# Proof Search in Propositional Linear Logic via Boolean Constraints Satisfaction

January 1, 1980

# Contents


**1 Intro** **2**
1.1 Why Prolog . . . . . 2

**2 The focused calculus** **4**
2.1 Normalization . . . . . 4
2.2 Focusing . . . . . 5
2.3 Constraints . . . . . 5

**3 Implementation** **12**
3.1 Formula transformations . . . . . 12
3.2 Helper predicates . . . . . 14
3.3 Focusing . . . . . 14
3.3.1 Asynchronous and focusing phase . . . . . 14
3.3.2 Identity rules . . . . . 15
3.3.3 Decide rules . . . . . 16
3.4 Building the tree . . . . . 17

**4 State of the art** **18**
4.1 APLL . . . . . 18
4.2 `llprover` . . . . . 19

**5 Testing** **20**
5.1 Infrastructure . . . . . 20
5.1.1 Prefix format . . . . . 21
5.1.2 File formats . . . . . 22
5.1.3 Formula generation . . . . . 22
5.2 Benchmarking . . . . . 23

# Chapter 1

# Intro

## 1.1 Why Prolog

Prolog as a language and as an environment has been historically tied to automated theorem proving for its ability to express these kind of algorithmns naturally. One particularly conventient characteristic of Prolog is its automatic management of backtracking, in most other languages we would have had to use exceptions to walk down the stack, or a queue of unfinished computations, which would have made the code much less readable.

Most Prolog implementations also support CLP or constraint logic programming. This is implemented through a series of libraries, these libraries allow to express constraint in the body of the clauses referencing some attribute of the variables; in our case we will use CLP($\mathcal{B}$)[**?**], which provides tools to deal with boolean constraints. By boolean constraint in this context we mean an expression made of Prolog variables and the constants 1 and 0, respectively true and false. The allowed operators in these expressions are the usual ones one would expect; in our case we will use exclusively conjunction, negation and equality, respectively

```
X * Y.
~ X.
X =:= Y.
```

Usually constraints will be accumualted in a list, for this reason CLP($\mathcal{B}$)provides the functor `*(L)` to express the conjunction of its members. A constraint may be checked using the predicate `sat/1`, which succeds iff the constraint is satisfiable. Since we only deal with conjunctions we define the helper predicate `check/1`

```
check(L) :-
        sat(*(L)).
```

The predicate `sat/1` may work a bit unexpectedly, to clarify its possibile outcomes we give a little example:

```
?- L = [X * Y =:= 1, X =:= 0], sat(*(L)).
false.
?- L = [X * Y =:= 0], sat(*(L)).
```

```
sat(1#X*Y).
?- L = [X * Y =:= 0, X =:= 1], sat(*(L)).
X = 1,
Y = 0.
```

Here we can see three different cases:

- the first case is unsatisfiable, so the predicate fails;
- the second case is not instantiated enough and so the constraint just gets rewritten;
- the third case shows how one constraint (`X =:= 1`) can force a variable to be unified to a value.

We use the library with the flag `clpb_monotonic` set to `true`. This make the algorithm many order of magnitude faster but mandates that all variables be wrapped by the functor `v/1`. This small explanation sums up the extent of the library we use in our prover.

One other characteristic of Prolog which revealed to be very handy for our prover is unification. Using this we didn't have to explicitly propagate the solutions of the SAT-solver, which instead were automatically propagated between branches.

# Chapter 2

# The focused calculus

## 2.1 Normalization

Since in linear logic negation is symmetric and involutive, it is usual to work only with formulae in negated normal form.

**Definition 2.1.1** (Negated Normal Form – NNF)**.** A farmula is in NNF if all its linear implications ($\multimap$) are expanded to pars ( $\parr$ ) and negation is found only at atoms. Intuitively, a sequent is in NNF if all its formulae are in NNF.

A generic formula is then normalized applying recursively the DeMorgan rules for linear logic, untill NNF is reached. The process of normalization takes a two-sided judgement, of the form

$$\Delta \vdash \Gamma$$

and transforms it into a one-sided judgement

$$\vdash \Delta'$$

where the right side is composed of the normalization of $\Gamma$ and $\Delta^{\perp}$.

This choice has some implementation-wise advantages, but for now we will only care about the fact that it shrinks the size of the complete calulus by roughly half since we only have to deal with the right rules of the connectives.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $\phi$ | $::=$ | $1$ | $\mid$ | $\phi \otimes \phi$ | $\mid$ | $\perp$ | $\mid$ | $\phi \parr \phi$ | (Multiplicatives and their constants) |
| | $\mid$ | $0$ | $\mid$ | $\phi \oplus \phi$ | $\mid$ | $\top$ | $\mid$ | $\phi \,\&\, \phi$ | (Additives and their constants) |
| | $\mid$ | $!\phi$ | $\mid$ | $?\phi$ | | | | | (Exponentials) |
| | $\mid$ | $\alpha^{\perp}$ | $\mid$ | $\alpha$ | | | | | (Where $\alpha$ is a term) |

Figure 2.1: Normalized linear logic formulae

As seen in Figure 2.1 we will use $\phi$ for formulae and $\alpha$ for terms.

## 2.2 Focusing

Focusing is a technique described by Andreoli in his seminal paper [**?**]. There he recognizes two alternating phases in a proof: a deterministic phase, where the order of rule application to the sequent does not matter; and a non deterministic phase, where several choices may be tried. These two phases are respectively called asynchronous and synchronous phase.

**Definition 2.2.1.** Given a formula $\phi$ we define the following predicates: "$\phi$ asy" indicates that the rule for the toplevel connective of the formula $\phi$ is asynchronous on the right, these connectives are

$$⅋, \&, ?, \top, \bot$$

conversely we define "$\phi$ sync" to indicate that the rule for the toplevel connective of $\phi$ is synchronous on the right, these are

$$\otimes, \oplus, !, 1$$

Furthermore in focusing everything is assigned a polarity of positive or negative. Synchronous connectives are defined to have a positive polarity, whereas asynchronous connectives are define to have a negative polarity. Terms also have a polarity, which may be assigned with some arbitrarly complex mechanisms. We will follow [**?**] and simply assing atoms with a negative polarity and negated atoms with a positive one.

