The Church - Rosser Property and a result in Combinatory Logic

A Thesis submitted for the Degree of Doctor of Philosophy in the Faculty of Science, in the University of Newcastle upon Tyne,

by

James Roger Hindley, M. Sc. (Belfast)

July, 1964.

CONTENTS

Not in this copy.

Proof that strong reduction cannot be finitely axiomatized.

Superceded by much simpler proof.

Material from Chs 1-4 published in:

Hindley, J.R. { "An abstract form of the Church-Rosser Theorem, I", J. Symbolic Logic 34 (1969), 545-560.
"An abstract Church-Rosser theorem, II: applications" J.S.L. 39 (1974), 1-21.

Result of Ch. 6 published with simpler proof, in "Axioms for strong reduction in combinatory logic", J.S.L. 32 (1967), 224-236.

Summary of Thesis

submitted in August 1964 for the degree of Ph.D. in the University of Newcastle upon Tyne, by James Roger Hindley.

"The Church - Rosser Property

and a result in Combinatory Logic".

In "Some Properties of Conversion" (Transactions of the American Math. Soc., 1936), A. Church and J. B. Rosser showed that any two inter-convertible λ-formulae could both be reduced to the same formula: this is called the Church-Rosser Theorem. Abstract forms of it, which unfortunately did not cover the original result as a special case, were later proved by M. H. A. Newman and H. B. Curry. Curry and Feys in their book "Combinatory Logic" proved the Theorem and extended it to a new kind of conversion.

To introduce the abstract "Church-Rosser Property" the following notation is used. Suppose r is any binary relation:

"X r Y" means that X bears the relation r to Y.

"$X \geqslant_r Y$" means that either $X = Y$ or there is a sequence $X_0, \ldots, X_n$ such that $X = X_0$, $X_0 r X_1$, ..., $X_{n-1} r X_n$ and $X_n = Y$.

"$X \sim_r Y$" means that either $X = Y$ or there is a sequence $X_0, \ldots, X_n$ such that $X = X_0$, $X_0 r X_1$ or $X_1 r X_0$, ..., $X_{n-1} r X_n$ or $X_n r X_{n-1}$, and $X_n = Y$.

The relations $\geqslant_r$ and $\sim_r$ correspond respectively to inter-convertibility and reducibility of λ-formulae.

A relation r has the Church-Rosser Property if $X \sim_r Y$ implies that there exists Z with $X \geqslant_r Z$ and $Y \geqslant_r Z$.

In the first two chapters of this thesis, abstract theorems are proved which do cover the original Church-Rosser Theorem as a special case, and give a simple way of extending it to the new conversion mentioned before.

A much simpler but weaker abstract result, due to Newman, is applied in the later chapters to give new proofs of a simple consistency lemma in recursive-function theory and a lemma in R. Harrop's paper "A Relativization Procedure for Propositional Calculi" (Proc. London Math. Soc., 1964).

Out of an attempt to apply my abstract theorem directly to the "strong reduction" relation (see the book "Combinatory Logic") arose a proof that this relation cannot be finitely axiomatized, which proof is included as the last chapter of the thesis.

I am very grateful to Dr. R. Harrop of the University of Newcastle upon Tyne for his advice and encouragement, also to the Northern Ireland Ministry of Education who financed most of the work with a Research Studentship.

INTRODUCTION

When they were developing their system of λ-conversion in the nineteen-thirties, Church, Kleene and Rosser needed to prove that any two interconvertible λ-formulae represented the same function. (See [6] or the end of this chapter for details.) They first did this by setting up a correspondence between λ-conversion and combinatory logic, and using consistency results from H. B. Curry's paper "Grundlagen der Kombinatorischen Logik" [17]. However they soon found a more direct way, part of which involved defining a reduction-process and proving that any two interconvertible λ-formulae could both be reduced to the same formula. This result has been called the Church-Rosser Theorem for λ-conversion, and I will be dealing here with more general forms of this theorem, which can be applied to other conversion relations, though the λ-system is by far the most substantial application.

To introduce the Church-Rosser property in its abstract form needs a little notation:

If r is any binary relation,

" $X\ r\ Y$ " means that X bears the relation r to Y,

" $X \sim_r Y$ " means that $X\ r\ Y$ or $Y\ r\ X$,

" $X \geqslant_r Y$ " means that either X is identical with Y (written " $X = Y$ " for short)

or there is a finite sequence $X_0, \ldots, X_n$ such that $X = X_0$, $X_0\ r\ X_1$, ... , $X_{n-1}\ r\ X_n$ and $X_n = Y$.

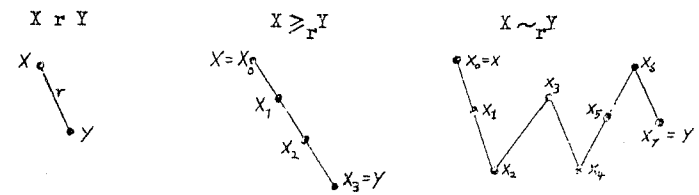
(The relation $\geqslant_r$ corresponds to the reduction-process mentioned before.)

" $X \sim_r Y$ " means that either $X = Y$

or there is a finite sequence $X_0, \ldots, X_n$ such that $X = X_0$, $X_0 \sim_r X_1$, ... , $X_{n-1} \sim_r X_n$, and $X_n = Y$.

($\sim_r$ corresponds to interconvertibility.)

These relations can be represented by diagrams, for example:

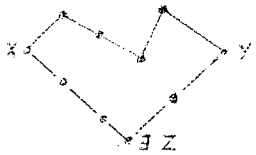


In the third diagram, $X_0\ r\ X_1$, $X_1\ r\ X_2$, $X_3\ r\ X_2$, $X_3\ r\ X_4$, etc.

A relation r has the <u>Church-Rosser Property</u> if and only if

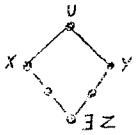
(CR) Whenever $X \sim_r Y$, there exists Z such that $X \geqslant_r Z$ and $Y \geqslant_r Z$.

For example:



All the known proofs of this property begin by proving some form of the special case

(D) Whenever $U \; r \; X$ and $U \; r \; Y$, there exists Z such that $X \geqslant_r Z$ and $Y \geqslant_r Z$.



Consequently the first two chapters of this thesis will deal with the connections between (CR) and various forms of (D) for as general a relation "r" as possible. Their results will be applied in Chapter 4 to give a new proof of the Church-Rosser Theorem for λ-conversion. In Chapter 5, a few other simpler applications will be discussed, including a consistency lemma in recursive function theory. In these simpler applications the results are not new and the proof of (D) is the main step, the step from (D) to (CR) being almost trivial. Note (D) $\not\Rightarrow$ (CR)

While trying unsuccessfully to apply this theory to combinatory logic I managed to answer partially a question posed by Curry and Feys in their book "Combinatory Logic", so this result is included as Chapter 6 of the thesis.

All results which are not mine will have their sources mentioned.

I am very grateful to Dr. R. Harrop of the University of Newcastle upon Tyne for his help and encouragement during the work for this thesis, and to the Northern Ireland Ministry of Education for financing most of it. I also wish to thank Miss K. Hedworth for duplicating the thesis, and D. E. Schroer for sending me part of his thesis [3].

A note on λ-conversion

To help the reader get the feel of the work, I will describe λ-conversion informally here and state the results of Church and Rosser, though most of this section will be done more rigorously later on.

Definition 0·1

λ-formulae are defined inductively as follows:

(i) There is an infinite (recursive) list of symbols called "variables" which, together with some "constants" (perhaps none), all are λ-formulae.

(ii) If X and Y are λ-formulae, then (XY) is a λ-formula. (Sometimes (XY) is written as "(X Y)"; the space between "X" and "Y" will be varied to make formulae more readable.)

(iii) If x is a variable and X is a λ-formula, then (λx X) is a λ-formula.

The phrase "defined inductively" means that the only λ-formulae are those obtained from the variables and constants by a finite number of applications of rules (ii) and (iii). In other words, an object X is a λ-formula if and only if the statement "X is a λ-formula" can be deduced from (i), by (ii) and (iii) used as rules of inference. For example, if x and y are variables, then

(λx x), (λy (λx (xy))) and (λx (λx (xy))) are λ-formulae.

Corresponding to each inductive definition is a method of proof by induction, on the steps used in the definition, which can be reduced

to induction on the natural numbers.

In the usual interpretations each λ-formula represents a function of some sort; the variables range over functions, and (XY) represents the value of the function X at the argument Y. (λx Z) represents the function whose value at x is Z; for instance, (λx x) represents the identity function. However, this thesis is not concerned with interpreting the λ-systems, but only with their formal properties — the "grammar" of the λ-language.

Capital letters X, Y, Z, M and N denote λ-formulae in this section and small letters x, y, z denote mutually distinct variables.

Definition 0·2 "Occurs"

(i) Any λ-formula occurs in itself;

(ii) If (XY) occurs in Z, then X and Y both occur in Z, and if (λx X) occurs in Z, then X occurs in Z.

By this definition, x does not occur in (λx (yz)) .

The phrase "An occurrence of X in a formula Y" has a fairly obvious intuitive meaning, but the formal definition is rather complicated and is left to Chapter 3. For example there are two occurrences of x in ((λz x) x), one in (λx (xz)) and none in (λx (yz)).

A variable x is bound in a formula Y if and only if a formula of the form (λx X) occurs in Y; any occurrences of x in (λx X) are said to be bound occurrences, while any occurrences not in

formulae of this form are free. In $((\lambda x\ (xy))\ x)$ for example, the left-hand "x" is not an occurrence at all, the middle "x" is a bound occurrence and the right-hand "x" is free. Also x is bound in $(\lambda x\ (yz))$, even though there are no occurrences of x here.

Substitution of a formula for a variable

Intuitively, substituting a formula N for a variable x occurring in X means replacing each occurrence of x by N, but this could cause trouble if not done carefully. For example $(\lambda y\ x)$ and $(\lambda z\ x)$ have the same interpretation (the function whose value is always x) yet simply substituting y for x in each formula gives $(\lambda y\ y)$ and $(\lambda z\ y)$, which have different interpretations. This difficulty led Curry in [5] to modify the definition of substitution — see clause (iiic) below.

Definition 0·3 **Substitution**

If N is a λ-formula and x is a variable;

(i) (a) $[N/x]\,x = N$,

(b) $[N/x]\,y = y$ for any variable or constant y distinct from x;

(ii) $[N/x](XY) = \left([N/x]X\ \ [N/x]Y\right)$ for all λ-formulae X and Y;

(iii) (a) $[N/x](\lambda x\ X) = (\lambda x\ X)$ for all λ-formulae X;

(b) $[N/x](\lambda y\ X) = \left(\lambda y\ [N/x]X\right)$ if $y \neq x$, and <u>either</u> y does not occur free in N <u>or</u> x does not occur free in X;

(c) $[N/x](\lambda y\ X) = \left(\lambda z\ [N/x][z/y]X\right)$ if $y \neq x$, y occurs free in N and x occurs free in X,

z being the first variable in the list given in Def. 0·1 which does not occur free in N or X.

<u>Note</u> Definition 0·3 is an inductive definition, but instead of introducing a new predicate as did Defs. 0·1 and 0·2, it is an algorithm for calculating $[N/x]X$ for all N, x and X: the fact that it does give a unique value for $[N/x]X$ is easily proved by induction on the definition of X.

$[N/x]X$ is the result of first altering any variables bound in X which are also free in N, and then replacing all free occurrences of x in X by occurrences of N. In this way no variables occurring free in N become bound in $[N/x]X$.

Example: $[y/x](\lambda y\ x) = \left(\lambda z\ [y/x][z/y]x\right)$ by (iiic) of Def. 0·3,

$= (\lambda z\ y)$ by (ib) and (ia).

Conversion of λ-formulae

Definition 0·4 **The relation α**

X bears the relation α to Y if and only if Y is the result of replacing an occurrence in X of a formula of the form $(\lambda x\ M)$ by $\left(\lambda y\ [y/x]M\right)$, where y is any variable not occurring free in M.

For example; in the notation defined earlier,

$(\lambda x\ (zx))\ \alpha\ (\lambda y\ (zy))$ since $[{}^{y}/_{x}](zx) = (zy)$

but not $(\lambda x\ (zx))\ \alpha\ (\lambda z\ (zz))$ because z occurs free in (zx).

The relations $\geqslant_\alpha$ and $\sim_\alpha$ are defined as before, $\sim_\alpha$ being called "α-equivalence" as it is transitive, reflexive and symmetric. α-equivalent formulae are always given the same interpretation in applications of λ-conversion.

<u>Definition 0·5</u> <u>The relation β</u>

X bears the relation β to Y if and only if Y is the result of replacing an occurrence in X of some formula of the form $((\lambda x\ M)\ N)$ by $[{}^{N}/_{x}]M$.

For example; $((\lambda x\ (zx))\ y)\ \beta\ (zy)$.

The relation αβ is defined by " X αβ Y if and only if X α Y or X β Y", and $\geqslant_{\alpha\beta}$ and $\sim_{\alpha\beta}$ are defined as before.

The replacement of a part of X by another formula according to Definition 0·4 (or 0·5) is called an α (or β) <u>contraction</u> of X, and a succession of contractions is a <u>reduction</u>. The reverse of a contraction $\{$e.g. replacing $[{}^{N}/_{x}]M$ by $((\lambda x\ M)\ N)\}$ is called an <u>expansion</u>. An α or β or αβ <u>conversion</u> is a succession of contractions and expansions; hence X is αβ-convertible to Y if and only if $X \sim_{\alpha\beta} Y$. The term "λ-conversion" is used to cover all the various sorts of conversions, including some which will be

defined in Chapter 4.

The original system of Church and Rosser consisted essentially of the relation α and a restricted form of β in which M had to contain some free occurrences of x. Actually the restriction was made by allowing $(\lambda x\ Y)$ to be a λ-formula only when x occurred free in Y. With this restriction on formulae and β-contraction they proved the following theorems. (see [7], page 479)

<u>Theorem 1</u>

Whenever $X \sim_{\alpha\beta} Y$, there must exist Z such that $X \geqslant_{\alpha\beta} Z$ and $Y \geqslant_{\alpha\beta} Z$.

<u>Corollary</u>

If $X \sim_{\alpha\beta} Y_1$ and $X \sim_{\alpha\beta} Y_2$ with no formulae of the form $((\lambda x\ M)\ N)$ occurring in Y_1 or Y_2, then $Y_1 \sim_\alpha Y_2$.

(Such formulae as Y_1 and Y_2 are called <u>β-normal forms</u> of X.)

<u>Theorem 2</u>

If X has a β-normal form, Y, then a number m can effectively be found such that any reduction starting with X will end at Y, or a formula Y' α-equivalent to Y, after at most m β-contractions.

<u>Corollary</u>

If X has a β-normal form, then so has any formula occurring in X.

The Corollary to Theorem 2 would be false if β-contraction were not restricted; for instance if $X = ((\lambda x\ y)\ N)$ with $y \neq x$, and N had no β-normal form, X would have the normal form y because $X\ \beta\ y$. (Such formulae N do exist.) This was one of Church's main reasons for restricting β, as in his interpretation formulae without normal forms were meaningless. However Theorem 1 still holds true without the restriction on β, and I shall not be concerned with Theorem 2; indeed my results could not be adapted to prove it.

In Chapter 4 I shall prove the analogue of Theorem 1 for unrestricted β-contraction; the proof can be adapted to the restricted β-contraction, but for reasons of space I shall not do this.

CHAPTER 1

Properties (D) and (CR)

After a section on notation, some simple connections between the properties (D) and (CR) are investigated here, partly with a view to extending Church and Rosser's Theorem 1 to include a third kind of contraction which was invented later by Curry.

Notation

These abbreviations and remarks will apply throughout the thesis.

Symbol	Meaning
=	is identical with
⇒	implies
⇔	is logically equivalent to
iff	if and only if
∴	therefore
ε	is a member of (a set)
∅	the empty set

Symbol	Meaning
$\leqslant$	less than or equal to (said of integers)
$>$	greater than (said of integers)
for $i = m \ldots n$	for every integer i such that $m \leqslant i$ and $i \leqslant n$
$\exists X$:	there exists X such that
$\exists X_o \ldots X_n$:	there exist a non-negative integer n and a finite sequence $X_o, \ldots, X_n$ such that

The sequence whose members are $X_1, \ldots, X_n$ in that order will be denoted by "$(X_1, \ldots, X_n)$"; "$\{X_1, \ldots, X_n\}$" will denote the set whose members are $X_1, \ldots, X_n$ and unless stated otherwise, it will be assumed that such sets are indexed so that $i \neq j \Rightarrow X_i \neq X_j$. The meaning of "$\{X_1, \ldots, X_n\}$" is extended to be an empty set when $n = 0$.

When certain things denoted by symbols are said to be <u>distinct</u>, it is understood that no two of the symbols denote the same thing; e.g. it was said above that in $\{X_1, \ldots, X_n\}$ the subscripts will be chosen so that $X_1, \ldots, X_n$ are distinct.

The letters m,n,h,i,j,k will denote non-negative integers unless otherwise stated. As a sub- or superscript, zero is written "o", not "0".

No rigorous distinction will be made between the use and mention of symbols, and quotation marks will be used just whenever they seem natural. References to "Corollary 2·1", etc., always indicate the corollary of a lemma, not a theorem.

Unless otherwise stated, all the relations mentioned will be binary relations, and if r is any binary relation,

" $X \not r Y$ " means that X does not bear the relation r to Y,

" $X \underline{r} Y$ " means that $X\ r\ Y$ or $X = Y$,

" $X_o r X_1 r \ldots r X_n$ " means, if $1 \leqslant n$, that $X_{i-1} r X_i$ for $i = 1 \ldots n$ and is also taken to mean "$X_o = X_n$" when $n = 0$.

Similarly statements involving a variety of relations may be strung together, for instance "X r Y, Y = W and W r Z" may be shortened to "X r Y = W r Z".

Now the definitions from the introduction can be re-stated;

$X \geqslant_r Y$ iff $\exists X_o \ldots X_n$: $X = X_o r X_1 r \ldots r X_n = Y$

$X \sim_r Y$ iff $\exists X_o \ldots X_n$: $X = X_o \sim_{1r} X_1 \sim_{1r} \ldots \sim_{1r} X_n = Y$

— the "X = Y" clauses being included in the notation as the case when n = 0.

The relation $\geqslant_r$ is transitive and reflexive; $\sim_r$ is transitive, reflexive and symmetric. Also

$$X\ r\ Y \Rightarrow X\ \underline{r}\ Y \Rightarrow X \geqslant_r Y \Rightarrow X \sim_r Y .$$

Further, the relation $\geqslant_{\underline{r}}$ is the same as $\geqslant_r$: that is, if s is defined by "X s Y iff $X \geqslant_r Y$", then $X \geqslant_s Y \Leftrightarrow X \geqslant_r Y$. ($\sim_s$ is also the same as $\sim_r$ in this case.)

