2.5 Normal Deductions

An intuitive strategy in constructing natural deductions is to apply introduction rules backwards to break the conclusion into subgoals and to apply elimination rules to hypotheses until the two meet. This strategy is in fact complete which has numerous consequences. One of the most important is *consistency* of the logic, that is, not every proposition is true. This is closely related to the local soundness property we have investigated for each of the connectives.

We call natural deductions which have been constructed with the strategy sketched above *normal*. Normalcy is a judgment about derivations, just as truth is a judgment about propositions. It is awkward to write out and reason about judgments on derivations, but there are standard techniques to avoid them. The most commonly used is to reformulate the judgment on derivations as a judgment on objects, in this case propositions. Instead of judging a derivation to be normal, the judgment expresses that "*A has a normal derivation*".

In our situation one judgment will not be sufficient, since we need to describe bottom-up reasoning (introduce the main connective of the conclusion) and top-down reasoning (eliminate the main connective of the hypothesis). Thus we have two mutually dependent judgments

$\Gamma; \Delta \vdash A \uparrow$ A has a normal derivation, and
$\Gamma; \Delta \vdash A \downarrow$ A has an atomic derivation,

where the latter formalizes the top-down reasoning from hypotheses (intuitionistic or linear). These judgments are defined by the following inference rules.

Hypotheses.

$$\frac{}{\Gamma; (\cdot, w{:}A) \vdash A \;\downarrow}\,w \qquad \frac{}{(\Gamma_1, u{:}A, \Gamma_2); \cdot \vdash A \;\downarrow}\,u$$

Multiplicative Connectives.

$$\frac{\Gamma; \Delta_1 \vdash A \;\uparrow \qquad \Gamma; \Delta_2 \vdash B \;\uparrow}{\Gamma; (\Delta_1 \times \Delta_2) \vdash A \otimes B \;\uparrow}\,{\otimes}\mathrm{I} \qquad \frac{\Gamma; \Delta \vdash A \otimes B \;\downarrow \qquad \Gamma; (\Delta', w_1{:}A, w_2{:}B) \vdash C \;\uparrow}{\Gamma; (\Delta' \times \Delta) \vdash C \;\uparrow}\,{\otimes}\mathrm{E}^{w_1,w_2}$$

$$\frac{\Gamma; (\Delta, w{:}A) \vdash B \;\uparrow}{\Gamma; \Delta \vdash A \multimap B \;\uparrow}\,{\multimap}\mathrm{I}^{w} \qquad \frac{\Gamma; \Delta \vdash A \multimap B \;\downarrow \qquad \Gamma; \Delta' \vdash A \;\uparrow}{\Gamma; \Delta \times \Delta' \vdash B \;\downarrow}\,{\multimap}\mathrm{E}$$

$$\frac{}{\Gamma; \cdot \vdash \mathbf{1} \;\uparrow}\,\mathbf{1}\mathrm{I} \qquad \frac{\Gamma; \Delta \vdash \mathbf{1} \;\downarrow \qquad \Gamma; \Delta' \vdash C \;\uparrow}{\Gamma; (\Delta' \times \Delta) \vdash C \;\uparrow}\,\mathbf{1}\mathrm{E}$$

Additive Connectives.

$$\frac{\Gamma;\Delta \vdash A \uparrow \qquad \Gamma;\Delta \vdash B \uparrow}{\Gamma;\Delta \vdash A \& B \uparrow}\,\&\mathrm{I} \qquad \frac{\Gamma;\Delta \vdash A \& B \downarrow}{\Gamma;\Delta \vdash A \downarrow}\,\&\mathrm{E_L} \qquad \frac{\Gamma;\Delta \vdash A \& B \downarrow}{\Gamma;\Delta \vdash B \downarrow}\,\&\mathrm{E_R}$$

$$\frac{}{\Gamma;\Delta \vdash \top \uparrow}\,\top\mathrm{I} \qquad \textit{No } \top \textit{ elimination rule}$$

$$\frac{\Gamma;\Delta \vdash A \uparrow}{\Gamma;\Delta \vdash A \oplus B \uparrow}\,\oplus\mathrm{I_L} \qquad \frac{\Gamma;\Delta \vdash B \uparrow}{\Gamma;\Delta \vdash A \oplus B \uparrow}\,\oplus\mathrm{I_R}$$