**Definition 2.2.2.** "$\alpha$ neg lit" is a predicate that is true only when $\alpha$ is a negative literal (i.e. an atom). Conversely "$\alpha$ pos lit" is a predicate that is only when $\alpha$ is a positive literal (i.e. a negated atom).

## 2.3 Constraints

Our calculus uses constraints to manage the resources.

**Definition 2.3.1** (Variables, expressions)**.** A boolean variable is simply a symbol to which one can associate a value of true or false. A boolean expression, in our case, is just a conjunction of possibly negated boolean variables.

**Definition 2.3.2** (New variables)**.** Sometimes we will write

$$x \text{ new}, X \text{ new}$$

These mean respectively that:

- the variable name $x$ has not yet occurred in any expression in the proof tree, i.e. does not appear in any constraint of the father, or of its (the father) siblings and their subtrees.
- each variable name $x_i, x_j \in X$ has not yet occurred in the proof and each variable in $X$ is distinct.

$$\forall i, j \mid i \neq j \Rightarrow x_i \neq x_j$$

$$
\begin{array}{rcll}
x & ::= & x_i \quad | \quad \overline{x_i} & \text{(Variable)} \\
e & ::= & x \wedge e \quad | \quad x & \text{(Expression)}
\end{array}
$$

Figure 2.2: Definition of a boolean variable and expression

As seen in Figure 2.2 we will call $e$ such a conjuction and $x$ the single boolean variables.

**Definition 2.3.3** (Annotated formula)**.** Given a formula $\phi$ defined as in Figure 2.1 and a boolean expression $e$ defined as in Definition 2.3.1, an *annotated formula* is simply a term

$$\mathrm{af}(\phi, e)$$

that associates the formula to the expression. We denote

$$\exp(\mathrm{af}(\phi, e)) = e$$

as the operation of extracting the boolean expression associated to a given formula, and then extend this notation to sequents such that $\exp(\Delta)$ is the set of all boolean expressions of $\Delta$.

It is important to note that only the topmost connective gets annotated, and not the subformulae.
The purpose of putting formulae and expressions together in the annotated formula is twofold:

- the actions taken on the formula determine the constraints that will be generated, and these depend on the variables associated to said formula;
- after the constraints are solved we can query the assignement of the variables and find out if the associated formula is used or not in a certain branch of a proof.

These constraints may be only of two kinds: "$e$ avail" and "$e$ used".

**Definition 2.3.4** (Constraints)**.** Given an annotated formula $\mathrm{af}(\phi, e)$ as in Definition 2.3.3, a constraint may be of two kinds

- "$e$ used" states that the formula $\phi$ gets consumed in this branch of the proof. This corresponds to saying the expression $e$ is true or

$$x_i \wedge \cdots \wedge x_j = \top$$

- "$e$ avail" states that the formula $\phi$ does not get consumed in this branch of the proof, and thus is available to be used in another branch. This corresponds to saying the expression $e$ is not true or

$$x_i \wedge \cdots \wedge x_j = \bot$$

We then extend these predicates to sequents

$$\Delta \text{ used} = \{e_2 \text{ used} \mid e_2 \in \exp(\Delta)\}$$
$$\Delta \text{ avail} = \{e_2 \text{ avail} \mid e_2 \in \exp(\Delta)\}$$

A branch is then considered as correct if its constraints are satisfiable. Otherwise the branch of the proof fails.

**Definition 2.3.5** (Satisfaiability of constraints)**.** Given a set of constraints $\Lambda$ and a function V

$$\mathrm{V} : \{x_1, x_2, \ldots, x_n\} \to \{\top, \bot\}$$

mapping variables to their value, such that

$$\Lambda = \{\ldots, e_i \text{ used}, e_j \text{ avail}, \ldots\}$$
$$\mathrm{V} = \{\ldots, (x_i, \top), (x_j, \bot), \ldots\}$$

we write $\Lambda{\downarrow}\mathrm{V}$ if

$$\bigwedge_{e \in \Lambda} e[x_1/\mathrm{V}(x_1), x_2/\mathrm{V}(x_2), \ldots, x_n/\mathrm{V}(x_n)] = \top$$

Here we are using the translation given in Definition 2.3.4 such that

$$e \text{ used} \Leftrightarrow e = \top$$
$$e \text{ avail} \Leftrightarrow e = \bot$$

It is worth noting that simply by rewriting the function V to

$$\mathrm{V} = \{\ldots, x_i = \top, x_j = \bot, \ldots\}$$

we get back a set of constraints.

We now expand the concept of triadic sequent of [**?**] by adding constraints

**Definition 2.3.6** (Members of the sequent)**.** Given any sequent this can be in either two forms:

- focused or in the synchronous phase, written:

$$\vdash \Psi : \Delta \Downarrow \phi \parallel \Lambda : \mathrm{V}$$

- in the asynchronous phase, written:

$$\vdash \Psi : \Delta \Uparrow \Phi \parallel \Lambda : \mathrm{V}$$

Where

- $\Psi$ is a set of unrestricted formulae, or all formulae that can be freely discarded or duplicated;

- $\Delta$ and $\Phi$ are multisets of linear (annotated) formulae, these are respectively the formulas "put to the side" and the formulae which are being "worked on" during a certain moment of the asynchronous phase;
- $\Lambda$ and V are the constraints and the solution as defined in Definition 2.3.5. By adding these members we make the flow of constraints through the proof tree explicit, leaving no ambiguity to where the constraints should be checked. This approach to constraints differs from the one in [**?**], which, on the other hand, preferred to keep generality. The choice of letters is mainly a mnemonic or visual one, constraints $\Lambda$ "go-up" the proof tree and solutions V "come down" from the leaves.

As explained in Definition 2.3.5, V may be used as a set of constraint itself; this states that a certain solution must be respected in a new one.