If r and s are any two relations, a new relation rs is defined by

$$X\ rs\ Y \text{ iff } X\ r\ Y \text{ or } X\ s\ Y .$$

$\geqslant_{rs}$, $\sim_{rs}$, etc. are defined as before. So $X \geqslant_r Y$ implies $X \geqslant_{rs} Y$ and $X \sim_r Y$ implies $X \sim_{rs} Y$. Similarly three or four relations can be combined.

A relation r has property (CR) iff

$$X \sim_r Y \Rightarrow \exists Z\colon\ X \geqslant_r Z \text{ and } Y \geqslant_r Z,$$

and r has property (D) iff

$$U\ r\ X \text{ and } U\ r\ Y \Rightarrow \exists Z\colon\ X \geqslant_r Z \text{ and } Y \geqslant_r Z.$$

If "(P)" denotes a property, "(P_r)" will often be used to denote the statement that r has property (P). For example the above two statements are (CR_r) and (D_r), and Church and Rosser's Theorem 1 asserted $(CR_{\alpha\beta})$. Certain special cases of (D) and some other properties will be denoted by superscripts; for example r has property (D^1) iff

$$(D^1_r)\colon\ U\ r\ X \text{ and } U\ r\ Y \Rightarrow \exists Z\colon\ X\ \underline{r}\ Z \text{ and } Y\ \underline{r}\ Z.$$

A list of relations' properties used in Chapters 1 and 2 is printed at the end of the thesis for easy reference.

Throughout the thesis the concepts of set, member, sequence, function, and other notions which should be familiar to most mathematicians, are taken for granted.

The first result simplifies (CR).

<u>Lemma 1·1</u>

For any relation r, the following three properties are equivalent:

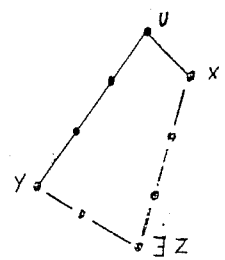
$$(G_r)\colon\ U\ r\ X \text{ and } U \geqslant_r Y \Rightarrow \exists Z\colon\ X \geqslant_r Z \text{ and } Y \geqslant_r Z,$$

$$(B_r)\colon\ U \geqslant_r X \text{ and } U \geqslant_r Y \Rightarrow \exists Z\colon\ X \geqslant_r Z \text{ and } Y \geqslant_r Z,$$

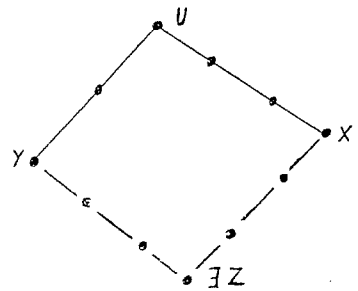
$$(CR_r)\colon\ X \sim_r Y \Rightarrow \exists Z\colon\ X \geqslant_r Z \text{ and } Y \geqslant_r Z.$$

Diagrams:

(G)



(B)



<u>Proof</u>:

$(CR_r) \Rightarrow (B_r) \Rightarrow (G_r)$, because (G_r) is a special case of (B_r) which is a special case of (CR_r). It remains to prove $(G_r) \Rightarrow (CR_r)$. By definition, $X \sim_r Y$ iff $\exists X_0 \ldots X_n\colon\ X = X_0 \sim_{1r} X_1 \sim_{1r} \cdots \sim_{1r} X_n = Y$, so it is sufficient to prove by induction on n that if (G_r) is true, then for $0 \leq n$,

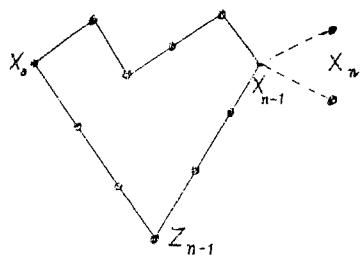
$$X_0 \sim_{1r} X_1 \sim_{1r} \cdots \sim_{1r} X_n \Rightarrow \exists Z_n\colon\ X_0 \geqslant_r Z_n \text{ and } X_n \geqslant_r Z_n.$$

<u>Basis</u>: When $n = 0$, that is $X_n = X_o$: choose $Z_o = X_o$.

<u>Induction step</u>: When $n > 0$ and Z_{n-1} exists with $X_o \geqslant_r Z_{n-1}$ and $X_{n-1} \geqslant_r Z_{n-1}$:

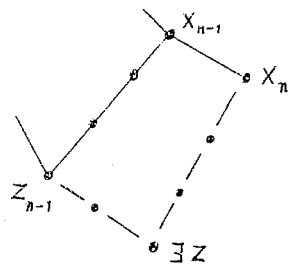
Either $X_n \, r \, X_{n-1}$

or $X_{n-1} \, r \, X_n$.



If $X_n \, r \, X_{n-1}$ then $X_n \geqslant_r Z_{n-1}$ by the transitivity of $\geqslant_r$, and Z_n may be chosen equal to Z_{n-1}.

If $X_{n-1} \, r \, X_n$, use (G_r) with "U", "X" and "Y" being X_{n-1}, X_n and Z_{n-1} respectively, to get Z such that $X_n \geqslant_r Z$ and $Z_{n-1} \geqslant_r Z$.



$X_o \geqslant_r Z$, because $X_o \geqslant_r Z_{n-1}$. Choose $Z_n = Z$, completing the induction.

This proof was suggested by Curry in [2] and is

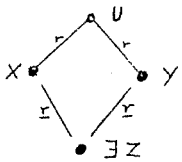
constructive (as are all proofs in this thesis) in the sense that it sets out a way of using the given existence - statement (G_r) to obtain Z.

To avoid repetition the equivalence of (G), (B) and (CR) will often be used without being explicitly mentioned.

<u>Theorem 1.1</u>

For any relation r; (D^1_r) implies (CR_r),

where (D^1_r) says that $U \, r \, X$ and $U \, r \, Y \Rightarrow \exists Z$: $X \, \underline{r} \, Z$ and $Y \, \underline{r} \, Z$.



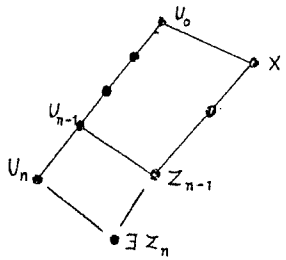
<u>Proof</u>:

It is enough to prove the following special form of (G_r) by induction on n:

$$U_o \, r \, X \text{ and } U_o \, r \, U_1 \, r \ldots r \, U_n \Rightarrow \exists Z_n: X \geqslant_r Z_n \text{ and } U_n \, \underline{r} \, Z_n .$$

When $n = 0$: choose $Z_o = X$.

When $n > 0$ and by the induction-hypothesis Z_{n-1} exists with $X \geqslant_r Z_{n-1}$ and $U_{n-1} \, \underline{r} \, Z_{n-1}$:



By definition, $U_{n-1} \underline{r} Z_{n-1} \Leftrightarrow U_{n-1} = Z_{n-1}$ or $U_{n-1}\, r\, Z_{n-1}$.

If $U_{n-1} = Z_{n-1}$, let Z_n be U_n. Then $U_n \geqslant_r Z_n$, and $X \geqslant_r Z_n$ because $X \geqslant_r Z_{n-1} = U_{n-1}\, r\, U_n = Z_n$.

If $U_{n-1}\, r\, Z_{n-1}$, apply $(D^1{}_r)$ to U_{n-1}, U_n and Z_{n-1} to obtain Z_n such that $U_n \underline{r} Z_n$ and $Z_{n-1} \underline{r} Z_n$. $X \geqslant_r Z_n$ because $X \geqslant_r Z_{n-1} \underline{r} Z_n$.

This is the simplest and most widely applied form of the Church-Rosser theorem, being first stated explicitly by M. H. A. Newman in [1]; it is this form which will be applied in the examples in Chapter 5. An example in [3] and another later in this chapter show that the unmodified property (D) does not imply (CR).

Combining two relations

Given two relations r and s, each having the Church-Rosser property, what extra conditions will ensure that the relation rs has the property too? Theorem 1·2 will show that (D^2), stated below, is sufficient, and after that theorem a few other possible conditions will be examined.

Lemma 1·2

Suppose r and s are any two relations.

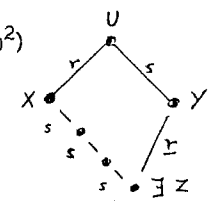
If

(D^2): $U\, r\, X$ and $U\, s\, Y \Rightarrow \exists Z$: $X \geqslant_s Z$ and $Y \underline{r} Z$

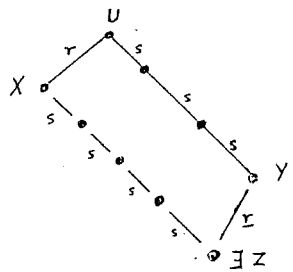
then

$U\, r\, X$ and $U \geqslant_s Y \Rightarrow \exists Z$: $X \geqslant_s Z$ and $Y \underline{r} Z$.

(D^2)



Conclusion



Proof:

It is enough to prove that

$U_o \; r \; X$ and $U_o s \; U_1 s \; \ldots \; s \; U_n \quad \Rightarrow \quad \exists Z_n$: $X \geqslant_s Z_n$ and $U_n \; \underline{r} \; Z_n$

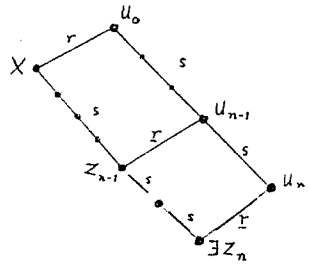
by induction on n.

When n = 0: let Z_o be X.

When $n > 0$ and Z_{n-1} exists with $X \geqslant_s Z_{n-1}$ and $U_{n-1} \; \underline{r} \; Z_{n-1}$:

Either $U_{n-1} = Z_{n-1}$

or $U_{n-1} \; r \; Z_{n-1}$.



If $U_{n-1} = Z_{n-1}$, let Z_n be U_n ; hence $X \geqslant_s Z_{n-1} = U_{n-1} \; s \; U_n = Z_n$, and so $X \geqslant_s Z_n$.

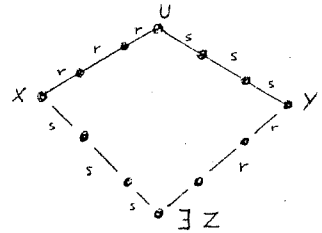
If $U_{n-1} \; r \; Z_{n-1}$, apply (D^2) with "U", "X" and "Y" being U_{n-1}, Z_{n-1} and U_n respectively, to get Z_n such that $U_n \; \underline{r} \; Z_n$ and $Z_{n-1} \geqslant_s Z_n$.

Hence $X \geqslant_s Z_n$.

By the way, putting s = r, Lemma 1·2 implies Theorem 1·1.

Lemma 1·3

(D^2) implies that $\quad U \geqslant_r X$ and $U \geqslant_s Y \quad \Rightarrow \quad \exists Z$: $X \geqslant_s Z$ and $Y \geqslant_r Z$.



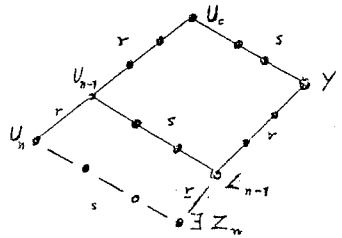
Proof:

It is enough to prove by induction on n that

$U_o r \; U_1 r \; \ldots \; r \; U_n$ and $U_o \geqslant_s Y \quad \Rightarrow \quad \exists Z_n$: $U_n \geqslant_s Z_n$ and $Y \geqslant_r Z_n$.

When n = 0: let Z_o be Y_o.

When $n > 0$ and $U_{n-1} \geqslant_s Z_{n-1}$ and $Y \geqslant_r Z_{n-1}$: applying Lemma 1·2 with "U", "X" and "Y" being U_{n-1}, U_n and Z_{n-1} respectively gives Z_n such that $U_n \geqslant_s Z_n$ and $Z_{n-1} \; \underline{r} \; Z_n$. Hence $Y \geqslant_r Z_n$, as required.



Theorem 1·2

If r and s are any relations, each having the Church- Rosser property, and (D^2) is true, then the relation rs has the Church-Rosser property. (In short: (CR_r), (CR_s) and (D^2) imply (CR_{rs}).)

Proof:

Since $U_o rs\ X \Leftrightarrow U_o r\ X$ or $U_o s\ X$, (G_{rs}) will follow from a proof by induction on n that

(i): $U_o s\ X$ and $U_o rs\ U_1 rs \ldots rs\ U_n \Rightarrow \exists Z_n : X \geqslant_{rs} Z_n$ and $U_n \geqslant_s Z_n$

(ii): $U_o r\ X$ and " " " $\Rightarrow$ " " and $U_n \geqslant_r Z_n$.

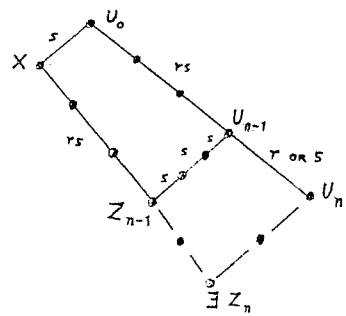
Proof of (i)

When n = 0: let Z_o be X.

When $n > 0$ and $X \geqslant_{rs} Z_{n-1}$ and $U_{n-1} \geqslant_s Z_{n-1}$:

Either $U_{n-1}\ s\ U_n$

or $U_{n-1}\ r\ U_n$.



If $U_{n-1}\ s\ U_n$, apply (B_s) to U_{n-1}, Z_{n-1} and U_n to get Z_n such that $U_n \geqslant_s Z_n$ and $Z_{n-1} \geqslant_s Z_n$; hence $X \geqslant_{rs} Z_n$.

If $U_{n-1} r\ U_n$, apply Lemma 1·3 to U_{n-1}, U_n and Z_{n-1}, to get Z_n such that $U_n \geqslant_s Z_n$ and $Z_{n-1} \geqslant_r Z_n$; hence $X \geqslant_{rs} Z_n$, ending the proof of (i).

As the conclusion of Lemma 1·3 is symmetrical in r and s,

the proof of (ii) can be got from that of (i) by interchanging "r" and "s".

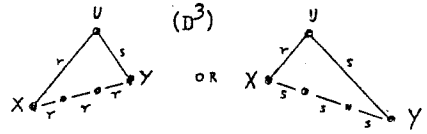
This is the theorem that is applied to extend (CR) to Curry's system of λ-conversion. (See Chapter 4)

Proving (CR) from (D) is rather like doing a jigsaw-puzzle with instances of (D) as the pieces. In Theorem 1·2 the pieces are of three kinds; one sort (unspecified) allows (CR_r) to be proved, another sort allows (CR_s), and the third is (D^2), which is a kind of "connecting-piece". What other possible connecting-pieces could there be? If the "r" in (D^2) is weakened to "$\geqslant_r$", the resulting condition does not give (CR_{rs}) from (CR_r) and (CR_s); in fact

(D^3): $U\ r\ X$ and $U\ s\ Y \Rightarrow Y \geqslant_r X$ or $X \geqslant_s Y$

is not sufficient, as the example on page 25 shows.

(D^3)

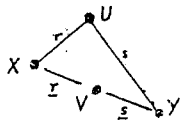


An example in the Appendix shows that

(D^4): $U\ r\ X$ and $U\ s\ Y \Rightarrow \exists V: X\ \underline{r}\ V\ \underline{s}\ Y$

is also insufficient.

(D^4):



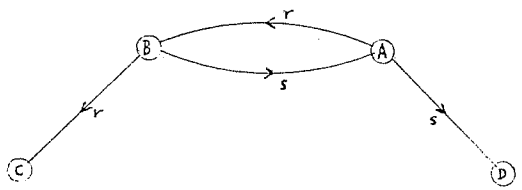
(D^3) and (D^4) are not even sufficient when (CR_r) and (CR_s) are strengthened to $(D^1{}_r)$ and $(D^1{}_s)$, but if "r" and "s" are interchanged in the conclusion of (D^4), the condition so formed, together with $(D^1{}_r)$ and $(D^1{}_s)$, implies (CR_{rs}). This follows from Theorem 1·3 in the Appendix.

It may be interesting to see if there is a simple way of telling whether or not a form of (D) can act as a connecting-piece, but I have not looked into the question.

<u>A system satisfying $(D^1{}_r)$, $(D^1{}_s)$ and (D^3) but not (CR_{rs}).</u>

This is a simplification of an example in Schroer's PhD thesis. Schroer attributes his example to Rosser.

If A, B, C and D are four distinct objects; define the relation r by $\left\{\begin{matrix} A\ r\ B \\ B\ r\ C \end{matrix}\right\}$ and the relation s by $\left\{\begin{matrix} B\ s\ A \\ A\ s\ D \end{matrix}\right\}$.



$$U\ r\ X \text{ and } U\ r\ Y \quad \Rightarrow \quad \begin{cases} \text{either } U = A \text{ and } X = Y = B \\ \text{or } U = B \text{ and } X = Y = C\ . \end{cases}$$

To prove $(D^1{}_r)$ in both these cases, choose $Z = X = Y$. Hence (CR_r) by Theorem 1·1. Similarly $(D^1{}_s)$ and (CR_s) are satisfied.

Also; $U\ r\ X$ and $U\ s\ Y$ $\Rightarrow$ $\begin{cases} \text{either } U = B,\ X = C \text{ and } Y = A \\ \text{or } U = A,\ X = B \text{ and } Y = D \end{cases}$

$\Rightarrow$ $Y \geqslant_r X$ or $X \geqslant_s Y$,

which proves (D^3).

However (CR_{rs}) is false, because $C \sim_{rs} D$ yet there is no Z with $C \geqslant_{rs} Z$ and $D \geqslant_{rs} Z$.

This example also shows that the original unmodified form of (D) does not imply (CR), since from the above,

$$U\ rs\ X \text{ and } U\ rs\ Y \quad \Rightarrow \quad \exists Z\colon\ X \geqslant_{rs} Z \text{ and } Y \geqslant_{rs} Z,$$

yet (CR_{rs}) is not satisfied.

Appendix to Chapter 1

Two minor results mentioned in the Chapter.

