pty.1 Normalization

int:pty:nor: sec

In this section we prove that, via some reduction order, any deduction can be reduced to a normal deduction, which is called the *normalization property*. We will make use of the propositions-as-types correspondence: we show that every proof term can be reduced to a normal form; normalization for natural deduction derivations then follows.

Firstly we define some functions that measure the complexity of terms. The *length* $\mathrm{len}(\varphi)$ of a formulas is defined by

$$\begin{aligned}\mathrm{len}(p) &= 0\\ \mathrm{len}(\varphi \wedge \psi) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1\\ \mathrm{len}(\varphi \vee \psi) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1\\ \mathrm{len}(\varphi \to \psi) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1.\end{aligned}$$

The complexity of a redex M is measured by its *cut rank* $\mathrm{cr}(M)$:

$$\begin{aligned}\mathrm{cr}((\lambda x^{\varphi}.\, N^{\psi})Q) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1\\ \mathrm{cr}(\mathrm{p}_i(\langle M^{\varphi}, N^{\psi}\rangle)) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1\\ \mathrm{cr}(\mathrm{case}(\mathrm{in}_i^{\varphi_i}(M^{\varphi_i}), x_1^{\varphi_1}.N_1^{\chi}, x_2^{\varphi_2}.N_2^{\chi})) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1\end{aligned}$$

The complexity of a proof term is measured by the most complex redex in it, and 0 if it is normal:

$$\mathrm{mr}(M) = \max\{\mathrm{cr}(N) | N \text{ is a sub term of } M \text{ and is redex}\}$$

int:pty:nor: lem:subst

Lemma pty.1. *If $M[N^{\varphi}/x^{\varphi}]$ is a redex and $M \not\equiv x$, then one of the following cases holds:*

1. *M is itself a redex, or*
2. *M is of the form $\mathrm{p}_i(x)$, and N is of the form $\langle P_1, P_2\rangle$*
3. *M is of the form $\mathrm{case}(i, x_1.P_1, x_2.P_2)$, and N is of the form $\mathrm{in}_i(Q)$*
4. *M is of the form xQ, and N is of the form $\lambda x.\, P$*

In the first case, $\mathrm{cr}(M[N/x]) = \mathrm{cr}(M)$; in the other cases, $\mathrm{cr}(M[N/x]) = \mathrm{len}(\varphi))$.

Proof. Proof by induction on M.

1. If M is a single variable y and $y \not\equiv x$, then $y[N/x]$ is y, hence not a redex.
2. If M is of the form $\langle N_1, N_2\rangle$, or $\lambda x.\, N$, or $\mathrm{in}_i^{\varphi}(N)$, then $M[N^{\varphi}/x^{\varphi}]$ is also of that form, and so is not a redex.
3. If M is of the form $\mathrm{p}_i(P)$, we consider two cases.

a) If P is of the form $\langle P_1, P_2\rangle$, then $M \equiv \mathrm{p}_i(\langle P_1, P_2\rangle)$ is a redex, and clearly
$$M[N/x] \equiv \mathrm{p}_i(\langle P_1[N/x], P_2[N/x]\rangle)$$
is also a redex. The cut ranks are equal.

b) If P is a single variable, it must be x to make the substitution a redex, and N must be of the form $\langle P_1, P_2\rangle$. Now consider
$$M[N/x] \equiv \mathrm{p}_i(x)[\langle P_1, P_2\rangle/x],$$
which is $\mathrm{p}_i(\langle P_1, P_2\rangle)$. Its cut rank is equal to $\mathrm{cr}(x)$, which is $\mathrm{len}(\varphi)$.

The cases of $\mathrm{case}(N, x_1.N_1, x_2.N_2)$ and PQ are similar. □

Lemma pty.2. *If M contracts to M', and $\mathrm{cr}(M) > \mathrm{cr}(N)$ for all proper redex sub-terms N of M, then $\mathrm{cr}(M) > \mathrm{mr}(M')$.*

Proof. Proof by cases.

1. If M is of the form $\mathrm{p}_i(\langle M_1, M_2\rangle)$, then M' is M_i; since any sub-term of M_i is also proper sub-term of M, the claim holds.

2. If M is of the form $(\lambda x^\varphi.\, N)Q^\varphi$, then M' is $N[Q^\varphi/x^\varphi]$. Consider a redex in M'. Either there is corresponding redex in N with equal cut rank, which is less than $\mathrm{cr}(M)$ by assumption, or the cut rank equals $\mathrm{len}(\varphi)$, which by definition is less than $\mathrm{cr}((\lambda x^\varphi.\, N)Q)$.

3. If M is of the form
$$\mathrm{case}(\mathrm{in}_i(N^{\varphi_i}), x_1^{\varphi_1}.N_1^\chi, x_2^{\varphi_2}.N_2^\chi),$$
then $M' \equiv N_i[N/x_i^{\varphi_i}]$. Consider a redex in M'. Either there is corresponding redex in N_i with equal cut rank, which is less than $\mathrm{cr}(M)$ by assumption; or the cut rank equals $\mathrm{len}(\varphi_i)$, which by definition is less than $\mathrm{cr}(\mathrm{case}(\mathrm{in}_i(N^{\varphi_i}), x_1^{\varphi_1}.N_1^\chi, x_2^{\varphi_2}.N_2^\chi))$. □

Theorem pty.3. *All proof terms reduce to normal form; all derivations reduce to normal derivations.*

Proof. The second follows from the first. We prove the first by complete induction on $m = \mathrm{mr}(M)$, where M is a proof term.