**Definition 2.3.7** (Splitting)**.** Given a sequent of annotated formulae $\Delta$ and a set of variables $X$ such that $|\Delta| = |X|$ we define the operation of splitting it as a function

$$\text{split}(\Delta, X) \mapsto (\Delta_L, \Delta_R)$$

where

$$\Delta_L = \{\text{af}(\phi_i, x_i \wedge e_i) \mid i \in \{1, \dots, n\}\}$$
$$\Delta_R = \{\text{af}(\phi_i, \overline{x_i} \wedge e_i) \mid i \in \{1, \dots, n\}\}$$

with $n$ the cardinality of $\Delta$, and $\phi_i$ (resp. $e_i$) the formula (resp. the expression) of the $i$-eth annotated formula in $\Delta$ using an arbitrary order. The same holds for $x_i$ and $X$.
With a slight abuse of notation we will write $\Delta_L^X$ and $\Delta_R^X$ respectively as the left projection and the right projection of the pair $(\Delta_L, \Delta_R)$.

As a small example for clarity, given the sequent

$$\Delta = \text{af}(a \otimes b, x_1), \text{af}(c^\perp, x_2)$$
$$X = \{x_3, x_4\}$$

this is split into

$$\Delta_L^X \mapsto \text{af}(a \otimes b, x_3 \wedge x_1), \text{af}(c^\perp, x_4 \wedge x_2)$$
$$\Delta_R^X \mapsto \text{af}(a \otimes b, \overline{x_3} \wedge x_1), \text{af}(c^\perp, \overline{x_4} \wedge x_2)$$

We are now ready to present the full calculus.

$$[\,\parr\,]\ \frac{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1, e), \mathrm{af}(\phi_2, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1 \parr \phi_2, e), \Phi \parallel \Lambda : \mathrm{V}}$$

$$[\bot]\ \frac{\vdash \Psi : \Delta \Uparrow \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\bot, e), \Phi \parallel \Lambda : \mathrm{V}} \qquad [\top]\ \frac{}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\top, -), \Phi \parallel \Lambda : \mathrm{V}}$$

$$[\,\&\,]\ \frac{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_2, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}' \qquad \vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}''}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1 \,\&\, \phi_2, e), \Phi \parallel \Lambda : \mathrm{V}', \mathrm{V}''}$$

$$[\,?\,]\ \frac{\vdash \Psi, \phi : \Delta \Uparrow \Phi \parallel \Lambda : \mathrm{V}}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(?\phi, -), \Phi \parallel \Lambda : \mathrm{V}}$$

$$[R\Uparrow]\ \frac{\neg\phi \text{ asy} \qquad \vdash \Psi : \Delta, \mathrm{af}(\phi, e) \Uparrow \Phi \parallel \Lambda : \mathrm{V}}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi, e), \Phi \parallel \Lambda : \mathrm{V}}$$

(a) Asynchronous rules

$$[\otimes]\ \frac{X \text{ new} \quad \vdash \Psi : \Delta_L^X \Downarrow \mathrm{af}(\phi_1, e) \parallel \Lambda, e \text{ used} : \mathrm{V}' \quad \vdash \Psi : \Delta_R^X \Downarrow \mathrm{af}(\phi_2, e) \parallel \mathrm{V}' : \mathrm{V}''}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1 \otimes \phi_2, e) \parallel \Lambda : \mathrm{V}''}$$

$$[\oplus_L]\ \frac{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1, e) \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1 \oplus \phi_2, e) \parallel \Lambda : \mathrm{V}} \qquad [\oplus_R]\ \frac{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_2, e) \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1 \oplus \phi_2, e) \parallel \Lambda : \mathrm{V}}$$

$$[1]\ \frac{\Lambda, e_1 \text{ used}, \Delta \text{ avail}{\downarrow}\mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(1, e_1) \parallel \Lambda : \mathrm{V}} \qquad [!]\ \frac{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi, e_1) \parallel \Lambda, e_1 \text{ used}, \Delta \text{ avail} : \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(!\phi, e_1) \parallel \Lambda : \mathrm{V}}$$

$$[R\Downarrow]\ \frac{\phi \text{ asy} \vee \phi \text{ neg lit} \qquad \vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi, e) \parallel \Lambda : \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi, e) \parallel \Lambda : \mathrm{V}}$$

(b) Synchronous rules

$$[I_1]\ \frac{\Lambda, e_1 \text{ used}, e_2 \text{ used}, \Delta \text{ avail}{\downarrow}\mathrm{V}}{\vdash \Psi : \Delta, \mathrm{af}(\phi, e_2) \Downarrow \mathrm{af}(\phi^{\perp}, e_1) \parallel \Lambda : \mathrm{V}} \qquad [D_1]\ \frac{\phi \text{ pos lit} \qquad \vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi, e) \parallel \Lambda : \mathrm{V}}{\vdash \Psi : \Delta, \mathrm{af}(\phi, e) \Uparrow . \parallel \Lambda : \mathrm{V}}$$

$$[I_2]\ \frac{\Lambda, e_1 \text{ used}, \Delta \text{ avail}{\downarrow}\mathrm{V}}{\vdash \Psi, \phi : \Delta \Downarrow \mathrm{af}(\phi^{\perp}, e_1) \parallel \Lambda : \mathrm{V}} \qquad [D_2]\ \frac{\phi \text{ pos lit} \qquad x \text{ new} \qquad \vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi, x) \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi, \phi : \Delta \Uparrow . \parallel \Lambda : \mathrm{V}}$$

(c) Identity and decide rules

Figure 2.3: Focused constraint calculus for Linear Logic

What is described in Figure 2.3 is roughly the "lazy" strategy described by [**?**].

**Definition 2.3.8.** Given an assignment V, we define

$$e[\mathrm{V}] = e[x_i/V(x_i), \ldots, x_j/V(x_j)]$$

as the value of the $e$ using assignment V. We then extend this notation to sequents, such that

$$\Delta[\mathrm{V}] = \{\phi \in \Delta \mid e[\mathrm{V}] = \top\}$$

We show now a translation from our focused method to the one of [**?**]:

**Theorem 2.3.1.** *Let* $\vdash \Psi$ *The calculus of Figure 2.3 is sound*

*Proof.* Let $<$ be weakening and $>$ contraction. We proceed with the base cases

$I_1$: Given a judgment

$$[I_1]\ \frac{\Lambda, e_1 \text{ used}, e_2 \text{ used}, \Delta \text{ avail}\downarrow \mathrm{V}}{\vdash \Psi : \Delta, \mathrm{af}(\phi, e_2) \Downarrow \mathrm{af}(\phi^{\perp}, e_1) \parallel \Lambda : \mathrm{V}}$$