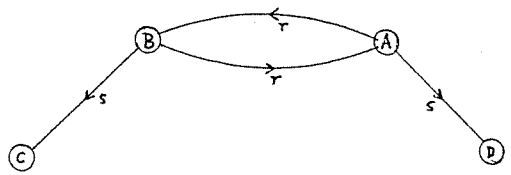
The property (D^4) says that

$$U\ r\ X \text{ and } U\ s\ Y \quad \Rightarrow \quad \exists V:\ X\ \underline{r}\ V\ \underline{s}\ Y.$$

The following system satisfies $(D^1{}_r)$, $(D^1{}_s)$ and (D^4) but not (CR_{rs}).

If A, B, C and D are four distinct objects,

define r by $\begin{Bmatrix} A\ r\ B \\ B\ r\ A \end{Bmatrix}$ and s by $\begin{Bmatrix} B\ s\ C \\ A\ s\ D \end{Bmatrix}$.



$$U\ r\ X \text{ and } U\ r\ Y \quad \Rightarrow \quad \left\{\begin{array}{ll} & U = A \text{ and } X = Y = B \\ \text{or} & U = B \text{ and } X = Y = A\ , \end{array}\right\} \text{ giving } (D^1{}_r)$$

$$U\ s\ X \text{ and } U\ s\ Y \quad \Rightarrow \quad \left\{\begin{array}{ll} & U = A \text{ and } X = Y = D \\ \text{or} & U = B \text{ and } X = Y = C, \end{array}\right\} \text{ giving } (D^1{}_s)$$

$$U\ r\ X \text{ and } U\ s\ Y \quad \Rightarrow \quad \left\{\begin{array}{ll} \text{either} & U = A,\ X = B \text{ and } Y = D \\ \text{or} & U = B,\ X = A \text{ and } Y = C\ , \end{array}\right.$$

$$= \quad \left\{\begin{array}{l} X\ r\ A\ s\ Y \\ \text{or } X\ r\ B\ s\ Y, \end{array}\right.$$

giving (D^4).

Yet $C \sim_{rs} D$ without there being Z such that $C \geqslant_{rs} Z$ and $D \geqslant_{rs} Z$.

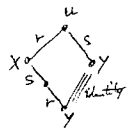
The theorem below has no applications of which I know, beyond the remark on page 25 about interchanging "r" and "s" in the conclusion of (D^4).

Theorem 1·3

If r and s are relations; $(D^1{}_r)$ and $(D^1{}_s)$, together with

(D^5): $\quad U\ r\ X \text{ and } U\ s\ Y \quad \Rightarrow \quad \exists V:\ X\ \underline{s}\ V\ \underline{r}\ Y$

imply (CR_{rs}).



Proof:

As in Theorem 1·2, it is enough to prove

(i): $\quad U_o r\ X \text{ and } U_o rs\ U_1 rs \ldots rs\ U_n \quad \Rightarrow \quad \exists Z_n:\ X \geqslant_{rs} Z_n \text{ and } U_n \geqslant_{rs} Z_n$

(ii): $\quad U_o s\ X \text{ and } \quad '' \quad '' \quad '' \quad = \quad '' \quad '' \quad '' \quad '' \quad ,$

$$\text{Now } U\ r\ X \text{ and } U\ rs\ Y \quad \Rightarrow \quad \left\{\begin{array}{l} \text{either } U\ r\ X \text{ and } U\ r\ Y \\ \text{or } U\ r\ X \text{ and } U\ s\ Y \end{array}\right.$$

$$\Rightarrow \begin{cases} \text{either } \exists Z\text{: } X \ \underline{r}\ Z \text{ and } Y \ \underline{r}\ Z, \text{ by } (D^1_r) \\ \text{or } \exists V\text{: } X \ \underline{s}\ V \ \underline{r}\ Y \qquad \text{by } (D^5) \end{cases}$$

$$\Rightarrow \begin{cases} \text{either } \exists Z\text{: } X \geqslant_{rs} Z \text{ and } Y \ \underline{r}\ Z \\ \text{or } X \geqslant_{rs} Y \end{cases}$$

$$\Rightarrow \exists Z\text{: } \begin{cases} \text{either } X \geqslant_{rs} Z \text{ and } Y \ \underline{r}\ Z \\ \text{or } X \geqslant_{rs} Z \text{ and } Y = Z \end{cases}$$

$$\Rightarrow \exists Z\text{: } X \geqslant_{rs} Z \text{ and } Y \ \underline{r}\ Z.$$

Thus (D^2), with "rs" instead of "s", is satisfied. Hence by Lemma 1·2,

$$U \ r\ X \text{ and } U \geqslant_{rs} Y \quad \Rightarrow \quad \exists Z\text{: } X \geqslant_{rs} Z \text{ and } Y \ \underline{r}\ Z,$$

which implies (i).

$$U \ s\ X \text{ and } U \ rs\ Y \quad \Rightarrow \begin{cases} \text{either } U \ s\ X \text{ and } U \ s\ Y \\ \text{or } U \ s\ X \text{ and } U \ r\ Y \end{cases}$$

$$\Rightarrow \begin{cases} \text{either } \exists Z\text{: } X \ \underline{s}\ Z \text{ and } Y \ \underline{s}\ Z, \text{ by } (D^1_s) \\ \text{or } \exists V\text{: } Y \ \underline{s}\ V \ \underline{r}\ X \qquad \text{by } (D^5) \end{cases}$$

$$\Rightarrow \exists Z, V\text{: } \begin{cases} \text{either } X \ \underline{s}\ Z \text{ and } Y \ \underline{s}\ V = Z \\ \text{or } X = Z \text{ and } Y \ \underline{s}\ V \ \underline{r}\ Z \end{cases}$$

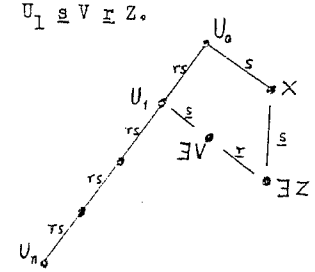
$$\Rightarrow \exists Z, V\text{: } X \ \underline{s}\ Z \text{ and } Y \ \underline{s}\ V \ \underline{r}\ Z.$$

Using this fact, (ii) will now be proved by induction on n:

When $n = 0$: choose $Z_0 = X$.

When $n > 0$: suppose $U_0 \ s\ X$ and $U_0 \ rs\ U_1 \ rs \ldots rs\ U_n$. Then by the above inference applied to U_0, X and U_1, there exist Z and V such

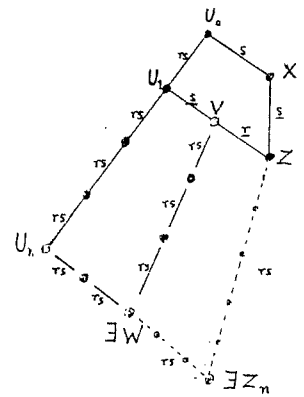
that $X \ \underline{s}\ Z$ and $U_1 \ \underline{s}\ V \ \underline{r}\ Z$.



Define W as follows:

If $U_1 = V$; let $W = U_n$. Then $V \geqslant_{rs} W$ and $U_n \geqslant_{rs} W$.

If $U_1 \ s\ V$; then, since also $U_1 \ rs\ U_2 \ rs \ldots rs\ U_n$, the induction-hypothesis may be applied to U_1, V and U_n to obtain W such that $V \geqslant_{rs} W$ and $U_n \geqslant_{rs} W$.



Now $V \ \underline{r}\ Z$:

If $V = Z$, choose Z_n to be W. Then $X \ \underline{s}\ Z = V \geqslant_{rs} W = Z_n$ and $U_n \geqslant_{rs} W = Z_n$, as required.

If $V\ r\ Z$; since $V \geqslant_{rs} W$, (i) can be applied to V, Z and W, giving Z_n such that $Z \geqslant_{rs} Z_n$ and $W \geqslant_{rs} Z_n$. Hence $X \geqslant_{rs} Z_n$ and $U_n \geqslant_{rs} Z_n$, completing the induction-step for (ii).

Actually Theorem 1·3 can be improved to show that $(D^1{}_s)$ and (CR_r) {not necessarily $(D^1{}_r)$}, together with

$$U\ r\ X \text{ and } U \underset{\subseteq}{s} Y \implies \exists Z,V:\ X\ \underline{s}\ V \geqslant_r Z \text{ and } Y \geqslant_r Z,$$

imply (CR_{rs}).

CHAPTER 2

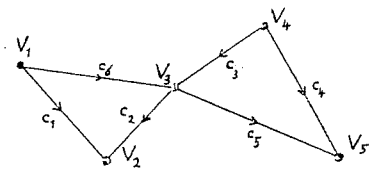
Reductions

Here the main purpose is to deduce (CR) in a system which covers $\alpha\beta$-conversion as a special case, though that part of the matter is left to Chapter 4. This deeper result is got by assuming a more complicated form of (D).

Diagrams of the kind that I used in Chapter 1 suggested to M. H. A. Newman that the Church-Rosser property could be given its most general form in topological language, as follows.

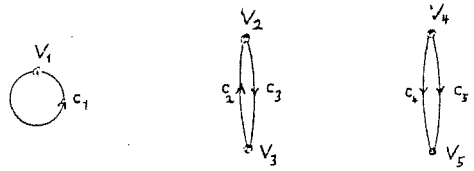
Informally speaking, a set of things called <u>vertices</u> is supposed to be linked together by <u>cells</u>, each cell running from one vertex, its <u>start</u>, to another vertex, its <u>end</u>. A cell may start and end at the same vertex, and not all the vertices need be linked together.

Example 1:



In Example 1, $V_1, \ldots, V_5$ are the vertices and $c_1, \ldots, c_6$ the cells, with arrows showing their directions; for example c_1 starts at V_1 and ends at V_2.

Example 2:



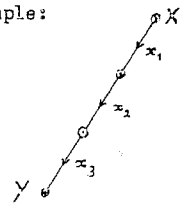
A system like these is called a <u>Reduction-complex</u>, and can be defined more rigorously as an ordered triple (C,V,f) in which C and V are sets whose members are called "cells" and "vertices" respectively, and f is a mapping from C to some of the ordered pairs of vertices. D. E. Schroer does this thoroughly in [3].

Any relation r generates a reduction-complex, obtained by defining a cell to run from X to Y if and only if X r Y. However not every reduction-complex is generated by a relation; for example the system above, in which c_4 and c_5 both run from V_4 to V_5, but are distinct cells.

(This example is due to Schroer, as is also much of the notation of this section.)

A <u>Reduction from X to Y</u> is a sequence of cells, say $(x_1,\ldots,x_n)$, such that the start of x_1 is X, the start of x_{i+1} is the end of x_i (for $i = 1\ldots n-1$) and the end of x_n is Y. The reduction is said to <u>start</u> at X, <u>end</u> at Y, and n is called its <u>length</u>. A reduction or cell starting at X will be said simply to be "<u>at X</u>".

Example:



The length of this reduction is 3.

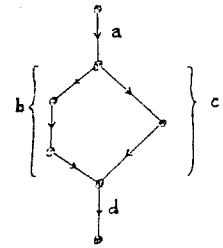
A <u>null</u> reduction is one consisting of no cells, though a starting-vertex is associated with it and it is said to end at the same vertex as it starts. Any null reduction will be denoted by "0", although a null reduction at one vertex is not the same as a null reduction at another vertex. The length of a null reduction is defined to be 0.

No distinction will be made between a cell and the reduction consisting of that cell alone, and reductions or cells which all start at the same vertex are called <u>co-initial</u>.

If b is the reduction $(x_1,\ldots,x_m)$, c is the reduction $(y_1,\ldots,y_n)$ and b ends at the start of c; b+c is defined as the reduction $(x_1,\ldots,x_m,y_1,\ldots,y_n)$. Also b+0 = b and 0+b = b by definition, for all reductions, b. Then if either exists, (a+b)+c = a+(b+c) {but not in general a+b = b+a!} and the reduction $(x_1,\ldots,x_n)$ can be written as "$x_1+\ldots+x_n$".

For reductions b and c; "$b \simeq c$" means that b and c are co-initial and both end at the same vertex. If $b \simeq c$, then $a+b \simeq a+c$ and $b+d \simeq c+d$, for all a, d.

Example: Here, $b \simeq c$.



For any reduction, $b = x_1+\ldots+x_n$, define $b_0 = 0$, and b_k, the <u>k-th stage</u> in the reduction, to be $x_1+\ldots+x_k$, for $k = 1\ldots n$.

Whenever a set of cells is mentioned it will be assumed that its members are co-initial.

In this chapter,

X, Y, Z, U, V, W denote vertices,

x, y, z, u, v, w denote cells,

a, b, c, d, e denote reductions, and

α, β denote sets of co-initial cells.

The conventions on page 13 are modified to allow "$\{\alpha_1,\ldots,\alpha_n\}$" to denote the union of $\alpha_1, \ldots, \alpha_n$, not a set of n sets.

The subject of this chapter is the relation r defined by "X r Y iff there is a cell running from X to Y", in a given reduction-complex which is described in the following pages. For convenience the subscripts "$_r$" will be omitted from "$\geqslant_r$", "$\sim_r$" and "$\underset{r}{\sim}$", etc. Obviously $X \geqslant Y$ if and only if there is a reduction from X to Y; "$X \geqslant Y$ by b" means that b is a reduction from X to Y.

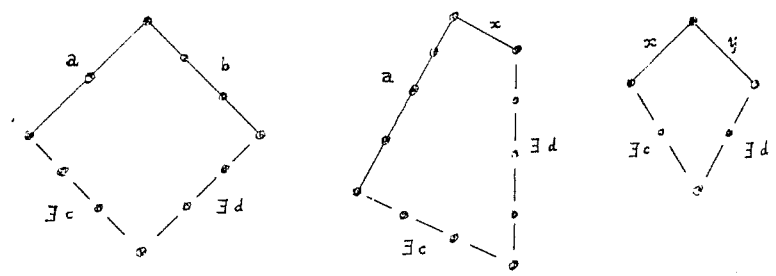
For this relation r; (B_r), (G_r) and (D_r) become

(B): a and b co-initial $\Longrightarrow$ $\exists c,d$: $a+c \simeq b+d$,

(G): a and x co-initial $\Longrightarrow$ $\exists c,d$: $a+c \simeq x+d$,

(D): x and y co-initial $\Longrightarrow$ $\exists c,d$: $x+c \simeq y+d$.

(B) (G) (D)



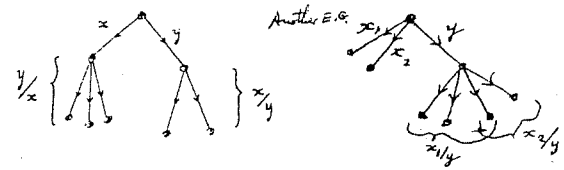
The complicated form of (D) mentioned earlier involves a special kind of reduction called an "MCD", whose definition needs the following concepts.

For every pair x, y of co-initial cells, there is assumed to be a set, $^x/_y$, possibly empty or infinite, of cells all starting at

(i.e. to be given as part of the definition of whatever reduction complex we are studying)

the end of y. These are called the Residuals of x with respect to y.

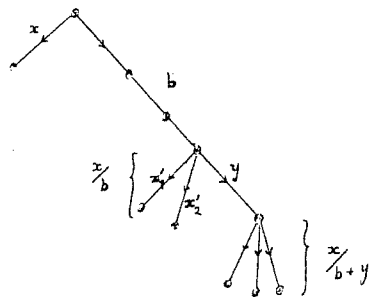
Example:



The set, $^x/_b$, of residuals of x after a reduction, b, co-initial with x, is defined inductively by

$$\begin{cases} {}^x/_0 \text{ contains only } x, \\ {}^x/_{b+y} \text{ is the union of all } {}^{x'}/_y \text{ , for all } x' \in {}^x/_b. \end{cases}$$

Example:



If α is a set of cells co-initial with b; $^\alpha/_b$ is the union of all $^x/_b$, for all $x \in \alpha$. If $\alpha = \emptyset$; $^\alpha/_b$ is empty too. From these definitions, $^x/_{a+b} = (^x/_a)/_b$ for any reduction a+b. Often "$^x/_y$" or "$^x/_b$" will be used to denote the individual residuals as well as the set of residuals, but the meaning will be clear from the context. Also "$^x/_b = z$" will mean that z is the sole member of $^x/_b$.

A development of a set α of cells is a reduction, b =

$= x_1+\ldots+x_n$, in which $x_i \in {}^{a}/_{b_{i-1}}$ for $i = 1\ldots n$. If $a = \emptyset$, its development is a null reduction. The development b is <u>complete</u> (and called a "C. D." of a) iff ${}^{a}/_{b} = \emptyset$.

For the given complex, there is assumed to be a relation $\subset$, which only holds among co-initial cells: in Chapter 4, cells will correspond roughly to replaceable parts of formulae like those in Definition 0·5, and the relation $\subset$ to that of one part being inside another.

"$x \not\subset y$" will be taken to mean that x and y are co-initial but not $x \subset y$.

"${}^{x}/_{z} \not\subset {}^{y}/_{z}$" means that there do not exist $x' \in {}^{x}/_{z}$ and $y' \in {}^{y}/_{z}$ with $x' \subset y'$, so it is true if ${}^{x}/_{z}$ or ${}^{y}/_{z}$ is empty.

<u>N. B.</u> "$\subset$" and "$\not\subset$" have nothing to do with the inclusion relation between <u>sets</u> of residuals, which relation will always be indicated by "—— is a subset of ——".

A cell y in a set β of cells is <u>minimal</u> in β iff

$$x \in \beta \text{ and } x \neq y \quad \Rightarrow \quad x \not\subset y .$$

A <u>Minimal Complete Development</u> ("MCD") of a set α of cells is a complete development, $b = x_1+\ldots+x_n$, of α such that

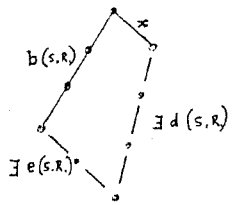
$$\text{for } i = 1\ldots n; \quad x \in {}^{a}/_{b_{i-1}} \text{ and } x \neq x_i \quad \Rightarrow \quad x \not\subset x_i .$$

In other words, an MCD is obtained by taking as the next cell a minimal residual of α. Of course not every set need have an MCD.

<u>Lemma 2·1</u>

Suppose that there is a certain class of reductions called "special reductions" such that every single cell is a special reduction; then (G) follows from

(G^1): $\begin{cases} \text{If a cell } x \text{ and a special reduction } b \text{ are co-initial, then} \\ \text{there exist special reductions } d \text{ and } e \text{ for which } x+d \simeq b+e. \end{cases}$



<u>Proof</u>:

The following property which implies (G) is proved by induction on the length of a:

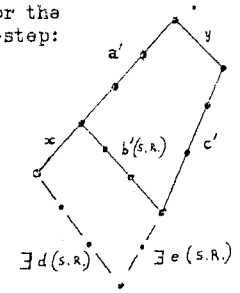
$$a \text{ and } y \text{ co-initial} \quad \Rightarrow \quad \exists b,c: \; a+b \simeq y+c \text{ and } b \text{ is a special reduction.}$$

When $a = 0$: choose $c = 0$ and $b = y$, which is a special reduction by the hypothesis of the lemma. Then $a+b = b = y = y+c$.