$$\frac{\Gamma;\Delta \vdash A \oplus B \downarrow \quad \Gamma;(\Delta', w_1{:}A) \vdash C \uparrow \quad \Gamma;(\Delta', w_2{:}B) \vdash C \uparrow}{\Gamma;(\Delta' \times \Delta) \vdash C \uparrow}\,\oplus E^{w_1,w_2}$$

$$\textit{No } \mathbf{0} \textit{ introduction rule} \qquad \frac{\Gamma;\Delta \vdash 0 \downarrow}{\Gamma;(\Delta' \times \Delta) \vdash C \uparrow}\,\mathbf{0E}$$

Quantifiers.

$$\frac{\Gamma;\Delta \vdash [a/x]A \uparrow}{\Gamma;\Delta \vdash \forall x.\ A \uparrow}\,\forall\mathrm{I}^a \qquad \frac{\Gamma;\Delta \vdash \forall x.\ A \downarrow}{\Gamma;\Delta \vdash [t/x]A \downarrow}\,\forall\mathrm{E}$$

$$\frac{\Gamma;\Delta \vdash [t/x]A \uparrow}{\Gamma;\Delta \vdash \exists x.\ A \uparrow}\,\exists\mathrm{I} \qquad \frac{\Gamma;\Delta \vdash \exists x.\ A \downarrow \qquad \Gamma;(\Delta', w{:}[a/x]A) \vdash C \uparrow}{\Gamma;(\Delta' \times \Delta) \vdash C \uparrow}\,\exists\mathrm{E}^{a,w}$$

Exponentials.

$$\frac{(\Gamma, u{:}A);\Delta \vdash B \uparrow}{\Gamma;\Delta \vdash A \supset B \uparrow}\,\supset\mathrm{I}^u \qquad \frac{\Gamma;\Delta \vdash A \supset B \downarrow \qquad \Gamma;\cdot \vdash A \uparrow}{\Gamma;\Delta \vdash B \downarrow}\,\supset\mathrm{E}$$

$$\frac{\Gamma;\cdot \vdash A \uparrow}{\Gamma;\cdot \vdash {!A} \uparrow}\,!I \qquad \frac{\Gamma;\Delta \vdash {!A} \downarrow \qquad (\Gamma, u{:}A);\Delta' \vdash C \uparrow}{\Gamma;(\Delta' \times \Delta) \vdash C \uparrow}\,!\mathrm{E}^u$$

Coercion.

$$\frac{\Gamma; \Delta \vdash A \downarrow}{\Gamma; \Delta \vdash A \uparrow}\downarrow\uparrow$$

The coercion $\downarrow\uparrow$ states that all atomic derivations should be considered normal. From the point of view of proof search this means that we can complete the derivation when forward and backward reasoning arrive at the same proposition. It easy to see that these judgments just restrict the set of derivations.

Property 2.5 (Soundness of Normal Derivations)

1. *If* $\Gamma; \Delta \vdash A \uparrow$ *then* $\Gamma; \Delta \vdash A$*.*

2. *If* $\Gamma; \Delta \vdash A \downarrow$ *then* $\Gamma; \Delta \vdash A$*.*

Proof: *By simultaneous induction on the given derivations. The computational contents of this proof are the obvious structural translation from* $\mathcal{N} :: (\Gamma; \Delta \vdash A \uparrow)$ *to* $\mathcal{N}^- :: (\Gamma; \Delta \vdash A)$ *and from* $\mathcal{A} :: (\Gamma; \Delta \vdash A \downarrow)$ *to* $\mathcal{A}^- :: (\Gamma; \Delta \vdash A)$*. Note that the coercion* $\downarrow\uparrow$ *disappears, since the translation of the premiss and conclusion are identical.* □

The corresponding completeness theorem, namely that $\Gamma; \Delta \vdash A$ implies $\Gamma; \Delta \vdash A \uparrow$, also holds, but is quite difficult to prove. This is the subject of the Normalization Theorem **??**. Together with the two judgments about atomic and normal derivations, we have refined substitution principles. Since hypotheses are atomic, they permit only the substitution of atomic derivations for hypotheses.