We get that

$$(\Delta, \mathrm{af}(\phi, e_2), \mathrm{af}(\phi^{\perp}, e_1))[V] \mapsto \phi, \phi^{\perp}$$

$$[<*]\ \frac{[I]\ \dfrac{}{\vdash \phi, \phi^{\perp}}}{\vdash ?\Psi, \phi, \phi^{\perp}}$$

$I_2$:

$$[I_2]\ \frac{\Lambda, e_1 \text{ used}, \Delta \text{ avail}\downarrow \mathrm{V}}{\vdash \Psi, \phi : \Delta \Downarrow \mathrm{af}(\phi^{\perp}, e_1) \parallel \Lambda : \mathrm{V}}$$

Again by substituting the variables we get that

$$[?]\ \frac{[<*]\ \dfrac{[I]\ \dfrac{}{\vdash \phi, \phi^{\perp}}}{\vdash ?\Psi, \phi, \phi^{\perp}}}{\vdash ?\Psi, ?\phi, \phi^{\perp}}$$

1:

$$[1]\ \frac{\Lambda, e_1 \text{ used}, \Delta \text{ avail}\downarrow \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(1, e_1) \parallel \Lambda : \mathrm{V}}$$

This uses the same reasoning as above:

$$[<*]\ \frac{[1]\ \dfrac{}{\vdash 1}}{\vdash ?\Psi, 1}$$

Assuming the premises hold we now proceed with the induction sted:

$\otimes$:

$$[\otimes]\ \frac{X \text{ new} \quad \vdash \Psi : \Delta_L^X \Downarrow \mathrm{af}(\phi_1, e) \parallel \Lambda, e \text{ used} : \mathrm{V}' \quad \vdash \Psi : \Delta_R^X \Downarrow \mathrm{af}(\phi_2, e) \parallel \mathrm{V}' : \mathrm{V}''}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1 \otimes \phi_2, e) \parallel \Lambda : \mathrm{V}''}$$

By inductive hypothesis both

$$\vdash \Psi : \Delta_L^X \Downarrow \mathrm{af}(\phi_1, e) \parallel \Lambda, e \text{ used} : \mathrm{V}'$$
$$\vdash \Psi : \Delta_R^X \Downarrow \mathrm{af}(\phi_2, e) \parallel \mathrm{V}' : \mathrm{V}''$$

hold. Now the set of all the variables referenced in the conclusion must be a subset of the sets of the variables of the branches, since a branch can only add new variables. Furthermore, given how the variables are defined, $\Delta_L^X[\mathrm{V}']$ and $\Delta_R^X[\mathrm{V}'']$ must be disjoint. Given this we get that this equals to

$$[>*]\ \frac{[\otimes]\ \dfrac{\vdash ?\Psi, \Delta', \phi_1 \qquad \vdash ?\Psi, \Delta'', \phi_2}{\vdash ?\Psi, ?\Psi, \Delta', \Delta'', \phi_1 \otimes \phi_2}}{\vdash ?\Psi, \Delta', \Delta'', \phi_1 \otimes \phi_2}$$

$\bot$:

$\top$:

$\parr$:

$$[\,\parr\,]\,\frac{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1, e), \mathrm{af}(\phi_2, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1 \parr \phi_2, e), \Phi \parallel \Lambda : \mathrm{V}}$$

Assuming the hypotesis holds

$$\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1, e), \mathrm{af}(\phi_2, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}$$

We trivially can

$$[\,\parr\,]\,\frac{\vdash ?\Psi, \Delta, \phi_1, \phi_2}{\vdash ?\Psi, \Delta, \phi_1 \parr \phi_2}$$

$\oplus_L$:

$$[\oplus_L]\,\frac{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1, e) \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1 \oplus \phi_2, e) \parallel \Lambda : \mathrm{V}}$$

$$[\oplus_L]\,\frac{\vdash ?\Psi, \Delta, \phi_1}{\vdash ?\Psi, \Delta, \phi_1 \oplus \phi_2}$$

$\oplus_R$:

$$[\oplus_R]\,\frac{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_2, e) \parallel \Lambda, e \text{ used} : \mathrm{V}}{\vdash \Psi : \Delta \Downarrow \mathrm{af}(\phi_1 \oplus \phi_2, e) \parallel \Lambda : \mathrm{V}}$$

$$[\oplus_R]\,\frac{\vdash ?\Psi, \Delta, \phi_2}{\vdash ?\Psi, \Delta, \phi_1 \oplus \phi_2}$$

$\&$ :

$$[\,\&\,]\,\frac{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_2, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}' \qquad \vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1, e), \Phi \parallel \Lambda, e \text{ used} : \mathrm{V}''}{\vdash \Psi : \Delta \Uparrow \mathrm{af}(\phi_1 \,\&\, \phi_2, e), \Phi \parallel \Lambda : \mathrm{V}', \mathrm{V}''}$$

$$[\,\&\,]\,\frac{\vdash ?\Psi, \Delta, \phi_1 \qquad \vdash ?\Psi, \Delta, \phi_2}{\vdash ?\Psi, \Delta, \phi_1 \,\&\, \phi_2}$$

!:

?:

$R\Downarrow$:

$R\Uparrow$:

$D_1$:

$D_2$:

■

# Chapter 3

# Implementation

We now describe the main implementation details of the prover. When explaining the code we will use some common names for variables, these are

- `A` is a set (`ordset`) of unrestricted atoms;
- `U` is a set (`ordset`) of unrestriched formulae;
- `F`, `F1`, ..., are formulae, and `Fs` and `D` are a lists of them;
- `S` is the queue of currently usable unrestricted formulae;
- `In` is a list of constraints.

## 3.1 Formula transformations

Before beginning the proof a sequent passes through a number of transformations. These transformations both preprocess the sequent to a more convenient form, and also add information about the subformulae.

As a first transformation the sequent gets normalized into a sequent in negated normal form (NNF). NNF is the form where all negations are pushed down to atoms and all linear implications ($\multimap$) are expanded into pars ( $\parr$ ) using the following tautology

$$a \multimap b \Leftrightarrow a^{\perp} \parr b$$

Normalization is a common technique – used in all the provers we compare with. The process is composed of just two steps

1. the left sequent is negated and appended to the right sequent, implemented by the predicate `negate_premises/3`;
2. the predicate `nnf/2`, which encodes the DeMorgan rules, is mapped recursively over the new sequent

This is possible since classic linear logic is symmetric and negation is involutive.