When $a = a'+x$ and there are b' (special) and c' with $a'+b' \simeq y+c'$: apply (G^1) to b' and x, to obtain special reductions d and e such that $x+d \simeq b'+e$. (Note: b' and x both start at the end of a'.) Choose $c = c'+e$ and $b = d$.

Then $a+b = a'+x+b = a'+x+d \simeq a'+b'+e \simeq y+c'+e = y+c$, completing the induction-step.

Diagram for the induction-step:



Corollary 2·1

If $^{x}/_{x} = \emptyset$ for all x, any single cell y would be an MCD of the set containing y alone; so by Lemma 2·1, (G^1) with MCDs as the special reductions would imply the Church-Rosser property.

On the next page is set out a list of conditions on residuals and the relation $\subset$, from which the Church-Rosser property will be deduced after a few remarks and lemmas. In the list, x, y, z, y_1, ..., y_n are arbitrary cells.

(D^7): If x and y are any co-initial cells, then there exist an MCD, a, of $^{x}/_{y}$ and an MCD, b, of $^{y}/_{x}$ such that $x+b \simeq y+a$.

(D^8): If (D^7) is true and z is any cell co-initial with x and y, then $^{z}/_{x+b} = {}^{z}/_{y+a}$ in the following two cases:

(i) $z \not\subset x$ and $z \not\subset y$,

(ii) $y \subset x$, $z \subset x$, $z \not\subset y$ and $^{z}/_{x} \not\subset {}^{y}/_{x}$.

(A1): $x \subset y \Rightarrow y \not\subset x$; and for all x, $x \not\subset x$.

(A2): $x \subset y$ and $y \subset z \Rightarrow x \subset z$.

(A3): If $x \not\subset y$ then $^{x}/_{y}$ has no more than one member.

(A4): $^{x}/_{x} = \emptyset$.

(A5): $y_1 \not\subset x$ and $y_1 \not\subset y_2 \Rightarrow {}^{y_1}/_{x} \not\subset {}^{y_2}/_{x}$.

(A6): If $y_i \subset x$ for $i = 1...n$ then there exists k $(1 \leq k \leq n)$ such that $j \neq k \Rightarrow y_j \not\subset y_k$ and $^{y_j}/_{x} \not\subset {}^{y_k}/_{x}$.

These conditions are written out on a page at the end of this thesis for easy reference.

Remarks on the conditions

Remark 1: Residuals were only defined in order to state (D^7), while the significance of (D^8) will come out in the proof of Theorem 2·1. If $^y/_x$ were ever infinite, only a finite number of residuals could be involved in the MCD b, but this would not mean that residuals could be re-defined to exclude the "redundant" ones, as then (D^8) might be upset. In using (D^7) the MCDs b and a may be referred to as "$^y\!\surd\!_x$" and "$^x\!\surd\!_y$" respectively, so that $x + {}^y\!\surd\!_x \simeq y + {}^x\!\surd\!_y$. So when there is only one residual of x with respect to y, "$^x\!\surd\!_y$" and "$^x/_y$" both may denote that residual.

Remark 2: If the conditionsare satisfied when all the cells in their hypotheses are distinct, they can be proved in their full power thus:

(A1): If $y = x$ then $y \not\subset x$ because for all x, $x \not\subset x$.

(A2): If $z = x$, then "$x \subset y$ and $y \subset z$" contradicts the first part of (A1).

If $x = y$ or $y = z$, then by the second part of (A1), $x \not\subset y$ or $y \not\subset z$.

(A3): If $y = x$, then $^y/_x$ has no more than one member by (A4).

(A4): Only one cell is mentioned.

(A5): (A3) shows that there is at most one residual $^{y_1}/_x$.

If $y_1 = x$ or $y_2 = x$, then $^{y_1}/_x$ or $^{y_2}/_x$ is empty by (A4), and

so $^{y_1}/_x \not\subset {}^{y_2}/_x$ by definition.

If $y_1 = y_2$; (A1) gives $^{y_1}/_x \not\subset {}^{y_1}/_x = {}^{y_2}/_x$ if there is one residual of y_1 with respect to x, and if there is no residual, $^{y_1}/_x \not\subset {}^{y_2}/_x$ by definition.

(A6): The indices are chosen so that $i \neq j \Rightarrow y_i \neq y_j$, and "$y_i = x$" would contradict (A1).

(D^7): If $y = x$, then by (A4), $^y/_x$ and $^x/_y$ are both empty.

Let $a = b = 0$, which is an MCD of $^y/_x$ and $^x/_y$.

(D^8): If $y = x$, then $^z/_{x+0} = {}^z/_{y+0}$. ($a = b = 0$ by above.)

If $z = y$, then $^z/_{y+a} = (^z/_y)/_a = \emptyset/_a$ by (A4)

$= \emptyset$,

and $^z/_{x+b} = {}^y/_{x+b} = (^y/_x)/_b = \emptyset$ because b is a complete development of $^y/_x$.

Similarly if $z = x$.

This remark saves a little work in applying Theorem 2·1 to λ-conversion. The reader may have noticed that the first part of (A1) is deducible from (A2) and the second part, but I have stated it separately for clarity.

Remark 3: (A4) brings Corollary 2·1 into play.

Remark 4: By (A2) and (A1), any finite set $\{y_1, \ldots, y_n\}$ of cells has a minimal member, if it has a member at all.

Proof: When $n = 1$: y_1 is minimal in $\{y_1\}$.

When $n > 1$ and $\{y_1,\ldots,y_{n-1}\}$ has a minimal member y_k:

If $y_n \not\subset y_k$, then y_k is minimal in $\{y_1,\ldots,y_n\}$.

If $y_n \subset y_k$, then y_n is minimal, because for $i = 1\ldots n-1$

$y_i \subset y_n \implies y_i \subset y_k$ by (A2)

which contradicts (A1) if $i = k$, and contradicts the minimality of y_k if $i \neq k$.

Also, if y_k is minimal in $\{y_1,\ldots,y_n\}$, then $y_i \not\subset y_k$ for <u>all</u> $i = 1\ldots n$ (including k) because $y_k \not\subset y_k$ by (A1).

(A6) says that in certain circumstances, there is a y_k which not only is minimal in $\{y_1,\ldots,y_n\}$ but also each member y' of y_k/x is minimal in $\left\{ y_1/x,\ldots,y_{k-1}/x,\{y'\},y_{k+1}/x,\ldots,y_n/x \right\}$.

Remark 5: By (A1),...,(A4), every finite set $\{y_1,\ldots,y_n\}$ of cells has an MCD.

Proof: When $n = 0$: 0 is the MCD required.

When $n = 1$: y_1 is an MCD of $\{y_1\}$, because $y_1/y_1 = \emptyset$ by (A4).

When $n > 1$: using Remark 4, choose the first cell of the MCD to be any y_k which is minimal in $\{y_1,\ldots,y_n\}$. Then each y_i/y_k has at most one member by(A3), and y_k/y_k has none, by (A4), so

$\left\{ y_1/y_k,\ldots,y_n/y_k \right\} = \left\{ y_1/y_k,\ldots,y_{k-1}/y_k, y_{k+1}/y_k,\ldots,y_n/y_k \right\}$ and this has no more than n-1 members. Suppose b is an MCD of these n-1 cells; then y_k+b is an MCD of $\{y_1,\ldots,y_n\}$.

To any MCD, b, corresponds a <u>finite</u> set of cells of which b is an MCD, because if $b = (x_1+\ldots+x_m)$ and is an MCD of an infinite set α, then each x_k must be a residual of some $y_k \in \alpha$. Hence b is an MCD of $\{y_1,\ldots,y_m\}$.

Lemma 2.2

Assuming (A1),...,(A6), (D^7) and (D^8):

If b and c are any MCDs of the set $\{y_1,\ldots,y_n\}$ of cells, and $x \not\subset y_i$ for $i = 1\ldots n$, then $c \simeq b$ and $x/c = x/b$. (Roughly; any two MCDs have the same end, and the same residuals of certain other cells.)

Proof:

The result is proved by induction on n.

When $n = 0$: the only possible MCD is null.

When $n = 1$: the only MCD is y_1 itself.

When $n > 1$: $y_1,\ldots,y_n$ can be re-labelled so that the first cells of c and b are y_1 and y_2 respectively. (y_1 might be the same as y_2.) Then $c = y_1+c'$, where c' is an MCD of the fewer-than-n cells in

$\left\{ {}^{y_2}/_{y_1}, \ldots, {}^{y_n}/_{y_1} \right\}$, and $b = y_2 + b'$, where b' is an MCD of the fewer-than-n cells in $\left\{ {}^{y_1}/_{y_2}, \ldots, {}^{y_n}/_{y_2} \right\}$.

If $x = y_i$ for some i, then ${}^{x}/_{c} = {}^{x}/_{b} = \emptyset$ by the definition of <u>complete</u> development. From now on, assume $x \neq y_i$ for i= 1...n. The induction-step is done in two stages.

<u>Stage 1</u>: By definition of b and c as MCDs, $y_i \not\leq y_1$ for all $i \neq 1$, and $y_j \not\leq y_2$ for all $j \neq 2$.

Therefore by (A5), ${}^{y_i}/_{y_1} \not\leq {}^{y_2}/_{y_1}$ for i= 3...n.

If ${}^{y_2}/_{y_1} \neq \emptyset$, it must have at most one member, by (A3), and by above and the proof of Remark 5, there exists an MCD of $\left\{ {}^{y_2}/_{y_1}, \ldots, {}^{y_n}/_{y_1} \right\}$ whose first cell is ${}^{y_2}/_{y_1}$. Suppose this MCD is ${}^{y_2}/_{y_1} + c''$. Then c" is an MCD of $\left\{ \left({}^{y_3}/_{y_1}\right) / \left({}^{y_2}/_{y_1}\right), \ldots, \left({}^{y_n}/_{y_1}\right) / \left({}^{y_2}/_{y_1}\right) \right\}$, $= \left\{ {}^{y_3}/_{(y_1 + {}^{y_2}/_{y_1})}, \ldots {}^{y_n}/_{(y_1 + {}^{y_2}/_{y_1})} \right\}$.

By the induction-hypothesis, ${}^{y_2}/_{y_1} + c'' \simeq c'$, because they are both MCDs of $\left\{ {}^{y_2}/_{y_1}, \ldots, {}^{y_n}/_{y_1} \right\}$.

If ${}^{y_2}/_{y_1} = \emptyset$, define c" to be c'. Then ${}^{y_2}/_{y_1} + c'' = 0 + c'' = c'$.

<u>Residuals of x:</u>

By (A3), ${}^{x}/_{y_1}$ either is empty or contains only one cell, x'.

If ${}^{x}/_{y_1} = \emptyset$, then ${}^{x}/_{c} = \emptyset$ and ${}^{x}/_{(y_1 + {}^{y_2}/_{y_1} + c'')} = \emptyset$.

If ${}^{x}/_{y_1} = \{x'\}$, then by (A5), $x' \not\leq {}^{y_i}/_{y_1}$ for i= 2...n. So the induction-hypothesis applied to c', $\left({}^{y_2}/_{y_1} + c''\right)$ and x' shows that ${}^{x'}/_{c'} = {}^{x'}/_{\left({}^{y_2}/_{y_1} + c''\right)}$. Also, by (A3), ${}^{x'}/_{\left({}^{y_2}/_{y_1}\right)}$ has at most one member.

Therefore ${}^{x}/_{c} = {}^{x}/_{(y_1 + c')} = {}^{x'}/_{c'} = {}^{x'}/_{\left({}^{y_2}/_{y_1} + c''\right)} = {}^{x}/_{\left(y_1 + {}^{y_2}/_{y_1} + c''\right)}$.

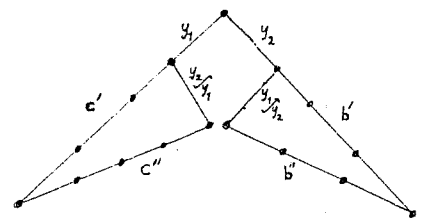
Summarizing; whether ${}^{y_2}/_{y_1} = \emptyset$ or not, $y_1 + {}^{y_2}/_{y_1} + c''$ is an MCD of $\{y_1, \ldots, y_n\}$ with the same end as c,

and ${}^{x}/_{c} = {}^{x}/_{\left(y_1 + {}^{y_2}/_{y_1} + c''\right)}$.

Similarly, if b" is an MCD of $\left\{ {}^{y_3}/_{\left(y_2 + {}^{y_1}/_{y_2}\right)}, \ldots, {}^{y_n}/_{\left(y_2 + {}^{y_1}/_{y_2}\right)} \right\}$

then $y_2 + {}^{y_1}/_{y_2} + b''$ is an MCD of $\{y_1, \ldots, y_n\}$ with the same end as b,

and ${}^{x}/_{b} = {}^{x}/_{\left(y_2 + {}^{y_1}/_{y_2} + b''\right)}$.



Stage 2: By (D^7), $y_1 + {}^{y_2}/_{y_1} \simeq y_2 + {}^{y_1}/_{y_2}$ and by (D^8) part (i) the residuals of x and of $y_3, \ldots, y_n$ are the same after either reduction. (from Stage 1, each can be seen to have at most one residual.) Hence applying the induction-hypothesis to c", b" and ${}^{x}/_{(y_1+{}^{y_2}/_{y_1})}$ $\left\{ \text{which is the same as } {}^{x}/_{(y_2+{}^{y_1}/_{y_2})} \right\}$ shews that $c'' \simeq b''$ and ${}^{x}/_{(y_1+{}^{y_2}/_{y_1}+c'')} = {}^{x}/_{(y_1+{}^{y_2}/_{y_1}+b'')} = {}^{x}/_{(y_2+{}^{y_1}/_{y_2}+b'')}$.

Therefore $c \simeq (y_1+{}^{y_2}/_{y_1}+c'') \simeq (y_1+{}^{y_2}/_{y_1}+b'') \simeq (y_2+{}^{y_1}/_{y_2}+b'') \simeq b$, and ${}^{x}/_{b} = {}^{x}/_{c}$, using Stage 1.

Lemma 2·3

If b is a development of $\{y_1, \ldots, y_n\}$ and $x \not\leq y_i$ for i= 1...n, then ${}^{x}/_{b}$ has at most one member, and ${}^{x}/_{b} \not\leq {}^{y_i}/_{b}$ for i= 1...n.

Proof:

Use induction on the length of b:

When b = 0: then ${}^{x}/_{b} = x$, and $x \not\leq y_i = {}^{y_i}/_{b}$ for i= 1...n.

When b = b'+z, z being a member of ${}^{y_j}/_{b'}$ for some j: by the induction-hypothesis, either ${}^{x}/_{b'} = \emptyset$ or ${}^{x}/_{b'} = \{x'\}$ for some x'.

If ${}^{x}/_{b'} = \emptyset$, then ${}^{x}/_{b} = \emptyset$ and hence ${}^{x}/_{b} \not\leq {}^{y_i}/_{b}$ for i= 1...n.

If ${}^{x}/_{b'} = \{x'\}$, then $x' \not\leq z$ by the induction-hypothesis, and so by (A3), ${}^{x'}/_{z}$ has at most one member. Since ${}^{x'}/_{z} = {}^{x}/_{b}$, this gives the first part of the result. To show ${}^{x'}/_{z} \not\leq {}^{y_i}/_{b}$ for i= 1...n, suppose y" is any member of ${}^{y_i}/_{b}$; then $y'' \in {}^{y'}/_{z}$ for some member y' of ${}^{y_i}/_{b'}$. By the induction-hypothesis, $x' \not\leq y'$; hence by (A5), ${}^{x'}/_{z} \not\leq {}^{y'}/_{z}$. Therefore ${}^{x'}/_{z} \not\leq y''$, as required.

Remark 6: If x, $y_1, \ldots, y_n$ are mutually co-initial cells, b is an MCD of $\{y_1, \ldots, y_n\}$ and $x \not\leq y_i$ for i= 1...n , then $b + {}^{x}/_{b}$ is an MCD of $\{x, y_1, \ldots, y_n\}$.

Proof: If $b = z_1 + \ldots + z_m$; Lemma 2·3 shows that ${}^{x}/_{b_k} \not\leq z_{k+1}$ for k= 0... m-1, so at each stage, z_{k+1} is minimal in $\left\{ {}^{x}/_{b_k}, {}^{y_1}/_{b_k}, \ldots, {}^{y_n}/_{b_k} \right\}$, satisfying the requirements for an MCD.

Similarly, if $x_1, \ldots, x_m, y_1, \ldots, y_n$ are mutually co-initial, b is an MCD of $\{y_1, \ldots, y_n\}$ and $x_i \not\leq y_j$ for i= 1...m and j= 1...n; then

$$b + \text{any MCD of } \left\{ {}^{x_1}/_{b}, \ldots, {}^{x_m}/_{b} \right\}$$

will be an MCD of $\{x_1, \ldots, x_m, y_1, \ldots, y_n\}$.

Also , if $j > i \Rightarrow y_j \not\leq y_i$, then the reduction b defined by

$\begin{cases} b_o = 0 \quad , \quad b_{k+1} = b_k + y \text{, where } y \text{ is the (sole) member of the first of } y_1/b_k, \ldots y_n/b_k \text{, which is not empty.} \\ \text{If there is no such } y \text{, then } b = b_k. \end{cases}$

is an MCD of $\{y_1, \ldots, y_n\}$.

Remark 7: If $x, y_1, \ldots, y_n$ are mutually co-initial, then an MCD, called an "x-MCD", of $\{y_1, \ldots, y_n\}$ can be constructed as follows.

If $n = 0$, the x-MCD is 0. Otherwise, first re-number the cells $y_1, \ldots, y_n$ so that for some number m:

for $i = 1 \ldots m$, $x \not\subset y_i$ and $x \neq y_i$ $\begin{cases} \text{if there are no such } y_i, \\ \text{put } m = 0. \end{cases}$

for $i = m+1 \ldots n$, $x \subset y_i$ or $x = y_i$ $\begin{cases} \text{if } x = y_{m+j} \text{ for some } j, \\ \text{arrange the cells so that} \\ j = 1. \end{cases}$

Also, using Remark 4, re-number $y_{m+1}, \ldots, y_n$ so that $h > j \Rightarrow y_{m+h} \not\subset y_{m+j}$. If $y_{m+1} = x$, do the numbering without altering y_{m+1}. (This is possible because $y_{m+h} \not\subset x$ for $h = 1 \ldots (n-m)$, by (A1).)