Lemma 2.6 (Substitution Principles for Normal Derivations)

1. *If* $\Gamma; (\Delta_1, w{:}A, \Delta_2) \vdash C \uparrow$ *and* $\Gamma; \Delta \vdash C \downarrow$ *then* $\Gamma; (\Delta_1, \Delta, \Delta_2) \vdash C \uparrow$

2. *If* $\Gamma; (\Delta_1, w{:}A, \Delta_2) \vdash C \downarrow$ *and* $\Gamma; \Delta \vdash C \downarrow$ *then* $\Gamma; (\Delta_1, \Delta, \Delta_2) \vdash C \downarrow$

3. *If* $(\Gamma_1, u{:}A, \Gamma_2); \Delta \vdash C \uparrow$ *and* $\Gamma_1; \cdot \vdash C \downarrow$ *then* $(\Gamma_1, \Gamma_2); \Delta \vdash C \uparrow$

4. *If* $(\Gamma_1, u{:}A, \Gamma_2); \Delta \vdash C \downarrow$ *and* $\Gamma_1; \cdot \vdash C \downarrow$ *then* $(\Gamma_1, \Gamma_2); \Delta \vdash C \downarrow$

Proof: By straightforward inductions over the structure of the first of the given derivations. □

A first immediate connection to local reductions is the following.

Property 2.7

1. *If* $\mathcal{N} :: (\Gamma; \Delta \vdash A \uparrow)$ *then* $\mathcal{N}^- :: (\Gamma; \Delta \vdash A)$ *contains no local redex.*

2. *If* $\mathcal{A} :: (\Gamma; \Delta \vdash A \downarrow)$ *then* $\mathcal{A}^- :: (\Gamma; \Delta \vdash A)$ *contains no local redex.*

Proof: By induction on the structure of $\mathcal{N}$ and $\mathcal{A}$, inspecting the possible forms of local redices in each case. □

We can now also give an alternative way to describe the connection between IL and ILL by showing the normal deductions can be translated in the opposite directions quite easily. We write $!\Delta$ for a context of the form $\cdot, u_1{:}!A_1, \ldots, u_n{:}!A_n$.

Lemma 2.8

1. *If* $\Gamma^+; !\Delta^+ \vdash A^+ \ \uparrow$ *in ILL then* $\Gamma, \Delta \vdash A$ *in IL.*
2. *If* $\Gamma^+; !\Delta^+ \vdash !A^+ \ \uparrow$ *in ILL then* $\Gamma, \Delta \vdash A$ *in IL.*
3. *If* $\Gamma^+; !\Delta^+ \vdash C \ \downarrow$ *in ILL then either* $C = B^+$ *or* $C = !B^+$ *for some* B *and* $\Gamma, \Delta \vdash B$ *in IL.*

Proof: By simultaneous induction on the structures of $\mathcal{N} :: (\Gamma^+; !\Delta^+ \vdash A^+ \ \uparrow)$ and $\mathcal{A} :: (\Gamma^+; !\Delta^+ \vdash C \ \downarrow)$. □

2.6 Cut-Free Sequent Calculus

The sequent calculus can be seen as a calculus of proof search for natural deductions. In this section we try to transcribe the process of searching for a *normal* natural deduction into an inference system. In the context of sequent calculus, proof search is seen entirely as the bottom-up construction of a derivation. This means that elimination rules must be turned "upside-down" so they can also be applied bottom-up rather than top-down. A sequent has the form $\Gamma; \Delta \Longrightarrow C$, where Γ corresponds to unrestricted hypotheses Δ to linear hypotheses, and C to the conclusion.

In terms of *judgments* we interpret a sequent via a splitting of the judgment "*A is true*" into two judgments: "*A is a resource*" and "*A is a true conclusion*". Ignoring unrestricted hypothesis for the moment, the main judgment

$$(\cdot, w_1{:}A_1, \ldots, w_n{:}A_n) \Longrightarrow C$$

expresses

> Under the linear hypothesis that we have resources $A_1, \ldots, A_n$ we judge C to be a true conclusion.

Adding unrestricted hypotheses, the judgment

$$(\cdot, u_1{:}B_1, \ldots, u_m{:}B_m); (\cdot, w_1{:}A_1, \ldots, w_n{:}A_n) \Longrightarrow C$$

expresses

> Under the unrestricted hypotheses that we have resources $B_1, \ldots, B_m$ and linear hyptheses that we have resources $A_1, \ldots, A_n$, we judge C to be a true conclusion.