The purpose of this process is to cut away a great deal of possible rules applicable to the sequent, sacrificing some of the structure of the sequent. In fact the number

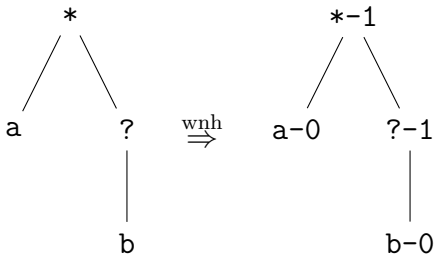
of rules we need to implement after normalization is more than halved, since we now need just the right rules, without the ones for negation and linear implication.

As a second transformation, to each formula we assign its why-not height, a measure borrowed from APLL's implemetation.

**Definition 3.1.1** (Why-not height)**.** Why-not height is the maximum number of nested "why-not"s in a formula, or

$$\mathrm{wnh}(\phi) = \begin{cases} 0 & \text{if } \phi \in \{\bot, \top, 1, 0\} \\ \max(\mathrm{wnh}(\phi_1), \mathrm{wnh}(\phi_2)) & \text{if } \phi \in \{\phi_1 \otimes \phi_2, \phi_1 \parr \phi_2, \phi_1 \oplus \phi_2, \phi_1 \,\&\, \phi_2\} \\ \mathrm{wnh}(\phi_1) & \text{if } \phi \in \{\phi_1{}^{\bot}, !\phi_1\} \\ 1 + \mathrm{wnh}(\phi_1) & \text{if } \phi \in \{?\phi_1\} \end{cases}$$

The purpose of this attribute is to guide the prover to the reasonably simpler choice – the one with the least nested exponentials – at different times during proof search. This will be seen in Section 3.3. After this transformation formulae are attribute trees, with at each node the why-not height of the subformula. For example the formula `*(a, ?(b))` becomes `*(a-0, ?(b-0)-1)-1`, or – as trees –




As a third and final transformation, each formula gets annotated. This means we associate a variable to each formula in the sequent as in Definition 2.3.3. Given a sequent $\Delta$ we obtain

$$\hat{\Delta} = \{\mathrm{af}(\phi, x) \mid x \text{ new}, \phi \in \Delta\}$$

To be clear, a variable is only assigned to the "top-level" formula, and subformulae are left unchanged.

In the implementation the concept of variable is split in two: the name of the variable – represented by a Prolog atom, and the value of the variable – represented by a Prolog variable. This is needed since, after checking the constraints, the SAT-solver unifies the variable to its value if it finds a satisfaiable solution, so the purpose of the atom is to associate the variable value to its name if the final proof. The process of annotation is implemented by the predicate `annotate/3`

```
%! annotate(+[Formulae], -[AFs], -[Constraints]) is det.
annotate(Fs, Afs, Cns) :-
  maplist([ F
          , af(F, X, Var)
          , v(Var) =:= 1
          ]>>(gensym(x, X)), Fs, Afs, Cns).
```

which is a simple map over the sequent. The constraints returned state that each formula must have its variable to one, that is to say each formulae must be used. These are the constraints the proof search starts with.

## 3.2 Helper predicates

We now define some helper predicates to work with the constraints. What we defined as $\Delta$ avail in Definition 2.3.4 corresponds to the predicate `set_to_zero/2`.

The other helper predicate implements the split function defined in Definition 2.3.7.

```
%! split_ctx(+[AFs], -[AFs], -[AFs], -[Cns], -[Cns]) is det.
split_ctx(Afs, Pos, Neg, PCns, NCns) :-
  maplist([ af(F, N, E)
          , af(F, VarPos, Y)
            , af(F, VarNeg, Z)
            , v(Y) =:= v(X) * v(E)
            , v(Z) =:= (~ v(X)) * v(E)
            ]>>(
              gensym(x, V),
              atomic_list_concat([N, V], '.', VarPos),
              atomic_list_concat([N, V], '.~', VarNeg)
  ), Afs, Pos, Neg, PCns, NCns).
```

It is again a map over the list of formulae, that generates the new formulae and the constraints accordingly. Three new Prolog variables are introduced: `X`, `Y` and `Z`. `X` is the new variable, the annotated formulae refer to the variable `Y` and `Z`, and constraints are added so that

$$y = x \wedge e$$
$$y = \overline{x} \wedge e$$

Compare this to the original definition of Definition 2.3.7, one can see that the two are basically identical other than the fact that here the name of the variable (the atom) and its value are treated separately.

## 3.3 Focusing

### 3.3.1 Asynchronous and focusing phase

During the asynchronous phase we have a list of formulae which are being worked on and a list of formulae which are put to the side; with the former being called `Fs` and the latter `D`. At each step we analyze the first element of the list `Fs`, and we keep scomposing the memebers of the list untill we cannot anymore. This process can be seen for example in the predicate for &

```
async(A, U, D, [F|Fs], S, M, In, _) :-
  F = af(((F1-H1) & (F2-H2))-_), N, E), !,
  ( H2 > H1
  -> async(A, U, D, [af((F1-H1), N, E)|Fs], S, M, [v(E) =:= 1|In], _),
     async(A, U, D, [af((F2-H2), N, E)|Fs], S, M, [v(E) =:= 1|In], _)
  ;  async(A, U, D, [af((F2-H2), N, E)|Fs], S, M, [v(E) =:= 1|In], _),
     async(A, U, D, [af((F1-H1), N, E)|Fs], S, M, [v(E) =:= 1|In], _)
  ).
```

Here we can see both the choice being made based on the why-not height of the two subformulae, and how the with is scomposed. Compare this with the & rule in Figure 2.3. The cut at line 2 represents the main concept of the asynchronous phase: if an asynchronous connective is encountered the only thing we ought to do is to scompose it.