1. If $m = 0$, M is already normal.

2. Otherwise, we proceed by induction on n, the number of redexes in M with cut rank equal to m.

a) If $n = 1$, select any redex N such that $m = \mathrm{cr}(N) > \mathrm{cr}(P)$ for any proper sub-term P which is also a redex of course. Such a redex must exist, since any term only has finitely many subterms.

   Let N' denote the reductum of N. Now by the lemma $\mathrm{mr}(N') < \mathrm{mr}(N)$, thus we can see that n, the number of redexes with $\mathrm{cr}(=)m$ is decreased. So m is decreased (by 1 or more), and we can apply the inductive hypothesis for m.

b) For the induction step, assume $n > 1$. the process is similar, except that n is only decreased to a positive number and thus m does not change. We simply apply the induction hypothesis for n. □

The fact that typed λ-terms normalize means that every such term *has a normal form*. If we think of β-reducing λ-terms to their normal form as executing a computation and the normal form as the value of the computation, this means that every computation in the typed λ-calculus eventually halts an produces a value. Moreover, type preservation ensures that the value has the right type. E.g., if N has type $\varphi \to \psi$ (i.e., it is a function that is supposed to work for arguments of type φ and produces values of type ψ) and we apply it to a term M of type φ (the input), (NM) reduces to a term N' (the output) and that output is guaranteed to be of type ψ.

In fact, terms in the typed λ-calculus don't just reduce to normal forms for one way of applying β-reductions to subterms, but *any* way of applying β-reductions to subtems eventually terminates in a normal form. This property is called *strong normalization*. It means that not only is there a way to guarantee that a computation eventually halts and produces a value, but *any* way to execute the computation eventually produces a value.

How do we know that different ways of executing a computation produce the *same* value? So far we just know (from type preservation) that all values it produces are of the same type. The typed λ-calculus has another important property: it is *confluent* or *Church-Rosser*. If $N \twoheadrightarrow N_1$ and $N \twoheadrightarrow N_2$ then there is some term N' such that $N_1 \twoheadrightarrow N'$ and $N_2 \twoheadrightarrow N'$. Recall that $N \twoheadrightarrow N'$ means: N' results from zero or more $\to$-reduction steps. If N_1 is in normal form then the only term N' such that $N_1 \twoheadrightarrow N'$ is N_1 itself (via zero $\to$-reduction steps). It follows that if N_1 and N_2 are both in normal form, then $N_1 = N' = N_2$. In other words, since $\twoheadrightarrow$ is strongly normalizing, every way of reducing a term eventually results in a normal form. Since $\twoheadrightarrow$ is Church-Rosser, any two normal forms are equal. Hence, computation in the typed λ-calculus always terminates and the value (normal form) is the same regardless of how the computation proceeds.

Proving that a relation is confluent is typically difficult. However, we can easily establish the following weaker condition:

Proposition pty.4 (Weak Church-Rosser Property). *If $N \to N_1$ and $N \to N_2$ then there is a term N' such that $N_1 \twoheadrightarrow N'$ and $N_2 \twoheadrightarrow N'$.*

Proof. The two terms N_1 and N_2 result from N by replacing the redex M_1 or M_2 by its reductum, respectively. The redexes M_1 and M_2 are subterms of N, and so cannot overlap. This means that either one is a subterm of the other, or they occur in different non-overlapping places in N. Consider the latter case: N is of the form $N(M_1, M_2)$. Replacing M_1 by its reductum M_1' results in N_1 which is $N(M_1', M_2)$, and replacing M_2 by its reductum M_2' results in N_2 which is $N(M_1, M_2')$. Both reduce to $N(M_1', M_2')$. For the other case, suppose M_2 is a sub-term of M_1 (the other case is symmetric) and distinguish cases according to what kind of redex M_1 is. E.g., if $M_1 \equiv \pi_1(\langle O_1, O_2\rangle)$ it reduces to O_1. If M_2 is a subterm of O_1, then converting M_2 results in O_1'. So converting M_1 first and then M_2 results in O_1'. But converting M_2 first results in $\pi_1(\langle O_1', O_2\rangle)$ and this reduces also to O_2. □

Lemma pty.5 (Newman's Lemma). *If $\twoheadrightarrow$ is strongly normalizing and has the weak Church-Rosser property, it is confluent.*

Proof. Since $\twoheadrightarrow$ is strongly normalizing, any reduction sequence results in a normal form. Normal forms are unique iff $\twoheadrightarrow$ is confluent. So suppose some term N has two distinct normal forms N' and N'', the result of reduction sequences

$$N = N_1' \to N_2' \to \ldots \to N_k' = N' \text{ and}$$
$$N = N_1'' \to N_2'' \to \ldots \to N_l'' = N''$$

(The reduction sequence must have length > 0 since otherwise N would already be in normal form.)

If $N_1' = N_1''$ then it has two distinct normal forms (N' and N''). If $N_1' \neq N_1''$ then by weak Church-Rosser there is some N''' such that $N_1' \twoheadrightarrow N'''$ and $N_1'' \twoheadrightarrow N'''$. Since $N' \neq N''$, either $N''' \neq N'$ or $N''' \neq N''$. Consequently, either N_1' or N_1'' has two distinct normal forms. We've shown that if N has two distinct normal forms, there is an N_1 such that $N \to N_1$ and N_1 has two distinct normal forms. Obviously we can keep going and produce $N \to N_1 \to N_2 \to \ldots$, but this is impossible because $\to$ is strongly normalizing. □

Photo Credits

Bibliography