This interpretation means that we now have an explicit inference rule which relates the judgment "*A is a resource*" to the judgment "*A is a true conclusion*". We call the resulting sequent an *initial sequent* and write I.

$$\frac{}{\Gamma; (\cdot, w{:}A) \Longrightarrow A}\,\mathrm{I}(w)$$

The remaining rules are divided into *right* and *left* rules, which correspond to the *introduction* and *elimination* rules of natural deduction, respectively. The right rules apply to the conclusion, while the left rules apply to resources. Since resources may be either linear or unrestricted, our notation would require two versions of each left rule. Instead we add one more hypothesis rule which allows us to copy an unrestricted to a linear hypothesis. This rule is labelled DL for *dereliction*.

$$\frac{(\Gamma_1, u{:}A, \Gamma_2); (\Delta, w{:}A) \Longrightarrow C}{(\Gamma_1, u{:}A, \Gamma_2); \Delta \Longrightarrow C}\,\mathrm{DL}^w(u)$$

In the following, we adhere to common practice and omit labels on hypotheses and consequently also on the justifications of the inference rules. The reader should keep in mind, however, that this is just a short-hand, and that there are, for example, two *different* derivations of $(\cdot, A, A); \cdot \Longrightarrow A$, one using the first copy of A and one using the second.

Finally, we permit implicit uses of exchange in the conclusion in order to move the principal proposition of a rule to the right-most position. In other words, we write Δ, A instead of $\Delta_1, w{:}A, \Delta_2$. We repeat the rules from above in their abbreviated form and the give the remaining left and right rules.

Hypotheses.

$$\frac{}{\Gamma; A \Longrightarrow A}\,\mathrm{I} \qquad \frac{(\Gamma, A); (\Delta, A) \Longrightarrow C}{(\Gamma, A); \Delta \Longrightarrow C}\,\mathrm{DL}$$

Multiplicative Connectives.

$$\frac{\Gamma; \Delta, A \Longrightarrow B}{\Gamma; \Delta \Longrightarrow A \multimap B}\multimap\mathrm{R} \qquad \frac{\Gamma; \Delta_1 \Longrightarrow A \qquad \Gamma; \Delta_2, B \Longrightarrow C}{\Gamma; \Delta_1 \times \Delta_2, A \multimap B \Longrightarrow C}\multimap\mathrm{L}$$

$$\frac{\Gamma; \Delta_1 \Longrightarrow A \qquad \Gamma; \Delta_2 \Longrightarrow B}{\Gamma; \Delta_1 \times \Delta_2 \Longrightarrow A \otimes B}\otimes\mathrm{R} \qquad \frac{\Gamma; \Delta, A, B \Longrightarrow C}{\Gamma; \Delta, A \otimes B \Longrightarrow C}\otimes\mathrm{L}$$

$$\frac{}{\Gamma; \cdot \Longrightarrow \mathbf{1}}\,\mathbf{1}\mathrm{R} \qquad \frac{\Gamma; \Delta \Longrightarrow C}{\Gamma; \Delta, \mathbf{1} \Longrightarrow C}\,\mathbf{1}\mathrm{L}$$

Additive Connectives.

$$\frac{\Gamma;\Delta \Longrightarrow A \qquad \Gamma;\Delta \Longrightarrow B}{\Gamma;\Delta \Longrightarrow A\&B}\,\&\mathrm{R} \qquad \begin{array}{c} \dfrac{\Gamma;\Delta, A \Longrightarrow C}{\Gamma;\Delta, A\&B \Longrightarrow C}\,\&\mathrm{L}_1 \\[1ex] \dfrac{\Gamma;\Delta, B \Longrightarrow C}{\Gamma;\Delta, A\&B \Longrightarrow C}\,\&\mathrm{L}_2 \end{array}$$

$$\frac{}{\Gamma;\Delta \Longrightarrow \top}\,\top\mathrm{R} \qquad \textit{No } \top \textit{ left rule}$$