If a formula cannot be further be broken apart – i.e. it is either an atom, a negated atom, or it has a toplevel synchronous connective – then it is put to the side in `D`. This can be seen in the rule `to_delta` which implements the rule $R\Uparrow$

```
async(A, U, D, [F|Fs], S, M, In, _) :-
  F = af((F1-_), _, _),
  not(is_asy(F1)), !,
  async(A, U, [F|D], Fs, S, M, In, _).
```

This process goes as long as `Fs` has still formulae inside.

When `Fs` is empty the phase switches, and the focusing process begins: we choose a formula – called `decide` – from either `D` or `U` and we scompose it untill either an asynchronous connective is left or a negated atom. This is represented by the rules $D_1$ and $D_2$ that will be discussed further ahead in Section 3.3.3.

### 3.3.2 Identity rules

This process of alternating asynchronous and synchronous phases in classic focusing goes on untill we have a only positive literal (in our case a negated atom) in `Fs` and the corresponding negative literal (in our case just an atom) in either `U` or `D`. When this happens the axioms – rules $I_1$ or $I_2$ – are applied to close the branch. In our case when we are focusing and we have a positive literal in `Fs`, we check if the corresponding negative literal exists in `D`. If this is true, then the variables of all the other formulae in `D` are set to zero using the predicate `set_to_zero/2` defined in Section 3.2, and the constraints are checked. This is encoded in the clause

```
focus(A, U, D, F, _, _, In) :-
  F = af(((~ T)-_), _, E1),
  is_term(T),
  select(af((T-_), _, E2), D, D1),
  set_to_zero(D1, Dz),
  append([v(E1) =:= 1, v(E2) =:= 1|Dz], In, Cns),
  check(Cns).
```

A slightly different process happens if instead a correspondence is found in `A` instead of `D`. Here `A` is a special set containing just unrestricted atoms. This is a small modification to APLL's approach based on the fact that once negative literals are put in a sequent they can never leave it, and is due to the fact that since `U` may be sorted many times, we try to keep the number of formulae in it small.

Some care is to be given to explaining how the constraints propagate. In fact, in constrast to Figure 2.3 the implementation does not have explicit propagation of the solution of the constraints. This is because Prolog's unification implicitly propagates a solution from one branch to another.

### 3.3.3 Decide rules

For the decide rules, particularly for $D_2$, we use a modified version of APLL's algorithm defined in Section 4.1. The method consists of not using directly the set $\Psi$ in the $D_2$ rule, but instead we keep a queue of ordered unrestricted formulae which can be refilled only a certain number of times per-branch. This can be seen in the definition of the rule `decide_2`

```
async(A, U, D, [], [H|T], M, In) :-
  \+ U = [],
  gensym(x, X),
  focus(A, U, D, af(H, X, E), T, M, [v(E) =:= 1|In]).
async(A, U, D, [], [_|T], M, In) :-
  \+ U = [],
  async(A, U, D, [], T, M, In).
async(A, U, D, [], [], M, In) :-
  \+ U = [],
  refill(U, M, S, M1),
  early_stop(A, U, D, S, M1, In).
```

Here the fifth argument is the queue and the sixth is the bound. Two cases arise:

- if `S = []` and `M > 0` then the sequent of unrestricted formulae `U` is taken and it is sorted based on why-not height. This can be seen in the predicate `refill/4`

  ```
  refill(U, M, S, M1) :-
          \+ M = 0,
          \+ U = [],
          sort(2, @=<, U, S),
          M1 is M - 1.
  ```

  Line 4 is a sort in increasing order on the second attribute (the why-not height), keeping duplicates. This new list of unrestricted formule becomes the new `S` and `M` is decreased. Otherwise if if `M` is 0 (line 2) the branch fails.

- if `S` is not empty, then the first formula in the queue is extracted and added to the working set. If the branch fails the formula gets discarded and the next one in the queue is tried.

In particular, if the queue `S` is refilled, we do not directly call `async/8`, but instead call another predicate: `early_stop/7` (line 11).

```
early_stop(_, _, _, [], _, _) :-
  false.
early_stop(A, U, D, [H|T], M, In) :-
  gensym(x, X),
  focus(A, U, D, af(H, X, E), T, M, [v(E) =:= 1|In]).
early_stop(A, U, D, [_|T], M, In) :-
  early_stop(A, U, D, T, M, In).
```

This is due the simple fact that if the branch was not provable and we instead called directly `async/8` at line 11, we would try to refill the branch `M` times. What `early_stop/7` does is fail if the queue has just been refilled and it turns out the branch was not provable.

All the rules $D_1$, $I_1$ are defined before the unrestricted counterparts, so that they are tried first.

## 3.4 Building the tree

In the listings above we omitted one parameter of the predicates, which purpose is to build the proof tree. At each call of async and focus one node of the proof tree is built. This contains the context of the call. For example in

```
async(A, U, D, [F|Fs], S, M, In, node(par, A, U, D, [F|Fs], [Tree])) :-
  F = af(((F1 / F2)-_), N, E), !,
  Fs1 = [af(F1, N, E), af(F2, N, E)|Fs],
  async(A, U, D, Fs1, S, M, [v(E) =:= 1|In], Tree).
```

we can see clearly the structure of the node: a label, the context and an – optionally empty – list of subtrees. A leaf is just a node with an empty list of subtrees.

This tree can be used in the end to reconstruct the actual proof tree by visiting it and – for each formula of each node – querying whether its variable is set to one, deleting it otherwise. A classic proof tree without the focusing infrastructure may be built by removing all the nodes regarding the phases (i.e. $R\Downarrow$ $R\Uparrow$ and decide rules) and by appending the sequents together as explained in **??**. A more sophisticated algorithm may even cancel out unwanted unrestricted formulae, that otherwise remain lingering in the sequent.

# Chapter 4

# State of the art

Most forward provers for classic linear logic use some combination of focusing and normalization to structure their proofs, with the notable exception of llprover not using normalization. We confront our prover with two other provers: llprover (1997, ) and APLL (circa 2019, ).

Usually the splitting is handled in two ways: trying every partition possible, or using something called the method of input/output . The latter tries to do one branch of the proof of a multiplicative, and then feeds the remaining formulae in the sequent of the other branch.

We now give a deeper look at the provers we confront with.

## 4.1 APLL

APLL is the underlying prover of click&collect. It provides 4 different searches – forward and backwards for classic and intuitionistic linear logic. We will focus on the backwards algorithm for classic linear logic.