Then $y_{m+j} \not\subset y_i$ for $i = 1 \ldots m$ and $j = 1 \ldots (n-m)$, because otherwise $x \subset y_{m+j} \subset y_i$ or $x = y_{m+j} \subset y_i$, which both imply $x \subset y_i$, contrary to the definition of i. Hence by Remark 6,

$$(\text{any MCD } b \text{ of } \{y_1, \ldots, y_m\}) + (\text{any MCD of } \{y_{m+1}/b, \ldots, y_n/b\})$$

will be an MCD of $\{y_1, \ldots, y_n\}$.

For the first part of the x-MCD; define an MCD, b, of $\{y_1, \ldots, y_m\}$ as follows:

$b_o = 0$.

If b_k is defined, then by Lemma 2·3, $x/b_k \not\subset y_i/b_k$ for $i = 1 \ldots m$ and x/b_k has at most one member x', since $x \not\subset y_i$ for $i = 1 \ldots m$. Also each y_i/b_k has at most one member y_i' (for $i = 1 \ldots m$) as in Remark 5.

(i) If there are no $y_i' \subset x'$: choose the next cell v in b to be any one minimal in $\{y_1', \ldots y_m'\}$, if $\{y_1', \ldots, y_m'\} \neq \emptyset$. Then $b_{k+1} = b_k + v$. If $\{y_1', \ldots, y_m'\} = \emptyset$, that is $y_i/b_k = \emptyset$ for $i = 1 \ldots m$, then let $b = b_k$.

(ii) If there are any $y_i' \subset x'$: choose v to be the one of these y_i' given by (A6). v is minimal in $\{y_1', \ldots, y_m'\}$ because

$y_i' \subset x' \Rightarrow y_i' \not\subset v$, by the definition of v, and

$y_i' \not\subset x' \Rightarrow y_i' \not\subset v$, since $(y_i' \subset v$ and $v \subset x')$ implies $y_i' \subset x'$ by (A2).

Because of the minimality of v at each stage, b is an MCD.

For the rest of the x-MCD, note that if y_{m+j}/b is not empty, it must have at most one member y_{m+j}' by Lemma 2·3. (for $j = 1 \ldots n-m$) Now for each stage b_k of b, $h > j \Rightarrow y_{m+h}/b_k \not\subset y_{m+j}/b_k$.

This is proved by induction on k: suppose $h > j$;

When $k = 0$: $\quad {}^{y_{m+h}}/_{b_o} = y_{m+h} \not\leq y_{m+j} = {}^{y_{m+j}}/_{b_o}$.

When $b_{k+1} = b_k + v$ and ${}^{y_{m+h}}/_{b_k} \not\leq {}^{y_{m+j}}/_{b_k}$:

Lemma 2·3 shows that ${}^{y_{m+h}}/_{b_k} \not\leq v$, since $y_{m+h} \not\leq y_i$ for $i = 1 \ldots m$ and v is the residual of some such y_i.

Hence by (A5), $\left({}^{y_{m+h}}/_{b_k}\right)/_v \not\leq \left({}^{y_{m+j}}/_{b_k}\right)/_v$;

that is, ${}^{y_{m+h}}/_{b_{k+1}} \not\leq {}^{y_{m+j}}/_{b_{k+1}}$ as required.

Hence $h > j \implies y'_{m+h} \not\leq y'_{m+j}$, and so the development of $\{y'_{m+1}, \ldots, y'_n\}$ defined as in the third part of Remark 6 is an MCD. Call this MCD "a". (If $m = n$, let $a = 0$.)

The x-MCD of $\{y_1, \ldots, y_n\}$ is defined to be b+a . Actually there may be several x-MCDs, depending, for example, on the particular minimal cell v chosen on the previous page.

Theorem 2·1

(A1), ..., (A6), (D^7) and (D^8) together imply

(G^1) **If a cell x and an MCD b are co-initial, then there exist MCDs e and d such that $x+d \simeq b+e$.**

Hence the Church-Rosser Property, by Remark 3 and Corollary 2·1.

The proof takes up the next 13 pages. First of all, let $\{y_1, \ldots, y_n\}$ be a set of cells of which b is an MCD, and let b^* be an x-MCD of $\{y_1, \ldots, y_n\}$. By Lemma 2·2, b^* has the same end as b (though ${}^x/_{b^*}$ may be different from ${}^x/_b$) so, replacing b by b^* in (G^1), it is enough to prove

($G^{1'}$) **If x, $y_1, \ldots, y_n$ are mutually co-initial and b is an x-MCD of $\{y_1, \ldots, y_n\}$, then there exist MCDs e and d such that $x+d \simeq b+e$.**

The proof of ($G^{1'}$) splits up into four cases:

(1) for $i = 1 \ldots n$, $x \not\leq y_i$ and $x \neq y_i$.

(2) for some i, $x = y_i$.

(3) for $i = 1 \ldots n$, $y_i \not\leq x$ and $x \neq y_i$. This overlaps with Case 1.

(4) for $i = 1 \ldots n$, $x \neq y_i$.

The whole result is implied by Cases 2 and 4 together.

In the proofs of Cases 1, 2 and 3, the term "(G^2)" will be used to denote ($G^{1'}$) with the following statements added:

"d is an MCD of $\{{}^{y_1}/_x, \ldots, {}^{y_n}/_x\}$ and e is an MCD of a subset of ${}^x/_b$, and if z is co-initial with x and $z \not\leq x$ and $z \not\leq y_i$ for $i = 1 \ldots n$, then ${}^z/_{x+d} = {}^z/_{b+e}$.".

{Obviously (G^2) implies ($G^{1'}$); the clause about z is just to make some induction-steps work.}

The clause "of a subset of x/b" rather than "of x/b" is to allow for a case where x/b might be infinite. (See later in proof of case 3.)

Cases 1 and 2:

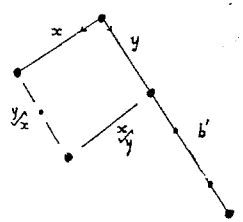
(G^2) will now be proved in Cases 1 and 2 together, by induction on n. Further it will be proved that e is an MCD of the whole set $x/_b$.

Basis: When n = 0 and so b = 0: choose d = 0 and e = x.
Then d is an MCD of $\emptyset$ and e is an MCD of $\{x\}$ which is the same as $x/_b$.

Induction-step: Assume that $n > 0$ and (G^2) with the above extra clause is true in both Cases 1 and 2 for all $n' \leq n-1$ (for all $x, z, y_1, \ldots y_{n'}$). Suppose that x, z, b and $\{y_1, \ldots, y_n\}$ are given as in (G^2); the two cases are now separated.

Case 1 of the induction-step:
For i= 1...n, $x \not\subset y_i$ and $x \neq y_i$. Here the number m of Remark 7 is the same as n. Re-number $y_1, \ldots, y_n$ so that y_1 is the first cell of b, and suppose $b = y_1 + b'$. y_1 will be called "y" for short. By (A3), $x/_y$ has at most one member, and by (D^7),

$$x+{}^{y}/_{x} \simeq y+{}^{x}/_{y} .$$



Also $y_i/_x \not\subset y/_x$ for i= 2...n . . . . . .(I)

Proof: Since b is an MCD, $y_i \not\subset y$ for i= 2...n.
If $y_i \not\subset x$, then by (A5), $y_i/_x \not\subset y/_x$.
If $y_i \subset x$, then by definition of b as an x-MCD, y must have been chosen by (ii) on page 46. Hence $y_i/_x \not\subset y/_x$ by (A6).

Hence $y_i/_{(x+y/_x)} = y_i/_{(y+x/_y)}$ for i= 2...n. . . . . .(II)

Proof: As in (I), $y_i \not\subset y$ for i= 2...n.
If $y_i \not\subset x$, then use (D^8) part (i).
If $y_i \subset x$, then as in (I), y must have been chosen by (ii) on page 46, and hence $y \subset x$. Use $(D^8 ii)$ together with (I).

Also $z/_{(x+y/_x)} = z/_{(y+x/_y)}$ by $(D^8 i)$ . . . . . (III)

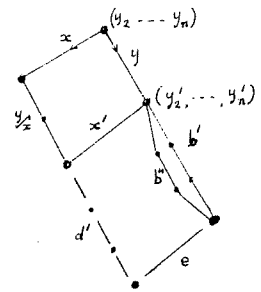
As in Remark 5, there are no more than n-1 residuals $\{y_2/_y, \ldots, y_n/_y\}$.
If any of $x/_y$, $z/_y$, $y_2/_y$, ..., $y_n/_y$ is non-empty, suppose its sole member is x', z', y_2', ..., or y_n' respectively.
By (A5) applied three times; for i= 2...n,

$$z/_y \not\subset y_i/_y , \quad x/_y \not\subset y_i/_y \text{ and } z/_y \not\subset x/_y \quad \ldots\ldots (IV)$$

The proof now splits up into two sub-cases, according as $x/_y$ is empty or not.

Subcase (i); When $x/_y$ is not empty, and its sole member is x':
By Remark 7 there exists an x'-MCD, b", of $\{y_2', \ldots, y_n'\}$. By Lemma 2·2 and (IV); $b' \simeq b''$, $x'/_{b'} = x'/_{b''}$ and $z'/_{b'} = z'/_{b''}$ $\left\{\text{if } z/_y = \{z'\}, \text{ not } \emptyset\right\}$.
By (IV), the induction-hypothesis can be applied to x', z', $\{y_2', \ldots, y_n'\}$ and b". {Case 2 is applied if $x' = y_i'$ for some i, otherwise Case 1 is used.} Hence there exist an MCD, d', of $\{y_2'/_{x'}, \ldots, y_n'/_{x'}\}$ and an MCD, e, of $x'/_{b''}$ such that

$$b''+e \simeq x'+d', \text{ and } z'/_{(b''+e)} = z'/_{(x'+d')} \text{ if } z/_y \neq \emptyset.$$



Choose d to be $({}^{y}\!\surd_{x}+d')$.

Hence $x+d = x+{}^{y}\!\surd_{x}+d' \simeq y+x'+d' \simeq y+b''+e \simeq y+b'+e = b+e$.

Now ${}^{y_i'}/_{x'} = {}^{(y_i/y)}\!/_{(x/y)} = {}^{y_i}\!/_{(y+{}^{x}\surd_{y})} = {}^{y_i}\!/_{(x+{}^{y}\surd_{x})}$ by (II). (If ${}^{y_i}/_{y} \neq \emptyset$)

So d' is an MCD of $\left\{{}^{y_2}\!/_{(x+{}^{y}\surd_{x})}, \ldots, {}^{y_n}\!/_{(x+{}^{y}\surd_{x})}\right\}$; hence by (I) and the second part of Remark 6, d is an MCD of $\left\{{}^{y_1}/_{x}, \ldots, {}^{y_n}/_{x}\right\}$, as required.

Also e is an MCD of ${}^{x'}/_{b''} = {}^{x'}/_{b'} = {}^{(x/y)}\!/_{b'} = {}^{x}\!/_{(y+b')} = {}^{x}/_{b}$.

<u>Residuals of z</u>:

If ${}^{z}/_{y} \neq \emptyset$; then

${}^{z}/_{(b+e)} = {}^{z}/_{(y+b'+e)} = {}^{(z/y)}\!/_{(b'+e)} = {}^{(z/y)}\!/_{(b''+e)} = {}^{(z/y)}\!/_{(x'+d')}$ by the induction-hypothesis applied to b";

$= \left({}^{z}\!/_{(y+{}^{x}\surd_{y})}\right)\!/_{d'} = \left({}^{z}\!/_{(x+{}^{y}\surd_{x})}\right)\!/_{d'}$ by (III).

$= {}^{z}/_{x+d}$ as required.

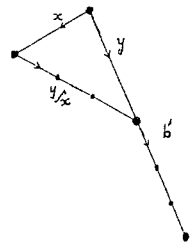
If ${}^{z}/_{y} = \emptyset$, then ${}^{z}\!/_{(x+{}^{y}\surd_{x})} = {}^{z}\!/_{(y+{}^{x}\surd_{y})} = \emptyset$, and so ${}^{z}/_{x+d} = \emptyset$.

Also ${}^{z}/_{b+e} = {}^{z}\!/_{(y+b'+e)} = \emptyset = {}^{z}/_{x+d}$.

<u>Subcase (ii)</u>; When ${}^{x}/_{y} = \emptyset$ and so ${}^{x}/_{b} = \emptyset$:

then $x+{}^{y}\surd_{x} \simeq y+{}^{x}\surd_{y} = y+0 = y$

and ${}^{y_i}\!/_{(x+{}^{y}\surd_{x})} = {}^{y_i}\!/_{(y+{}^{x}\surd_{y})} = {}^{y_i}/_{y}$ by(II).



Choose d to be $({}^{y}\surd_{x}+b')$ and e to be 0.

The rest of the reasoning is the same as on page 51 —— replacing "x'" by "0" and "d'" by "b'", and letting b" = b'.

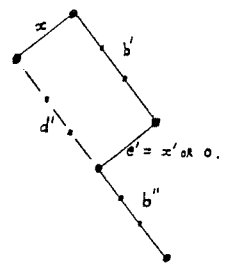
<u>Case 2</u> of the induction-step: for some i, $x = y_i$.

Define m as in Remark 7 and let b' be the "b" of that remark, and b" be the "a" (without its first cell, if ${}^{x}/_{b'} \neq \emptyset$)

Then, since $x = y_{m+1}$, either $b = b'+x'+b''$ or $b = b'+0+b''$, according as ${}^{x}/_{b'} = \{x'\}$ or $\emptyset$. Also $m \leqslant n-1$.

Applying Case 1 of the induction-hypothesis to $\{y_1, \ldots, y_m\}$, x and b', gives an MCD d' of $\left\{{}^{y_1}/_{x}, \ldots, {}^{y_m}/_{x}\right\}$ and an MCD e' of ${}^{x}/_{b'}$ such that $x+d' \simeq b'+e'$, and ${}^{z^*}/_{x+d'} = {}^{z^*}/_{b'+e'}$ . . . . . (V)

for any cell z^* with $z^* \not\simeq y_i$ for i= 1...m and $z^* \not\simeq x$.



Since there is no more than one residual $x/_{b'}$, there can be only one possible MCD, e', of $x/_{b'}$. That is, e' = x' or 0 according as $x/_{b'} = \{x'\}$ or $\emptyset$. Therefore by the previous page, b = b'+e'+b".

Also, by its definition, b" is an MCD of $\left\{ y_{m+2}/_{(b'+e')}, \ldots, y_n/_{(b'+e')} \right\}$.

Choose d = (d'+b") and e = 0.

Then $x+d = x+d'+b'' \simeq b'+e'+b'' = b = b+0 = b+e$.

e is an MCD of $x/_b$, because $x/_b = y_{m+1}/_b = \emptyset$ since b is a <u>complete</u> development.

d is an MCD of $\left\{ y_1/_x, \ldots, y_n/_x \right\}$.

<u>Proof</u>: d consists of

(the MCD d' of $\left\{ y_1/_x, \ldots, y_m/_x \right\}$) + (an MCD of $\left\{ y_{m+2}/_{(b'+e')}, \ldots, y_n/_{(b'+e')} \right\}$).

But $y_{m+j}/_{(b'+e')} = y_{m+j}/_{(x+d')}$ by (V) with y_{m+j} as z^*.
(for j= 2... n-m)

$= \left(y_{m+j}/_x \right)/_{d'}$.

Since by (A5), $y_{m+j}/_x \not\subset y_i/_x$ for i= 1...m, the second part of Remark 6 shows that d is an MCD of

of $\left\{ y_1/_x, \ldots, y_m/_x, y_{m+2}/_x, \ldots, y_n/_x \right\}$, $= \left\{ y_1/_x, \ldots, y_n/_x \right\}$ by (A4), since $y_{m+1} = x$.

Also $z/_{(x+d)} = z/_{(x+d'+b'')} = z/_{(b'+e'+b'')}$ by (V) with z as "z^*".

$= z/_b = z/_{(b+e)}$.

<u>Case 3</u>: for i= 1...n, $y_i \not\subset x$ and $x \neq y_i$.

The overlapping of this case with Case 1 is necessary for it to be applied to Case 4 later. [redacted] is proved by induction on n.

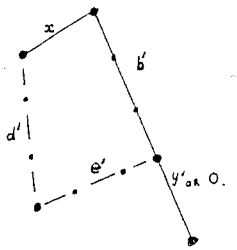
When n = 0: let d = 0 and e = x.

When n > 0: if there are no y_i with $x \subset y_i$, use Case 1. Otherwise by Remark 7, b = b'+b*, where b' is an x-MCD of $\{y_1, \ldots, y_{n-1}\}$ and $b^* = \begin{cases} 0 \text{ if } y_n/_{b'} = \emptyset \\ y' \text{ if } y_n/_{b'} = \{y'\}. \end{cases}$

As in Remark 7, $x \subset y_n$ and $y_n \not\subset y_i$ for i= 1... n-1. Call y_n "y".

By the induction-hypothesis applied to x, b' and $\{y_1, \ldots y_{n-1}\}$ there exist an MCD d' of $\left\{ y_1/_x, \ldots, y_{n-1}/_x \right\}$ and an MCD e' of a subset of $x/_{b'}$ such that $x+d' \simeq b'+e'$, and $z^*/_{(x+d')} = z^*/_{(b'+e')}$ . . . . . (VI)

for any cell z^* with $z^* \not\subset x$ and $z^* \not\subset y_i$ for i= 1... n-1.



Now $y \not\subset x$ since $x \subset y$, so by (VI) applied to y;

$$y/_{(x+d')} = y/_{(b'+e')} \quad \ldots\ldots\ldots\ldots \text{(VII)}$$

If $y/_{b'} = \emptyset$, then $b = b'$; define $e = e'$ and $d = d'$.

Hence $x+d \simeq b+e$ and $z/_{(x+d)} = z/_{(b+e)}$ by (VI). Also e is an MCD of a subset of $x/_{b'} = x/_{b}$. d would be an MCD of $\{y_1/_x, \ldots, y_n/_x\}$ if $(y_n/x)/_d = \emptyset$ and at each stage d_k of d, $(y_n/x)/_{d_k} \not\subset (y_i/x)/_{d_k}$ for i= 1... n-1. The former is true because $(y_n/x)/_d = y/_{x+d} = y/_{b'+e'}$ {by (VII)}, $= \emptyset$. The latter is true by Lemma 2·3, since $y_n/_x \not\subset y_i/_x$ by (A5), for i= 1...n-1.