$$\begin{array}{c} \dfrac{\Gamma;\Delta \Longrightarrow A}{\Gamma;\Delta \Longrightarrow A \oplus B}\,\oplus\mathrm{R}_1 \\[1ex] \dfrac{\Gamma;\Delta \Longrightarrow B}{\Gamma;\Delta \Longrightarrow A \oplus B}\,\oplus\mathrm{R}_2 \end{array} \qquad \frac{\Gamma;\Delta, A \Longrightarrow C \qquad \Gamma;\Delta, B \Longrightarrow C}{\Gamma;\Delta, A \oplus B \Longrightarrow C}\,\oplus\mathrm{L}$$

$$\textit{No } \mathbf{0} \textit{ right rule} \qquad \frac{}{\Gamma;\Delta, \mathbf{0} \Longrightarrow C}\,\mathbf{0}\mathrm{L}$$

Quantifiers.

$$\frac{\Gamma;\Delta \Longrightarrow [a/x]A}{\Gamma;\Delta \Longrightarrow \forall x.\ A}\,\forall\mathrm{R}^a \qquad \frac{\Gamma;\Delta, [t/x]A \Longrightarrow C}{\Gamma;\Delta, \forall x.\ A \Longrightarrow C}\,\forall\mathrm{L}$$

$$\frac{\Gamma;\Delta \Longrightarrow [t/x]A}{\Gamma;\Delta \Longrightarrow \exists x.\ A}\,\exists\mathrm{R} \qquad \frac{\Gamma;\Delta, [a/x]A \Longrightarrow C}{\Gamma;\Delta, \exists x.\ A \Longrightarrow C}\,\exists\mathrm{L}^a$$

Exponentials.

$$\frac{(\Gamma, A);\Delta \Longrightarrow B}{\Gamma;\Delta \Longrightarrow A \supset B}\,\supset\mathrm{R} \qquad \frac{\Gamma;\cdot \Longrightarrow A \qquad \Gamma;\Delta, B \Longrightarrow C}{\Gamma;\Delta, A \supset B \Longrightarrow C}\,\supset\mathrm{L}$$

$$\frac{\Gamma;\cdot \Longrightarrow A}{\Gamma;\cdot \Longrightarrow\, !A}\,!\mathrm{R} \qquad \frac{(\Gamma, A);\Delta \Longrightarrow C}{\Gamma;\Delta, !A \Longrightarrow C}\,!\mathrm{L}$$

We have the following theorems relating normal natural deductions and sequent derivations.

Theorem 2.9 (Soundness of Sequent Derivations)

If $\Gamma;\Delta \Longrightarrow A$ *then* $\Gamma;\Delta \vdash A\ \uparrow$.

Proof: By induction on the structure of the derivation of $\Gamma;\Delta \Longrightarrow A$. Initial sequents are translated to the $\downarrow\uparrow$ coercion, and use of an unrestricted hypothesis follows by a substitution principle (Lemma 2.6). For right rules we apply the corresponding introduction rules. For left rules we either directly construct a derivation of the conclusion after an appeal to the induction hypothesis ($\otimes$L, $\mathbf{1}$L, $\otimes$L, $\mathbf{0}$L, $\exists$L, !L) or we appeal to a substitution principle of atomic natural deductions for hypotheses ($\multimap$ L, &L$_1$, &L$_2$, $\forall$L, $\supset$L). □

Theorem 2.10 (Completeness of Sequent Derivations)

1. *If* $\Gamma;\Delta \vdash A\ \uparrow$ *then there is a sequent derivation of* $\Gamma;\Delta \Longrightarrow A$*, and*
2. *if* $\Gamma;\Delta \vdash A\ \downarrow$ *then for any formula* C *and derivation of* $\Gamma;\Delta', A \Longrightarrow C$ *there is a derivation of* $\Gamma;(\Delta' \times \Delta) \Longrightarrow C$*.*

Proof: By simultaneous induction on the structure of the derivations of $\Gamma;\Delta \vdash A\ \uparrow$ and $\Gamma;\Delta \vdash A\ \downarrow$. □

2.7 Another Example: Concurrent Systems

Another class of examples for linear logic is the description of concurrent systems. Linear logic can be used to represent whole classes of concurrent systems, such as Petri Nets [MOM91] or Milner's π-calculus [MPP92]. At present we are concerned only with the basic principles. We also now employ sequent derivations instead of natural deductions to model computations.