The program is written in OCaML and implements a standard focused proof search on normalized formulae as seen in [**?**]. In this section we will illustrate two noteworthy charateristics of its implementation:

- Sequent splitting when encountering a tensor is done by generating all the numbers up to $2^{|\Delta|}$ – where $\Delta$ is the sequent – and using the bit representation of those to create the two subsets. This can be seen in the function `split_list`, which in turn calls `split_list_aux`

  ```
  let rec split_list_aux (acc1, acc2) l k = match l with
    | [] -> acc1, acc2
    | hd :: tl ->
        if k mod 2 = 0
        then split_list_aux (acc1, hd :: acc2) tl (k / 2)
        else split_list_aux (hd :: acc1, acc2) tl (k / 2)
  ```

  where the argument `k` is the number that determines the decomposition of the sequent. This function is called recursively when a tensor is encountered during proof search, starting at $k = 2^{|\Delta|}$ and decreasing by one at each iteration

```
(* ... *)
| Tensor (g, h) ->
  let rec split_gamma k =
    if k = -1 then None
    else
      let gamma1, gamma2 = split_list gamma k in
        try
          (* ... *)
        with NoValue ->
          split_gamma (k - 1)
  in
    let k = fast_exp_2 (List.length gamma) - 1 in
      (* ... *)
```

As we will see in 5.2 this implementation choice will result in a degradation of performance on formulae with a high number of multiplicatives.

## 4.2 `llprover`

`llprover` is a prover by Naoyuki Tamura. Where APLL had different provers for implicative and classical linear logic, this prover encodes all the rules as the same predicate `rule/6`, using the first argument as a selector for the system. Using classical logic as the system uses all the rules, included the ones for implicative linear logic. For this reason the prover does not implement normalization.

Another particular characteristic of llprover is that it uses a local bound with iterative deepening, so in the benchmarks for formulae which need a lot of contractions, it will perform slightly worse.

# Chapter 5

# Testing

!!! VERY MUCH STILL WIP !!!

## 5.1 Infrastructure

The infrastructure for the project is divided in two parts:

- the nix "glue"
- python utilities to call and confront provers

In nix everything must be packaged as a derivation, so derivations are written for all the programs we interact with:

- the provers, such as APLL or llprover
- the formula generator adapted from APLL described in Section 5.1.3
- the LLTP parser

All these derivations, together with a derivation for the python environment, are then used to define a single development environment to run the jupyter notebook with all the necessary dependencies. Furthermore having used "flakes" – a nix experimental feature – all dependencies are locked to a certain commit, thus ensuring better reproducibility.

The main logic for the benchmarking is define in the python module `testprover.py`. Here for simplicity we assume that a prover returns a code of 0 if it found a solution to a sequent, or any other number otherwise. This condition is already met by our prover and by llprover; for APLL instead a wrapper is provided.

Defining the call to our prover using this library is as simple as writing

```
pc = Registered()

@pc.register('sat-ll')
@call_prover(PrefixTree.SAT_LL_DICT)
def call_sat_prover(premises, conclusions):
        return [ 'sat-ll'
```

```
, '-b', '3'
, f'{premises} |- {conclusions}'
]
```

The innermost decorator (line 3) accepts a dictionary, and is needed to auomatically call the prover with a test entry (as in Section 5.1.2), time it and eventually terminate the process it if the time runs out. The outermost decorator (line 4) instead simply adds an entry `sat-ll` associated with the prover call to the register `pc`. This register is just an association name to function, and it is what is actually passed to the benchmarking function.
The library then provides two functions

- the function `testall` accepts a single prover and a test suite and checks if the output of the prover corresponds to the expected value for the test;
- the function `benchmark` accepts a register and a test suite and returns the times and outcomes of each prover.

All the outputs of the functions above are pandas `DataFrame`s, which means that they can be easily queried, dumped to csv, aggregated, or visualized using most plotting libraries.

### 5.1.1 Prefix format

Since for benchmarking we will interface with a lot of different provers, each with its own syntax for expressions, the need for a common format which was easy to parse and translate arose. For this purpose we define a prefix format for linear logic formulae inspired by the format used by [**?**] for implicational formulae

| formula | symbol |
|---|---|
| $\phi_A \otimes \phi_B$ | `*AB` |
| $\phi_A \parr \phi_B$ | `\|AB` |
| $\phi_A \oplus \phi_B$ | `+AB` |
| $\phi_A \,\&\, \phi_B$ | `&AB` |
| $\phi_A \multimap \phi_B$ | `@AB` |
| $\phi_A{}^{\perp}$ | `^A` |
| $?\phi_A$ | `?A` |
| $!\phi_A$ | `!A` |

Furthermore each single character not representing an operator is considered as a variable name. Longer names can be specified by enclosing them in single apices as in `'varname'`. As an example we give the translation of DeMorgan for the tensor:

$$\text{trans}((a \otimes b)^{\perp} \multimap a^{\perp} \parr b^{\perp}) = \texttt{@\^{}ab|\^{}a\^{}b}$$

### 5.1.2 File formats

We use json as a standard format to store the tests because of its vast adoption by most programming languages. A test suite is thus defined as a list of test cases

```
TestCase ::= {
  "id": <Number>,
  "premises": [ <PrefixFormula>* ],
  "conclusions": [ <PrefixFormula>* ]
}
```

where

**id**
: is a number with the sole purpose of tracing back the test case from the output;

**premises**
: is a list of premises as prefix formulae;

**conclusions**
: a list of conclusions as prefix formulae.

Other arbitrary fields may be present, for example we will use the following optional fields:

**thm**
: whether this test case is a tautology or not, may be null;

***, &, +, ...**
: the number of times a specific connective appears in the test case;

**notes**
: human readable text about the test case, for example its infix representation;

**size**
: an indicative number of the size of the formula;

**atoms**
: the upper bound on the number of atoms.

### 5.1.3 Formula generation

One of the sources of formulae we'll use in Section 5.2 is APLL's random formula generator. The version we'll use is a slight modification of it where:

- the output is in the json format described in Section 5.1.2
- one can choose to generate normalized formulae or not;
- one can choose which connectives appear in the generated formula.