From now on, assume $y/_{b'} \neq \emptyset$.

$$y/_{b'} \not\subset x/_{b'}, \quad z/_{b'} \not\subset y/_{b'} \quad \text{and} \quad z/_{b'} \not\subset x/_{b'} \quad \ldots\ldots\ldots \text{(VIII)}$$

<u>Proof</u>: b' is an MCD of $\{y_1, \ldots, y_{n-1}\}$ and hence is a development of $\{x, y_1, \ldots, y_{n-1}\}$. Since $y \not\subset x$ and $y \not\subset y_i$ for i= 1... n-1, Lemma 2·3 gives $y/_{b'} \not\subset x/_{b'}$. Similarly $z/_{b'} \not\subset x/_{b'}$. b' is also a development of $\{y, y_1, \ldots, y_{n-1}\}$

so by Lemma 2·3, $z/_{b'} \not\subset y/_{b'}$.

Suppose that $x_1, \ldots, x_h$ $(0 \leq h)$ are the members of $x/_{b'}$ whose residuals are the cells of e' (compare the second part of Remark 5); then e' is an MCD of $\{x_1, \ldots, x_h\}$. Also suppose $y/_{b'} = \{y'\}$, and $z/_{b'} = \{z'\}$ or $\emptyset$.

Note: $x/_{b'}$ might be infte.

By (VIII); $y' \not\subset x_i$ and $z' \not\subset x_i$ for i= 1...h, and $z' \not\subset y'$ (if z' exists).

Now by Remark 7 there exists a y'-MCD, e^*, of $\{x_1, \ldots, x_h\}$. By Lemma 2·2, $e' \simeq e^*$ and $y'/_{e^*} = y'/_{e'}$ because $y' \not\subset x_i$ for i= 1...h. Similarly $z'/_{e^*} = z'/_{e'}$. (See the diagram on the next page.)

Case 2 or 1 (according as y' is or is not one of $x_1, \ldots x_h$) can be applied to z', y', $\{x_1, \ldots, x_h\}$ and e^* to obtain an MCD, d", of $\{x_1/_{y'}, \ldots, x_h/_{y'}\}$ and an MCD, e", of $y'/_{e^*}$ such that

$$e^*+e'' \simeq y'+d'' \quad \text{and} \quad z'/_{(e^*+e'')} = z'/_{(y'+d'')} \quad \ldots\ldots \text{(IX)}$$

(if z' exists)

If $x/_{b'}$ infte, then d" will not be an MCD of all of $((x/_{b'})/_{y'})$. So e will not be an MCD of all of $(x/_{b'})/_{y'}$ in this case

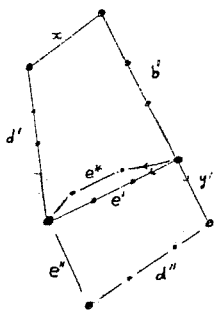
Let $d = d'+e''$ and $e = d''$.

Then e is an MCD of $\{x_1/_{y'}, \ldots, x_h/_{y'}\}$, which is a subset of $(x/_{b'})/_{y'}$, which is the same as $x/_{(b'+y')} = x/_b$.

By Remark 6, d will be an MCD of $\{y_1/_x, \ldots y_n/_x\}$ if $y_n/_x \not\subset y_i/_x$

for $i = 1 \ldots (n-1)$ and e'' is an MCD of $(y_n/x)/d'$. But the former is true by (A5), and for the latter, e'' is an MCD of y'/e^* which is the same as $y'/e' = (y/b')/e' = y/(b'+e') = y/(x+d')$ by (VII). So d is an MCD of $\{y_1/x, \ldots, y_n/x\}$.

Also $x+d = (x+d'+e'') \simeq (b'+e'+e'') \simeq (b'+e^*+e'') \simeq (b'+y'+d'') = b+e$.



Residuals of z

If $z/b' = \{z'\}$, then

$$z/b+e = z/(b'+y'+e) = z'/(y'+e) = z'/(e^*+e'') \text{ by (IX), since } e = d''.$$

$$= (z'/e^*)/e'' = (z'/e')/e'' = z'/(e'+e'') = z/(b'+e'+e'')$$

$$= z/(x+d'+e'') \text{ by (VI)}$$

$$= z/x+d .$$

If $z/b' = \emptyset$, then $z/b+e = \emptyset$ too. Also $z/(b'+e') = \emptyset$, so by (VI), $z/x+d' = \emptyset$. Therefore $z/x+d = \emptyset = z/b+e$.

<u>Case 4</u>: for $i = 1 \ldots n$, $x \neq y_i$.

In this case $(G^{1'})$ will be proved without involving (G^2).

Given x, $\{y_1, \ldots, y_n\}$ and b as in $(G^{1'})$, let b' and b" respectively be the reductions "b" and "a" of Remark 7. Then $b = b'+b''$. Since $x \not\subset y_i$ and $y_{m+j} \not\subset y_i$ for $i = 1 \ldots m$ and $j = 1 \ldots n-m$, there must be at most one member in each of x/b' and y_{m+j}/b', by Lemma 2-3. Also, by a proof like the first part of (VIII), with "y_{m+j}" instead of "y";

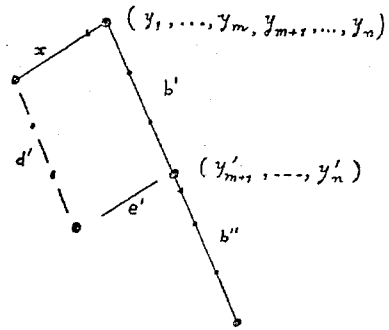
$$y_{m+j}/b' \not\subset x/b' \quad \ldots\ldots\ldots\ldots\ldots\ldots (X)$$

(Here, $y_{m+j} \not\subset x$ because $x \subset y_{m+j}$ by the definition of m in Remark 7.)

Case 1 applied to x, $\{y_1, \ldots, y_m\}$ and b' gives an MCD, d', of $\{y_1/x, \ldots, y_m/x\}$ and an MCD, e', of x/b' such that

$$b'+e' \simeq x+d' \quad \text{and} \quad z^*/(b'+e') = z^*/(x+d') \quad \ldots\ldots\ldots (XI)$$

for any cell z^* with $z^* \not\subset x$ and $z^* \not\subset y_i$ for $i = 1 \ldots m$.



y_{m+j} satisfies the conditions of (XI), for j= 1...(n-m), so

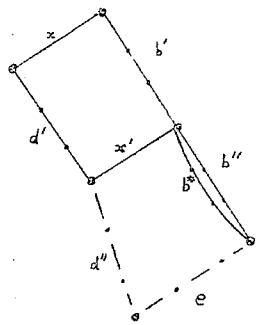
$$y_{m+j}/_{(b'+e')} = y_{m+j}/_{(x+d')} \quad \text{. . . . . (XII)}$$

Define $y'_{m+1},\ldots,y'_n$, x' to be the sole members of $y_{m+1}/_{b'},\ldots,y_n/_{b'}$, $x/_{b'}$ respectively (if they are not empty). Since e' is an MCD of $x/_{b'}$, e' = x' or 0 according as $x/_{b'} = \{x'\}$ or $\emptyset$.

<u>Subcase (i)</u>; Suppose $x/_{b'} = \{x'\}$.

By Remark 7 there exists an x'-MCD, b^*, of $\{y'_{m+1},\ldots,y'_n\}$. By Lemma 2·2, $b^* \simeq b''$, since b" is an MCD of $\{y'_{m+1},\ldots,y'_n\}$. By (X), $y'_{m+j} \not\leq x'$ for j= 1...n-m.

Therefore Case 3 (or Case 2 if x' is one of $y'_{m+1},\ldots,y'_n$) is applicable to x', $\{y'_{m+1},\ldots,y'_n\}$ and b^*, giving an MCD, d", of $\{y'_{m+1}/_{x'},\ldots,y'_n/_{x'}\}$ and an MCD, e, of a subset of $x'/_{b^*}$ such that $x'+d'' \simeq b^*+e$.



Let d = d'+d".

Now for j= 1... n-m, $y'_{m+j}/_{x'} = y_{m+j}/_{(b'+x')} = y_{m+j}/_{(x+d')}$ by (XII) since e' = x',

$$= \left(y_{m+j}/_x\right)/_{d'},$$

so d" is an MCD of $\left\{\left(y_{m+1}/_x\right)/_{d'},\ldots,\left(y_n/_x\right)/_{d'}\right\}$.

For i= 1...m and j= 1... n-m, $y_{m+j}/_x \not\leq y_i/_x$ by (A5).

Hence the second part of Remark 6 shows that d is an MCD of $\{y_1/_x,\ldots,y_n/_x\}$.

Also $x+d = (x+d'+d'') \simeq (b'+e'+d'') = (b'+x'+d'') \simeq (b'+b^*+e)$

$\simeq (b'+b''+e)$

$= b+e.$

Hence $(G^{1'})$ is satisfied.

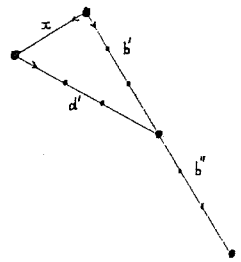
Note: e is an MCD of a subset of $x'/_{b^*}$, which might not be the same as $x'/_{b''}$. So we cannot say that e is an MCD of a subset of $x/_b$.

<u>Subcase (ii)</u>; When $x/_{b'} = \emptyset$, then e' = 0.

Let e = 0 and d = d'+b". (See the diagram on the next page.)

The rest of the reasoning is the same as in Subcase (i), replacing "x'" by "0" and "d'" by "b'", and letting b^* be b".

Diagram for subcase (ii):



The proof of Theorem 2·1 is now complete. Though it looks rather complicated here, when it is re-written to apply only to $\alpha\beta$-conversion it becomes one of the shortest current proofs of the Church-Rosser Theorem.

Other people's results

Several authors have proved abstract analogues of the original Church-Rosser theorem, the first being Newman in [1], whose results however do not include λ-conversion as a special case (as is shown in the review [4]).

His main results are:

(1): If r and s are relations and there are no infinite "chains" $X_0 \; s \; X_1 \; s \; X_2 \; s \ldots\ldots$ (not even chains with repeated members like $X_0 \; s \; X_1 \; s \; X_0 \; s \; X_1 \; s \ldots.$ are allowed)

and

$U \; r \; X$ and $U \; s \; Y \implies \exists Z$: $Y \geqslant_r Z$, and $X \geqslant_s Z$ by a non-null reduction,

then

$U \geqslant_r X$ and $U \geqslant_s Y \implies \exists Z$: $Y \geqslant_r Z$, and $X \geqslant_s Z$ by a non-null reduction.

(2): (CR) is true for any reduction-complex satisfying the following conditions: (x, y, z are any mutually co-initial cells)

(Δ_1): ${}^x/_y = \emptyset$ if and only if $x = y$. (${}^x/_y$ is defined as before.)

(Δ_2): $x \neq y$ implies that there are no cells common to ${}^x/_z$ and ${}^y/_z$.

(Δ_3): If x and y are distinct and co-initial; there exist developments a, b of ${}^x/_y$ and ${}^y/_x$ respectively, such

that $x+b \simeq y+a$. $\{(\Delta_3)$ also holds when $x = y$; compare Remark 2. $\}$

(Δ_4): If (Δ_3) is true and z is any cell co-initial with x,y, then ${}^{z}/_{x+b} = {}^{z}/_{y+a}$.

Finally there is assumed to be a relation J (which only holds between co-initial cells) such that

(J_1): If $x\ J\ y$, then ${}^{x}/_{y}$ contains exactly one member.

(J_2): If $x\ \underline{J}\ y$, then $x'\ \underline{J}\ y'$ for all $x' \in {}^{x}/_{z}$ and $y' \in {}^{y}/_{z}$.

(3): (CR) is still derivable if (Δ_1) is replaced in the above list by (Δ_1^*) given below and an extra condition (J_3) is added.

(Δ_1^*): ${}^{x}/_{x} = \emptyset$ for all x, and if ${}^{x}/_{y} = \emptyset$ then either $x = y$ or ${}^{y}/_{x}$ has exactly one member.

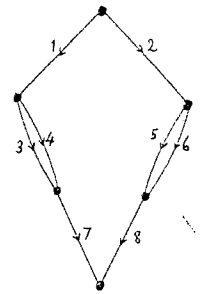
(J_3): If $x \neq y$ and $x\ J\ z$ and $y\ J\ z$, then ${}^{x}/_{y}$ has exactly one member.

Result (1) is like Lemmas 1·2 and 1·3 of this thesis, and results (2) and (3) neither include nor are included by my Theorem 2·1, αβ-contraction being a system satisfying my assumptions and not Newman's, while the example overleaf satisfies Newman's assumptions and not mine.

Cells are numbered from 1 to 8.

J is defined by the statements

$3\ J\ 4,\quad 4\ J\ 3,\quad 5\ J\ 6,\quad 6\ J\ 5.$



Definition of Residuals: ${}^{x}/_{x} = \emptyset$ for all x,

$${}^{1}/_{2} = \{5,6\}$$
$${}^{2}/_{1} = \{3,4\}$$
$${}^{5}/_{6} = {}^{6}/_{5} = 8$$
$${}^{3}/_{4} = {}^{4}/_{3} = 7$$

(Δ_1), (Δ_1^*), (Δ_2), (J_1) and (J_3) can easily be verified.

For (J_2): If $x\ J\ y$, then from the diagram, z must be x or y, and hence either ${}^{x}/_{z}$ or ${}^{y}/_{z}$ is empty.

If $x = y$, then it must be proved that for all z co-initial with x, $x'\ \underline{J}\ x''$ for all members x', x'' of ${}^{x}/_{z}$. This is immediate if $z = x$ or ${}^{x}/_{z}$ has only one member. Otherwise, ${}^{x}/_{z} = \{5,6\}$ or $\{3,4\}$, and the result follows by definition of J.

For (Δ_3): The only pairs of co-initial cells $\{x, y\}$ with $x \neq y$ are $\{3,4\}$, $\{5,6\}$, and $\{1,2\}$.

$3+{}^{4}/_{3} = 3+7 \simeq 4+7 = 4+{}^{3}/_{4}$. Similarly for $\{5,6\}$.

For $\{1,2\}$: $3+7 = 3+{}^{4}/_{3}$ and so $(3+7)$ is a development of $\{3,4\} = {}^{2}/_{1}$. Likewise $5+8$ is a development of ${}^{1}/_{2}$, and as required, $1+(3+7) \simeq 2+(5+8)$.

For (Δ_4): Since there are only two cells at any vertex, z must be the same as x or y, and hence ${}^{z}/_{x+b} = {}^{z}/_{y+a} = \emptyset$, because

in each case b and a are <u>complete</u> developments. (Compare Remark 2.)

However, if there were a relation, $\subset$, satisfying (A1) and (A3);

$1 \subset 2 \quad \Rightarrow \quad 2 \not\subset 1$ by (A1)

$\Rightarrow \quad {}^{2}/_{1}$ would have no more than one member, by (A3).

Therefore $1 \not\subset 2$, and so by (A3), ${}^{1}/_{2}$ would have to have at most one member, which is false. Hence this example does not satisfy (A1) and (A3) together, although it satisfies Newman's assumptions.

H. B. Curry has also "generalized" the Church-Rosser Theorem, in [2], but his result also does not include $\alpha\beta$-contraction. (See [4] and page 149 of Curry and Feys' [5] .)

The conditions from which he deduced (CR) are as follows.

(Δ_1'): ${}^{x}/_{x} = \emptyset$ for all x.

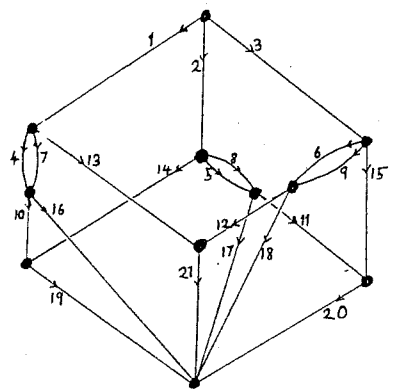
(Δ_3) and (Δ_4) as before.

(J_1'): If x J y, then ${}^{x}/_{y}$ has at most one member.

(J_2'): If x J y, then x' J y' for all $x' \in {}^{x}/_{z}$ and $y' \in {}^{y}/_{z}$.

(J_4): For all co-initial x and y; x J y or y J x.

Again, $\alpha\beta$-contraction satisfies my assumptions but not the ones above, and the system on the next page satisfies these conditions but not my (A1),...,(A3).



The cells are numbered from 1 to 21 and run from an upper point to a lower.

<u>Definition of Residuals:</u> for all x, ${}^{x}/_{x} = \emptyset$.

${}^{1}/_{3} = \{6,9\}$, ${}^{3}/_{1} = 13$.	${}^{4}/_{13} = {}^{7}/_{13} = 21$, ${}^{13}/_{4} = {}^{13}/_{7} = 16$.
${}^{3}/_{2} = \{5,8\}$, ${}^{2}/_{3} = 15$.	${}^{5}/_{14} = {}^{8}/_{14} = 19$, ${}^{14}/_{5} = {}^{14}/_{8} = 17$.
${}^{2}/_{1} = \{4,7\}$, ${}^{1}/_{2} = 14$.	${}^{6}/_{15} = {}^{9}/_{15} = 20$, ${}^{15}/_{6} = {}^{15}/_{9} = 18$.
${}^{4}/_{7} = {}^{7}/_{4} = 10$.	${}^{10}/_{16} = \emptyset$, ${}^{16}/_{10} = 19$.
${}^{5}/_{8} = {}^{8}/_{5} = 11$.	${}^{11}/_{17} = \emptyset$, ${}^{17}/_{11} = 20$.
${}^{6}/_{9} = {}^{9}/_{6} = 12$.	${}^{12}/_{18} = \emptyset$, ${}^{18}/_{12} = 21$.

J is defined by

1 J 2, 2 J 3, 3 J 1, x J x for all x; and for all x and y distinct from 1, 2 and 3, x J y.

(Δ_1'), (J_1'), (J_2') and (J_4) can easily be verified, and (Δ_3) is proved

by checking each pair of co-initial cells. The developments involved are complete in each case, so (Δ_4) need only be verified when x, y and z are distinct. (Compare Remark 2.) The only such trios are $\{1,2,3\}$, $\{6,9,15\}$, $\{5,8,14\}$, and $\{4,7,13\}$.