Unlike the planning example, in concurrent computation there is no overall goal, just an evolution of state. Thus the right-hand side of the judgment should be "empty", which we model by $\mathbf{0}$, the impossible goal. Thus the basic representation of a concurrent system is

$$\Gamma_0;\Delta \Longrightarrow \mathbf{0}$$

where Γ_0 are the rules of computation and Δ is the state (including the processes, messages, *etc.*). A partial derivation

$$\begin{array}{c}\Gamma_0;\Delta_1 \Longrightarrow \mathbf{0}\\ \vdots\\ \Gamma_0;\Delta_0 \Longrightarrow \mathbf{0}\end{array}$$

represents a computation from Δ_0 to Δ_1.

We consider a simple example with the following atomic propositions.

send(x,y,m)	x is sending the message m to y
message(x,y,m)	message m from x to y is in transit
listen(y)	y is listening for messages addressed to y
received(y,x,m)	y has received message m from x

The computation rules are linear implications, available as unrestricted hypotheses.

$$\begin{array}{rcl} \mathrm{sendMsg} & : & \forall x.\ \forall y.\ \forall m.\ \mathrm{send}(x,y,m) \multimap \mathrm{message}(x,y,m) \\ \mathrm{receiveMsg} & : & \forall x.\ \forall y.\ \forall m.\ \mathrm{message}(x,y,m) \otimes \mathrm{listen}(y) \\ & & \qquad\qquad\qquad \multimap \mathrm{listen}(y) \otimes \mathrm{received}(y,x,m) \end{array}$$

Here, y continues to listen after it has received and stored a message. However, the receiver cannot distinguish the order in which messages were sent or received. This can be modelled by explicitly adding time stamps to the predicates above, or by using *non-commutative linear logic* (see Chapter **??**). Protocols for communication which require acknowledgments and other complex exchanges can be modelled based on the simple ideas above. For example, to express that a message may be lost, we can add the following rule.

$$\mathrm{loseMsg} \quad : \quad \mathrm{message}(x,y,m) \multimap \mathbf{1}$$

Here and below we omit universal quantifiers for the sake of brevity: all free variables in a rule are implicitly universally quantified on the outside.

Other connectives also have interesting computational interpretations. For example, a global abort message from x can be implemented using $\mathbf{0}$.

$$\mathrm{abortSys} \quad : \quad \mathrm{abort}(x) \otimes \mathrm{authorized}(x) \multimap \mathbf{0}$$

If x is authorized and aborts, we obtain $\mathbf{0}$ as part of the state from which we can prove anything and terminate the computation. However, there is nothing in the reading of derivations as deductions which would force this to be "immediate": other computations could still proceed.

Alternative conjunction represents non-deterministic choice. Since we intend that any derivation represents a legal computation, this means a resource $A \& B$ could evolve to either A or B. For example, if storing a message might fail in the sense that it simply disappears, we can specify:

$$\mathrm{receiveMsg}' \quad : \quad \mathrm{message}(x,y,m) \otimes \mathrm{listen}(y) \multimap \mathrm{listen}(y) \otimes (\mathrm{received}(y,x,m) \& \mathbf{1})$$

Quantifiers can also be used to advantage. For example, we can send a message to anyone.

$$\mathrm{sendMsgAny} \quad : \quad \mathrm{sendany}(x,m) \otimes (\forall y.\ \mathrm{message}(x,y,m))$$

However, this message can only ever be seen by one recipient. If we want to publish a message so everyone can see it, and see it as often as they like without storing it locally, we can specify:

$$\mathrm{publishMsg} \quad : \quad \mathrm{publish}(x,m) \otimes {!}(\forall y.\ \mathrm{message}(x,y,m))$$

Some protocols establish "new connections", and some security protocols require the sender to generate a "fresh" message which has never been seen before. We can model both of these with an existential quantifier, since its left rule will introduce a new parameter, which may not occur in the present state.

$$\mathrm{sendFresh} \quad : \quad \mathrm{fresh}(x, y) \multimap \exists m.\ \mathrm{message}(x, y, m)$$

The reader is invited to verify how sequent derivations, constructed in a bottom-up fashion, model computations. In each case we match the left-hand side of a linear implication in Γ_0 against components of the state, and then add the components of the right-hand side.