A noteworthy detail is how the parameters `size` and `atoms` mentioned in Section 5.1.2 are defined, since these are directly related to how the formulae are generated:

- when one specifies a number of atoms `atoms`, the generator initializes an array containing `atoms` atoms, their negations, and the constants $\bot, \top, \ldots$. During the generation of the formula this array is randomly accessed, choosing an element when needed. This means that `atoms` represents an upper bound to the number of different atoms that may appear in the formula, not their exact number.

- when a formula is generated, at each step it is chosen whether to generate a unary or binary connective based on a threshold:

  - if a unary connective is chosen, the process continues with a size of `size`$-1$;
  - if a binary connective is chosen, the program chooses a random value between 0 and `size`, and it generates the two branches of the formula, with size respectively $k$ and `size` $- k$.

## 5.2 Benchmarking

We'll mainly use three sources for formulae:

- llprover's tests
- LLTP, especially the translations of Kleene's intuitionistic formulae
- randomly generated formulae made by the genrator described in 5.1.3

llprovers tests are composed mainly by simple linear logic tautologies, e.g. the DeMorgan rules, for this reason these tests are used more as a simple and fast suite to catch the most obvious bugs between iterations of the prover.

We now show the results of running the provers on two datasets: KLE-cbn and KLE-cbv, respectively the call-by-name and call-by-value translations of Kleene's theorems. These translations introduce a high number of exponentials, and this causes – other than timeouts because of the added complexity – some failures. These failures are not due to bugs, but instead happen because the prover has reached its bound for that formula. The benchmarks are done using a timeout of 60 s and a bound of 3.

Kleene CBN

| prover | timeouts | failures | successes | success rate | avg. time (succ.) | avg. time (tot.) |
|---|---|---|---|---|---|---|
| APLL | 0 | 16 | 72 | $\approx 0.80$ | 0.037 s | 0.055 s |
| llprover | 20 | 6 | 62 | $\approx 0.70$ | 1.709 s | 3.253 s |
| sat-ll | 4 | 18 | 66 | $\approx 0.75$ | 0.130 s | 0.185 s |

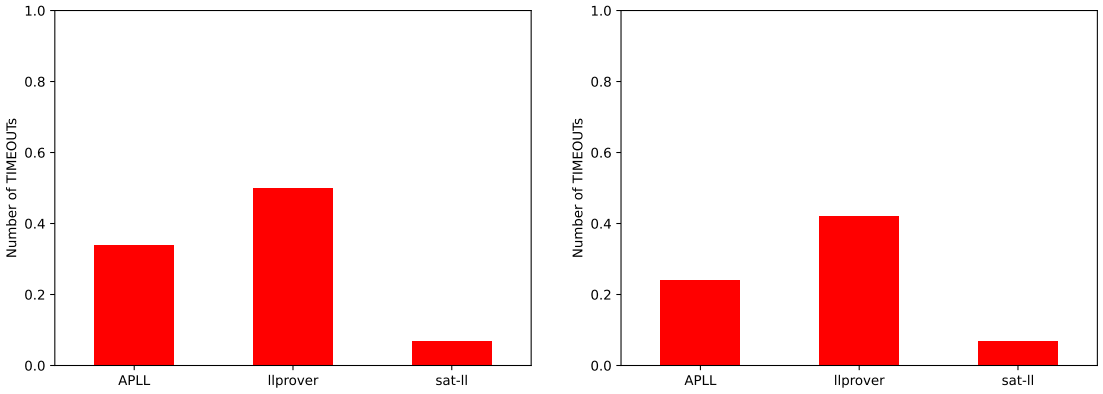
Kleene CBV

| prover | timeouts | failures | successes | success rate | avg. time (succ.) | avg. time (tot.) |
|---|---|---|---|---|---|---|
| APLL | 0 | 17 | 71 | $\approx 0.80$ | 0.035 s | 0.326 s |
| llprover | 20 | 6 | 62 | $\approx 0.70$ | 0.981 s | 2.179 s |
| sat-ll | 5 | 15 | 68 | $\approx 0.77$ | 0.443 s | 0.496 s |

There are mainly two downsides with using random formulae:

- most cases do not hold any structure,
- ???

Using random formulae we can clearly see that our prover outperforms APLL (and llprover) when dealing with formulae rich in multiplicatives.




(a) Multiplicative case (b) Multiplicative and additive case

Figure 5.1: Percentage of number of timeouts out of a hundred formulae

We can see that in the multiplicative and additive case the difference begin to level. The additive case is not that significant as the formulae remain manageable and no major differences can be seen.

As soon as exponentials come into play the differences level out. It can be seen in 5.2 that in full linear logic our prover performs slightly worse than APLL.

All these test were done generating suits of 100 tests. Figure 5.1a's tests were composed of normalized formulae of `size` 100, and `atoms` 50, with just the connectives $\otimes$ and $\parr$. Figure 5.1b's tests were composed of normalized formulae formulae

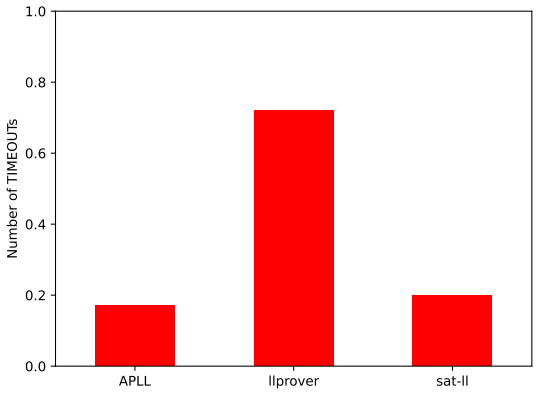



Figure 5.2: Full linear logic

of `size` 500, and `atoms` 250, with the connectives $\otimes$, $\parr$ , & and $\oplus$. Finally 5.2's tests were composed of normalized formulae of `size` 500, and `atoms` 250, with all the connectives.

When looking at the results of full linear logic, it is important to note that unlike the tests with multiplicatives and additives, some of the results may be early failures because of the bound. Since llprover uses incremental search, its times are often the slowest. Similarly our prover is consistently slightly slower that APLL, this difference is negligible and due to the fact that APLL is compiled, whereas our prover is interpreted.