Testing $\{6,9,15\}$ for (Δ_4):

$$^{15}/_{(6+^{9}/_{6})} = {}^{(15/6)}/_{(9/6)} = {}^{18}/_{12} = {}^{(15/9)}/_{(6/9)} = {}^{15}/_{(9+^{6}/_{9})}.$$

$$^{6}/_{(15+^{9}/_{15})} = {}^{20}/_{20} = \emptyset = {}^{12}/_{18} = {}^{6}/_{(9+^{15}/_{9})}.$$

Similarly $^{9}/_{(15+^{6}/_{15})} = \emptyset = {}^{9}/_{(6+^{15}/_{6})}$. So (Δ_4) is satisfied.

The trios $\{5,8,14\}$ and $\{4,7,13\}$ can be checked likewise.

Testing $\{1,2,3\}$:

$$^{1}/_{(2+b)} = {}^{(1/2)}/_{b} = {}^{14}/_{b} \text{ where b is either (5+11) or (8+11)}$$

$$= {}^{14}/_{(5+11)} \text{ or } {}^{14}/_{(8+11)} \quad \text{(i.e. a C. D. of } {}^{3}/_{2} \text{ ; see diagram.)}$$

$$= {}^{17}/_{11} = \{20\}$$

$$^{1}/_{(3+^{2}/_{3})} = {}^{\{6,9\}}/_{15} = \{{}^{6}/_{15}, {}^{9}/_{15}\} = \{20\} = {}^{1}/_{(2+b)}, \text{ which}$$

verifies (Δ_4) when z = 1. When z is 2 or 3 the working is similar. Thus (Δ_4) is satisfied.

(A1),...,(A3) are not satisfied together because (A3) would imply that $1 \subset 3$, $3 \subset 2$ and $2 \subset 1$, and hence (A2) would give $1 \subset 2$ and $2 \subset 1$, contradicting (A1).

Part of Curry and Feys' proof in [5] of the Church-Rosser Theorem for $\alpha\beta$-contraction is done in an abstract form, and shows that (CR) holds when there is a relation F (which only holds between co-initial cells) such that

(Δ_3) and (Δ_4) are true,

(H_0): x F y and y F x $\Longleftrightarrow$ x = y.

(H_1): x F y and y F z $\Longrightarrow$ x F z.

(H_2): (not x F y) $\Longrightarrow$ $^{x}/_{y}$ has exactly one member.

(H_3): $^{x}/_{x} = \emptyset$ for all x.

(H_4): If x F y and $z \neq y$, then for each $x' \varepsilon {}^{x}/_{z}$ there exists $y' \varepsilon {}^{y}/_{z}$ such that x' F y'.

$$\left.\begin{array}{ll} (H_5): & x' = y' \Longrightarrow x = y \\ (H_6): & x' \text{ A } y' \Longrightarrow x \text{ A } y \text{ or } x \text{ A } z \\ (H_7): & x' \text{ A } y' \Longrightarrow x \text{ A } y \text{ or (not } y \text{ A } z) \end{array}\right\} \text{for all } x' \varepsilon {}^{x}/_{z} \text{ and } y' \varepsilon {}^{y}/_{z},$$

where "x A y" means "x F y and (not y F x)".

Also $^{x}/_{y}$ is finite for all x and y.

In fact Curry and Feys prove more than (CR); they prove

(E): { Any finite set α of cells has a complete development, and if c and b are any two C. D.s of α, then $c \simeq b$.

and

(E'): { If (E) is true and z is any cell co-initial with α, then $^{z}/_{c} = {}^{z}/_{b}$.

From (E) they deduce (CR); see page 72 later. They do not actually mention the "$^{x}/_{y}$ is finite" clause that was given above, but seem to use it implicitly in the deduction of (CR) from (E).

Using (E) and (E') it can be shown that any reduction-complex satisfying (Δ_3), (Δ_4), (H_o), ..., (H_7) will satisfy (A1),... ..., (A6), (D^7) and (D^8), as long as $^x/_y$ is finite for all x and y.

Proof:

Given a complex satisfying (Δ_3), (Δ_4), (H_o), ..., (H_7), in which $^x/_y$ is always finite; define

$$x \subset y \quad \text{iff} \quad x\ F\ y \text{ and } x \neq y.$$

Then $x \subset y$ iff $x\ A\ y$, because $x\ F\ y$ implies $(y = x \iff y\ F\ x)$, by (H_o). By Remark 2; (A1),...,(A6), (D^7) and (D^8) need only be proved when the cells in their hypotheses are distinct.

For (A1): $x \subset y$ and $y \subset x \Rightarrow x\ F\ y$ and $y\ F\ x$ and $y \neq x$, contrary to (H_o).

$x \subset x \Rightarrow x\ F\ x$ and $x \neq x$, which is impossible.

For (A2): $x \subset y$ and $y \subset z \Rightarrow x\ F\ y$ and $y\ F\ z$, and $z \neq x$ by (A1)

$\Rightarrow z \neq x$ and $x\ F\ z$ by (H_1)

$\Rightarrow x \subset z$.

For (A3): $x \not\subset y \Rightarrow$ not $x\ F\ y$ (since "$x \neq y$" is assumed)

$\Rightarrow$ $^x/_y$ has only one member, by (H_2).

For (A4): Use (H_3).

For (A5): $y_1 \not\subset x$ and $y_1 \not\subset y_2 \Rightarrow$ (not $y_1\ A\ x$) and (not $y_1\ A\ y_2$)

$\Rightarrow$ not $y_1'\ A\ y_2'$, for all $y_1' \varepsilon\ ^{y_1}/_x$ and all $y_2' \varepsilon\ ^{y_2}/_x$, by (H_6).

$\Rightarrow y_1' \not\subset y_2'$, giving (A5).

For (A6): Given $y_1,\ldots,y_n$ and x with $y_i \subset x$ for $i = 1\ldots n$, Remark 4 shows (using (A1) and (A2)) that there is a y_k for which $i \neq k \Rightarrow y_i \not\subset y_k$. Since $y_k \subset x$ and "A" is the same as "$\subset$", (H_7) implies (not $y_i'\ A\ y_k'$) for all $y_i' \varepsilon\ ^{y_i}/_x$ and all $y_k' \varepsilon\ ^{y_k}/_x$. Hence $y_i' \not\subset y_k'$ as required. (For all $i \neq k$)

For (D^7) and (D^8): By Remark 4; for any co-initial cells x and y there exist MCDs a' and b' of the finite sets $^x/_y$ and $^y/_x$ respectively. The developments b, a, given by (Δ_3) are complete, because $(^x/_y)/_a = {}^x/_{y+a} = {}^x/_{x+b}$ by (Δ_4)

$= \emptyset$ by (H_3), and similarly for b.

Therefore by (E) and (E'), b and a have the same ends and residuals of z as b' and a' respectively.

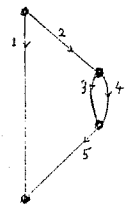
Hence $a' \simeq a \simeq b$ by (Δ_3)

$\simeq b'$

and $^z/_{y+a'} = {}^z/_{y+a} = {}^z/_{x+b}$ by (Δ_4)

$= {}^z/_{x+b'}$, proving (D^7) and (D^8).

Since (H_2) is stronger than (A3) there are systems satisfying (A1),...,(A6), (D^7), (D^8) but not (H_2) and (H_o) together, for example the simple one overleaf.



Cells are numbered from 1 to 5. The relation $\subset$ is defined to hold only between 1 and 2. (i. e. $1 \subset 2$.)

Definition of Residuals: ${}^{x}/_{x} = \emptyset$ for all x; ${}^{1}/_{2} = \{3,4\}$; ${}^{2}/_{1} = \emptyset$.

${}^{3}/_{4} = {}^{4}/_{3} = 5$.

(A1),...,(A6), (D^7) and (D^8) can fairly easily be verified, but (H_2) would imply 1 F 2, and hence not 2 F 1 by (H_o), and so ${}^{2}/_{1}$ would have to have exactly one member. This depends on ∈ being identity, so it is very weak.

To apply the abstract part of their work to αβ-contraction, Curry and Feys prove first that Church's restricted αβ-contraction satisfies (Δ_3), (Δ_4), and (H_o),...,(H_7), which imply (E), and then extend (E) to unrestricted αβ-contraction by a separate short proof, since unrestricted β-contraction does not satisfy (H_2). A more direct proof of ($CR_{\alpha\beta}$) using Theorem 2·1 will be given in Chapter 4.

In his doctoral thesis, [3], which is not yet published as far as I know, D. E. Schroer has examined abstract forms of the

Church-Rosser Theorem in detail, and his work does apply to λ-conversion. I do not think his results include mine, or mine his, but have not proved this.

Property (E)

Most of the derivations of the Church-Rosser property, except [2], this thesis and perhaps [3], have proved (E) first and derived (CR) from it, roughly as follows.

If x, y_1, ..., y_n are co-initial and b is a complete development of $\{y_1,\ldots,y_n\}$, then by (E) there must exist a C. D., e, of ${}^{x}/_{b}$ and a C. D., d, of $\{{}^{y_1}/_{x},\ldots,{}^{y_n}/_{x}\}$. (Assuming these two sets are finite.) Since x+d and b+e are both C. D.s of $\{x, y_1,\ldots,y_n\}$, (E) shows that $x+d \simeq b+e$. Hence Lemma 2·1 with C. D.s as the "special reductions" gives (CR).

Since (E) is a more powerful result than the bare Church-Rosser property, it may be interesting to know what extra conditions (if any) have to be added to (A1),...,(A6), (D^7) and (D^8) in order to derive it.

Property (D)

Also common to most of the derivations of (CR) are the two forms of property (D): one saying that to any pair of co-initial cells x and y correspond reductions b and a with $x+b \simeq y+a$ $\{$e. g. (D^7) or $(\Delta_3)\}$ and the other form saying that $z/_{x+a} = z/_{y+b}$ as well. $\{$e. g. (D^8) or (Δ_4).$\}$

In their original proof for restricted $\alpha\beta$-conversion, Church and Rosser proved separately each case of (Δ_3) that had to be used, but (Δ_4) seems so obvious in $\alpha\beta$-conversion that it was not explicitly mentioned: this omission was pointed out by Newman, and it has been suggested that it makes their proof incomplete (see [5], page 149). However Kleene does not agree with this criticism (see [9], page 285). Since the result is correct and most proofs have gaps anyway, the point at issue seems to reduce to "Did Church and Rosser know at the time that they were using (Δ_4) besides (Δ_3)?" which is not very important.

Curry says "No", he doesn't think they did.

(D^8) does not seem quite as strong as (Δ_4), and there is in the Appendix a complex possessing (A1),...,(A6), (D^7) and (D^8) yet not (Δ_4). However its residuals can easily be re-defined to give it (Δ_4), and I do not know of any examples where this re-definition is impossible. Also in the Appendix is an example showing that (Δ_3) and (Δ_4) by themselves do not imply (CR).

The history of the Church-Rosser theorem is given in [5], page 149, and short notes are in [4], [8], and page 285 of [9]. Ladrière in [10] page 376 shows how the theorem can be viewed as restricting the forms of proofs in Church's logical system based on λ-conversion (which is described in [6]).

Cells with Positions

It is interesting to note that assumptions (A1),...,(A6), (D^7) and (D^8) can be greatly simplified in the following circumstances, which are true of many relations defined by replacing parts of formulae by others, as in θ-contraction.

Every cell x is assumed to have a thing p(x) called its <u>position</u> associated with it, such that if x and y are co-initial,

$$x \neq y \implies p(x) \neq p(y)$$

but p(x) may be the same as p(y) if x and y are at different vertices. There is also assumed to be a relation $\prec$, holding between positions, such that for all positions p, q and r;

(B1) $p \prec q \implies q \not\prec p$; also $p \not\prec p$ for all p;

(B2) $p \prec q$ and $q \prec r \implies p \prec r$;

(B3) $q \prec p$ and $q \prec r \implies p = r$ or $p \prec r$ or $r \prec p$.

Then the statements "$p \prec q$", "$p = q$", "$q \prec p$" and "$p \mid q$" (which is defined as "$p \neq q$ and $p \not\prec q$ and $q \not\prec p$") are exhaustive and mutually exclusive.

<u>Definition 2·1</u> <u>Residuals</u> (of y with respect to x)

This is not a proper definition, but a set of assumptions about residuals, whose lay-out any future definition of residuals will follow.

(I) If $p(x) = p(y)$, and so $x = y$, then ${}^{y}/_{x} = {}^{x}/_{y} = \emptyset$.

(II) If $p(x) \mid p(y)$, then there is supposed to be a cell v starting at the end of x, with $p(v) = p(y)$; also a cell u starting at the end of y, with $p(u) = p(x)$, such that $x+v = y+u$. ${}^{y}/_{x}$ is $\{v\}$ $\left(\text{and } {}^{x}/_{y} \text{ is } \{u\}\right)$.

(III) If $p(x) \prec p(y)$, then either (a): ${}^{y}/_{x} = \emptyset$
or (b): ${}^{y}/_{x}$ contains only one cell, v, and $p(v) = p(y)$.

(IV) If $p(y) \prec p(x)$, then ${}^{y}/x$ is a finite or empty set of cells $\{v_1,\ldots,v_n\}$ such that $p(v_i) \prec p(x)$ or $p(v_i)=p(x)$, for i= 1...n.

To apply Theorem 2·1 to a complex like this, define

$$x \subset y \text{ iff } p(x) \prec p(y),$$

giving (A1) and (A2) from (B1) and (B2), also (A3) and (A4) from Definition 2·1.

For (A5): Suppose $p(y_1) \not\prec p(x)$ and $p(y_1) \not\prec p(y_2)$; then by Def. 2·1(I-III), either ${}^{y_1}/_{x} = \emptyset$, or ${}^{y_1}/_{x}$ has just one member y_1' and $p(y_1') = p(y_1)$.

If $p(y_2) \prec p(x)$, then for each member v of ${}^{y_2}/_{x}$, $p(v) \prec p(x)$ or $p(v) = p(x)$, by Def. 2·1(IV). Hence $p(y_1) \not\prec p(v)$, because otherwise $p(y_1) \prec p(x)$ $\{$by (B2) if $p(v) \prec p(x)\}$ which is false. Therefore $p(y_1') \not\prec p(v)$, that is $y_1' \not\subset v$, as required.

If $p(y_2) \not\prec p(x)$, then either ${}^{y_2}/_{x}$ is empty, or it contains only one member y_2' and $p(y_2') = p(y_2)$. Hence $p(y_1') \not\prec p(y_2')$; that is, $y_1' \not\subset y_2'$ as required.

(A6) and (D^7) must be checked in each particular application of this note, but (D^8) can be greatly simplified here, as follows.

For three co-initial cells x, y and z, which may be assumed distinct by Remark 2, there are 27 ways that p(x), p(y) and p(z) may be inter-related using "$\prec$". Let p = p(x), q = p(y) and r = p(z). Then

$$\left.\begin{array}{r} r \mid p \\ \text{or } r \prec p \\ \text{or } p \prec r \end{array}\right\} \text{ and } \left\{\begin{array}{r} p \mid q \\ \text{or } p \prec q \\ \text{or } q \prec p \end{array}\right\} \text{ and } \left\{\begin{array}{r} q \mid r \\ \text{or } q \prec r \\ \text{or } r \prec q \end{array}\right. .$$

Out of these 27 possibilities the following ones contradict the conjunction of (B1), (B2) and (B3). (Proved by checking each in turn.)

$r \mid p$ & $p \prec q$ & $q \prec r$	$r \prec p$, $p \prec q$, $q \prec r$
$r \mid p$, $q \prec p$, $q \prec r$	$p \prec r$, $p \mid q$, $r \prec q$
$r \mid p$, $q \prec p$, $r \prec q$	$p \prec r$, $p \prec q$, $q \mid r$
$r \prec p$, $p \mid q$, $q \prec r$	$p \prec r$, $q \prec p$, $q \mid r$
$r \prec p$, $p \mid q$, $r \prec q$	$p \prec r$, $q \prec p$, $r \prec q$
$r \prec p$, $p \prec q$, $q \mid r$	

To help in the checking, remember that (B1),...,(B3) imply that for all positions p, q and r; $p \prec q \Rightarrow q \not\prec p$; $p \not\prec p$; $p \prec q$ and $q \prec r \Rightarrow p \prec r$; $q \prec p$ and $q \prec r \Rightarrow$ not $p \mid r$; "$p \prec q$", "$q \prec p$", "$p \mid q$" are mutually exclusive; also $q \prec p$ and $p \mid r \Rightarrow q \mid r$. (because "q = r", "$q \prec r$" and "$r \prec q$" imply contradictions.)

[If q=r, then r≺p, contrary to "p|r". If q≺r, then (B3) is contradicted. If r≺q, then r≺p by (B2), contrary to "p|r".]

The remaining possibilities are:

$r \mid p$, $p \mid q$, $q \mid r$	
$r \mid p$, $p \mid q$, $q \prec r$	$p \prec r$, $p \mid q$, $q \mid r$
$r \mid p$, $p \mid q$, $r \prec q$	$r \prec p$, $p \mid q$, $q \mid r$
$r \mid p$, $p \prec q$, $q \mid r$	$r \mid p$, $q \prec p$, $q \mid r$
$r \mid p$, $p \prec q$, $r \prec q$	$r \prec p$, $q \prec p$, $q \mid r$
$r \prec p$, $p \prec q$, $r \prec q$	$r \prec p$, $q \prec p$, $r \prec q$
$p \prec r$, $p \mid q$, $q \prec r$	
$p \prec r$, $p \prec q$, $q \prec r$	$p \prec r$, $q \prec p$, $q \prec r$
$p \prec r$, $p \prec q$, $r \prec q$	$r \prec p$, $q \prec p$, $q \prec r$

If (D^8) were proved for the left-hand column of cases, the rest could be dealt with by interchanging "q" and "p".

The third and sixth cases on the left, and their mates on the right, are irrelevant because (i) and (ii) in (D^8) only require the conclusion to be true when

either (i) $r \not\prec p$ and $r \not\prec q$

or (ii) $\left\{\begin{array}{l} q \prec p \text{ and } r \prec p \text{ and } r \not\prec q \text{ and } {}^{z}/_{x} \not\subset {}^{y}/_{x}, \\ \text{or } p \prec q \text{ and } r \prec q \text{ and } r \not\prec p \text{ and } {}^{z}/_{y} \not\subset {}^{x}/_{y}. \end{array}\right.$

(Because x and y may be interchanged in (ii).)

In the first and fourth cases on the left, $r \mid p$ and $r \mid q$; in the seventh and eighth cases on the left, $p \prec r$ and $q \prec r$. Now $x + {}^{y}/_{x}$ and $y + {}^{x}/_{y}$ are both developments of $\{x, y\}$. Hence if case (a) never happens in Def. 2·1(III), then the following lemma, with

$a = \{x, y\}$, shows that ${}^{z}/_{x+y/x}$ has only one member, and the position of that member is r, in all four cases mentioned above. Similarly ${}^{z}/_{y+x/y}$ has just one member, with position r. Hence ${}^{z}/_{(x+y/x)} = {}^{z}/_{(y+x/y)}$ because two co-initial cells with the same position are identical.

