,\mathrm{ID} \qquad \mathcal{E}\;\; A \triangleright C}{A \triangleright C}\,\mathrm{cut}$$

Case 2:

$$\dfrac{\dfrac{\mathcal{D}\;\; A \triangleright B}{A \triangleright B \oplus C}\oplus R_1 \qquad \dfrac{\mathcal{E}\;\; B \triangleright D \qquad \mathcal{F}\;\; C \triangleright D}{B \oplus C \triangleright D}\oplus L^{\triangleright}}{A \triangleright D}\,\mathrm{cut}$$

Constructing:

$$\dfrac{\mathcal{D}\;\; A \triangleright B \qquad \mathcal{E}\;\; B \triangleright D}{A \triangleright D}\,\mathrm{I.H.}$$

In the cases above, either the cut disappear or we get smaller pieces in the proof.
Case 3:

$$\dfrac{\dfrac{\mathcal{D}\;\; A \triangleright D}{A\&B \triangleright D}\,\&L^{\triangleright} \qquad \mathcal{E}\;\; C \triangleright D}{A\&B \triangleright D}$$

Constructing:

$$\dfrac{\mathcal{D}\;\; A \triangleright C \qquad \mathcal{E}\;\; C \triangleright D}{\dfrac{A \triangleright D}{A\&B \triangleright D}\,\&L^{\triangleright}}$$

The case above is slightly trickier and may be referred as “simultaneous induction”.

2.1 Example 1.2 revisited

With this new cut elimination theorem we are now able to disprove $A\&(B\oplus C) \vdash (A\&B) \oplus (A\&C)$ by showing $A\&(B \oplus C) \triangleright (A\&B) \oplus (A\&C)$ is not possible. Applying inference rule gives us:

$$\dfrac{\dfrac{\dfrac{}{A \triangleright A}\, ID_A}{A\&(B \oplus C) \triangleright A}\, \&L_1 \qquad \dfrac{\dfrac{\dfrac{}{B \triangleright B}\, ID_B \qquad C \triangleright B}{B \oplus C \triangleright B}\, \oplus L}{A\&(B \oplus C) \triangleright B}\, \&L_2}{A\&(B \oplus C) \triangleright A\&B}\, \&R$$
$$\dfrac{}{A\&(B \oplus C) \triangleright \dashv (A\&B) \oplus (A\&C)}\, \oplus R_1$$

But by looking at the shape of the rules available we can see that the only rule applicable is ID and this is only the case when $C = B$ but we are considering a general C and B hence we are stuck, meaning that this isn't provable and hence not true.