2nd case on left also falls to this argument. (See p.80)

Lemma 2·4

Assuming that case (a) never happens in Def. 2·1(III):
if z is co-initial with the members of a, c is a development of a, and for all $x \in a$, either $p(x) \mid p(z)$ or $p(x) \prec p(z)$,
then ${}^{z}/_{c}$ has exactly one member, its position is $p(z)$, and for all $x' \in {}^{a}/_{c}$, either $p(x') \mid p(z)$ or $p(x') \prec p(z)$.

Proof:

Induction on the length of c is used.

When c = 0: the result is immediate.

When $c = c'+v$ and $v \in {}^{a}/_{c'}$: then by the induction-hypothesis, ${}^{z}/_{c'}$ has only one member, z', and $p(z') = p(z)$ and either $p(v) \mid p(z')$ or $p(v) \prec p(z')$. Now ${}^{z}/_{c} = {}^{z}/_{(c'+v)} = {}^{z'}/_{v}$.

If $p(v) \mid p(z')$, then by Def. 2·1(II), ${}^{z'}/_{v}$ is one cell, whose position is $p(z')$, which equals $p(z)$, giving the first part of the conclusion.

If $p(v) \prec p(z')$, then by Def. 2·1(III) and the assumption that case (a) never happens, ${}^{z'}/_{v}$ must again be one cell, whose position is $p(z')$.

Now any $x' \in {}^{a}/_{c}$ must be a member of ${}^{x''}/_{v}$ for some $x'' \in {}^{a}/_{c'}$. By the induction-hypothesis, either $p(x'') \mid p(z)$ or $p(x'') \prec p(z)$.

By Def. 2·1, since $x' \in {}^{x''}/_{v}$; $p(x') = p(x'')$ or $p(x') \prec p(v)$ or $p(x') = p(v)$. Hence either $p(x') \mid p(z)$ or $p(x') \prec p(z)$, as required. {This is immediate if $p(x') = p(x'')$ or $p(x') = p(v)$; if $p(x') \prec p(v)$ it follows from (B2) if $p(v) \prec p(z)$, and from the bottom of page 77 if $p(v) \mid p(z)$.} The lemma is now proved.

In the second case on the left on p.78; if case (a) of Def 2·1 never happens, then ${}^{z}/_{y}$ is one cell with position r. By Def. 2·1(II), ${}^{x}/_{y}$ and ${}^{y}/_{x}$ are both single cells, with positions p and q respectively. Therefore ${}^{z}/_{(y+x/y)} = {}^{(z/y)}/_{(x/y)}$ and is one cell, with position r, by Def. 2·1(II). Since $r \mid p$; ${}^{z}/_{x}$ is one cell with position r, and ${}^{z}/_{(x+y/x)} = {}^{(z/x)}/_{(y/x)}$ which is one cell with position r if case (a) never happens. Therefore ${}^{z}/_{(x+y/x)} = {}^{z}/_{(y+x/y)}$.

So when case (a) never happens in Def. 2·1(III), the only cases in (D^8) left to examine are the fifth and ninth. By part (ii) of (D^8), even these cases are only needed when ${}^{z}/_{y} \not\prec {}^{x}/_{y}$.

Summary

When

each cell x has a position p(x) such that $p(x) = p(y) \Rightarrow x = y$,
there is a relation $\prec$ satisfying (B1), (B2) and (B3),
residuals satisfy Definition 2·1, and
(B4): case (a) of Def. 2·1 never happens,

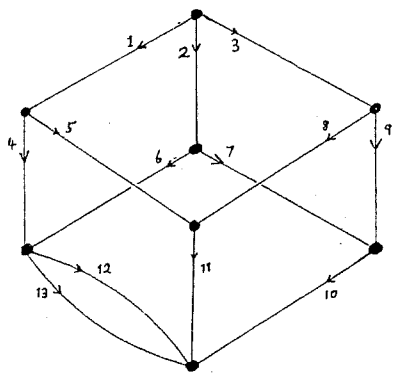
then by Theorem 2·1, the following properties together imply (CR):

$$\begin{cases} (D^7) \\ (A6) \\ (D^8) \text{ when } p(x) \prec p(y) \text{ and } p(z) \prec p(y) \text{ and } {}^{z}/_{y} \not\subset {}^{x}/_{y}, \text{ and} \\ \qquad \text{either } p(x) \mid p(z) \text{ or } p(x) \prec p(z). \end{cases}$$

This section saves quite a bit of work in Chapter 4; in β-contraction the most complicated case in which to prove ${}^{z}/_{(x+y/x)} = {}^{z}/_{(y+x/y)}$ is the sixth in the list, and this has been proved irrelevant. (as far as (D^8) is concerned.) The "${}^{z}/_{y} \not\subset {}^{x}/_{y}$" clause avoids another difficulty.

Appendix to Chapter 2

A Complex satisfying (A1),...,(A6), (D^7), (D^8), but not $(\triangle_4)$



Definition of Residuals: ${}^{x}/_{x} = \emptyset$ for all x;

${}^{1}/_{3} = 8$,	${}^{3}/_{1} = 5$,	${}^{8}/_{9} = 10$,	${}^{9}/_{8} = 11$,
${}^{2}/_{3} = 9$,	${}^{3}/_{2} = 7$,	${}^{6}/_{7} = 10$,	${}^{7}/_{6} = 13$,
${}^{1}/_{2} = 6$,	${}^{2}/_{1} = 4$,	${}^{12}/_{13} = {}^{13}/_{12} = \emptyset$.	
${}^{4}/_{5} = 11$,	${}^{5}/_{4} = 12$,		

The relation $\subset$ is defined by "$3 \subset 2$".

(A1),...,(A6) are easily verified, and (D^7) can be proved by checking each pair of cells in turn.

For (D^8): by Remark 2, the only cells to consider are $\{1, 2, 3\}$.

$${}^{1}/_{(2+3/2)} = {}^{(1/2)}/_{(3/2)} = {}^{6}/_{7} = 10 = {}^{8}/_{9} = {}^{1}/_{(3+2/3)}.$$

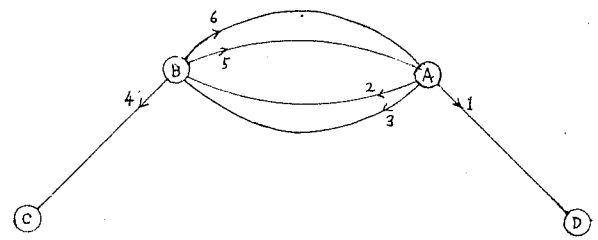
Similarly $^{2}/_{(1+^{3}/_{1})} = 11 = {}^{2}/_{(3+^{1}/_{3})}$. Since z = 3 satisfies neither (i) nor (ii) of (D^8), (D^8) has now been proved.

However (Δ_4) requires also that $^{3}/_{(1+^{2}/_{1})} = {}^{3}/_{(2+^{1}/_{2})}$, which is false because

$$^{3}/_{(1+^{2}/_{1})} = {}^{5}/_{4} = 12, \text{ yet } {}^{3}/_{(2+^{1}/_{2})} = {}^{7}/_{6} = 13.$$

But defining $^{7}/_{6} = 12$ instead of 13 gives (Δ_4), and does not upset (A1),...,(A6), (D^7) or (D^8), so this example is not very satisfactory.

<u>A Complex satisfying (Δ_3) and (Δ_4) but not (CR)</u>



Residuals: $^{x}/_{x} = \emptyset$ for all x;

$$^{1}/_{2} = {}^{1}/_{3} = \{6,5\}, \qquad {}^{2}/_{1} = {}^{3}/_{1} = \emptyset,$$
$$^{3}/_{2} = {}^{2}/_{3} = 4, \qquad {}^{5}/_{6} = {}^{6}/_{5} = 1,$$
$$^{4}/_{5} = {}^{4}/_{6} = \{2,3\}, \qquad {}^{5}/_{4} = {}^{6}/_{4} = \emptyset.$$

(Δ_3) is proved by checking each pair of cells. For $\{3,1\}$ in particular, $(6+1) = (6+^{5}/_{6})$ and so $^{(6+1)}/$ is a complete development of $\{6,5\} = {}^{1}/_{3}$. 0 is a C. D. of $^{3}/_{1}$, and $(3+(6+1)) = (1+0)$, satisfying (Δ_3).

For (Δ_4): The only co-initial trios are $\{1,2,3\}$ and $\{4,5,6\}$.

Consider $\{1,2,3\}$: by the symmetry between 2 and 3, $^{1}/_{(2+^{3}/_{2})} = {}^{1}/_{(3+^{2}/_{3})}$.

Also $^{2}/_{(3+(6+1))} = {}^{4}/_{(6+1)} = {}^{\{2,3\}}/_{1} = \emptyset = {}^{\emptyset}/_{0} = {}^{2}/_{(1+0)}$.

Hence $^{3}/_{(2+\text{ a C. D. of } ^{1}/_{2})} = {}^{3}/_{(1+\text{ a C. D. of } ^{2}/_{1})}$ by the line above and the symmetry between 2 and 3. Hence by the symmetry between $\{1,2,3\}$ and $\{4,5,6\}$, (Δ_4) must be satisfied in all cases.

However (CR) is false, because $C \sim D$ yet there is no Z with $C \geqslant Z$ and $D \geqslant Z$.

CHAPTER 3

Formulae

This chapter is just a collection of definitions and lemmas about the structure of formulae, which results will be useful later on. The concepts of occurrence of a formula, the position of one formula inside another, and replacement of parts of formulae are formalized, and the lemmas show that the definitions do have the properties one would expect.

As all the systems of formulae which I use are defined inductively, Definitions 3·1 to 3·5 will be inductive, either introducing a new predicate or being algorithms for calculating something. Since this chapter was first written, Rosza Péter has published a paper, [11], showing that such definitions correspond to primitive-recursive functions. In it she defines positions much as I do in this chapter.

Curry has also analyzed replacement & component in [19] & [5]

Definition 3·1 A typical set of formulae.

(When written with a capital "F", "Formula" will refer to the set defined here, of which λ-formulae and others are special cases.)

(i) There is assumed to be a set, not empty but perhaps infinite, of things called atoms, all of which are Formulae.

(ii) There is also a set, perhaps empty or infinite, of construction-operations ("constructors" for short), and if ϕ is any constructor, with m argument-places, $X_1,\ldots,X_m$ all being Formulae implies that $\phi(X_1,\ldots,X_m)$ is a Formula.

It is also assumed that

(a) For all constructors ϕ and Formulae $X_1, \ldots, X_m$; $\phi(X_1,\ldots,X_m)$ is not an atom.

(b) If $\phi(X_1,\ldots,X_m) = \psi(Y_1,\ldots,Y_n)$ for some constructors ϕ, ψ and Formulae $X_1,\ldots,X_m$, $Y_1,\ldots,Y_n$, then $\phi = \psi$, $m = n$ and $X_i = Y_i$ for $i = 1\ldots m$.

The letters X, Y, Z, U, V and W denote arbitrary Formulae in this chapter, and ϕ, ψ denote constructors with m and n argument-places respectively.

Example: λ-formulae have as atoms the variables and constants mentioned in Definition 0·1, the construction-operations being:

(I): putting two λ-formulae side-by-side in parentheses

(II): putting a λ-formula into parentheses with a "λx" on its left (for each variable x).

So there are an infinite number of constructors. Atoms are supposed not to contain parentheses; then (a) and (b) of Def. 3·1 can easily be proved.

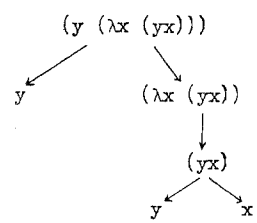
<u>Definition 3·2</u> <u>"Occurs"</u>

(i) Any Formula occurs in itself.

(ii) If ϕ is any constructor and $\phi(X_1,\ldots,X_m)$ occurs in X, then X_i occurs in X for i= 1...m.

When Y occurs in X, X is said to <u>contain</u> Y.

The Formulae occurring in X are all those obtained by breaking X down into "simpler" Formulae, for example:



(y (λx (yx))), y, (λx (yx)), (yx) and x all occur in (y (λx (yx))).

If U occurs in X, how are two different occurrences of U in X to be distinguished? The simplest way seems to be to associate

objects called "positions" with Formulae occurring in X. A position is taken to be any finite sequence of non-negative integers whose first member is o. (For convenience, zero is written "o" in positions.)

If t and s are any sequences of integers;

"ts" denotes the sequence consisting of all members of t in order followed by all the members of s in order.

$t \prec s$ (t is an "extension" of s) iff there is a non-empty sequence u such that t = su.

"t-s" denotes the position ou (NOT just u) if t = su. So t-s = o if t = s. {"ou" denotes $(o,i_1,\ldots,i_n)$ if u is $(i_1,\ldots,i_n)$.}

$t \mid s$ (t is "disjoint" from s) iff $t \not\prec s$ and $s \not\prec t$ and $t \neq s$.

The <u>length</u> of a sequence is the number of members it has.

An integer i will not be distinguished from the sequence whose only member is i, so by the above definitions, a sequence (i,j,k) may be written as "ijk". Unless stated otherwise, the letters p, q and r will denote positions in future, and in Chapters 3 and 4, s, t and u will denote finite or empty sequences of non-negative integers.

Definition 3·2 can now be expanded to include positions.

<u>Definition 3·3</u> <u>Occurring at a position</u>

(i) Any Formula occurs in itself at position o.

(ii) If $\phi(X_1,\ldots,X_m)$ occurs in X at position p, then X_i occurs in X at position pi, for i= 1...m.

"U occurs in X at position p" will often be written as "$U \subset_p X$" or as "X contains U at position p". Induction on Defs. 3·2 and 3·3 shows that $\quad U \text{ occurs in } X \iff \exists p\colon U \subset_p X,$ and if $U \subset_p X$, then only the first member of p is o.

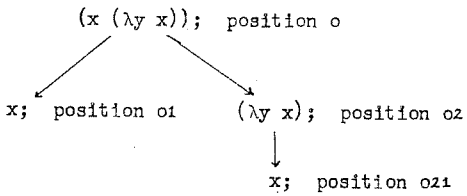
Example: For λ-formulae the definition of occurring at a position is

(i) $X \subset_o X$ for all λ-formulae X,

(ii) If $(X_1\ X_2) \subset_p X$, then $X_1 \subset_{p1} X$ and $X_2 \subset_{p2} X$.

If $(\lambda x\ X_1) \subset_p X$, then $X_1 \subset_{p1} X$.

The positions of formulae occurring in (x (λy x)) are as follows:



Definition 3·4 Components

A component of a Formula X is any ordered pair (U, p) for which $U \subset_p X$. (U, p) is also called an occurrence of U in X, and will be denoted by "$\underline{U}_p$" for short.

If $\underline{U}_p$ and $\underline{V}_q$ are components of X;

$\underline{U}_p$ is in $\underline{V}_q$ (or "$\underline{V}_q$ contains $\underline{U}_p$") iff $p = q$ or $p \prec q$,

$\underline{U}_p \mid \underline{V}_q$ (or "$\underline{U}_p$ is disjoint from $\underline{V}_q$") iff $p \mid q$.

For instance, (x (λy x)) has four components altogether; $\underline{(x\ (\lambda y\ x))}_o$, $\underline{(\lambda y\ x)}_{o2}$, $\underline{x}_{o1}$ and x_{o21}, there being two occurrences of x. Also $\underline{x}_{o21}$ is in $\underline{(\lambda y\ x)}_{o2}$ but $\underline{x}_{o1}$ is not. $\underline{x}_{o1}$ is disjoint from $\underline{x}_{o21}$.

Definition 3·5 Replacement

If $U \subset_p X$ and V is any Formula; the result, $\left\{\frac{V}{U}\,p\right\}X$, of replacing U by V at position p in X is defined by the following algorithm:

(i) $\left\{\frac{V}{X}\,o\right\}X = V$,

(ii) If $\phi(X_1,\ldots,X_m) \subset_p X$, then $\left\{\frac{V}{X_i}\,pi\right\}X = \left\{\frac{\phi(X'_1,\ldots,X'_m)}{\phi(X_1,\ldots,X_m)}\,p\right\}X$

where $X'_j = X_j$ for all $j \neq i$, and $X'_i = V$. (for $i = 1\ldots m$)

It will be shown later that (i) and (ii) do define replacement in all cases. Sometimes forming $\left\{\frac{V}{U}\,p\right\}X$ is called "replacing $\underline{U}_p$ by V".

Example: Replacing (λy x) by (zy) at position o2 in (x (λy x)):

$$\left\{\frac{(zy)}{(\lambda y\ x)}\,o2\right\}(x\ (\lambda y\ x)) = \left\{\frac{(x\ (zy))}{(x\ (\lambda y\ x))}\,o\right\}(x\ (\lambda y\ x)) \quad \text{by (ii)}$$

$$= (x\ (zy)) \quad \text{by (i)}.$$

Now it will be shown that positions, components and replacements do have the properties demanded by intuition; most of the proofs will be set out in full, even though they are quite simple.

Lemma 3·1

$s \mid t$ iff there exist u, s', t' and integers j_1 and j_2 such that $s = uj_1s'$, $t = uj_2t'$ and $j_1 \neq j_2$.

Proof:

If $s = (h_1, \ldots, h_m)$ and $t = (k_1, \ldots, k_n)$, then either there is a least number i such that $h_i \neq k_i$, in which case

$$\text{define} \begin{cases} u = \emptyset \text{ if } i = 1; \quad \text{otherwise } u = (h_1, \ldots, h_{i-1}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad = (k_1, \ldots, k_{i-1}) \\ j_1 = h_i; \quad j_2 = k_i; \\ s' = (h_{i+1}, \ldots, h_m) \text{ or } \emptyset \text{ according as } m > i \text{ or } m = i; \\ t' = (k_{i+1}, \ldots, k_n) \text{ or } \emptyset \text{ according as } n > i \text{ or } n = i, \end{cases}$$

or there is no such number, in which case $h_i = k_i$ for all i not greater than m or n, and so $s \prec t$, $s = t$ or $t \prec s$, according as $m > n$, $m = n$ or $n > m$.

Lemma 3·2

For all s, t and u;

(1): $s \not\prec s$; and $s \prec t \Rightarrow t \not\prec s$.

(2): $s \prec t$ and $t \prec u \Rightarrow s \prec u$.

(3): $u \prec s$ and $u \prec t \Rightarrow$ not $s \mid t$.

(4): $s \mid u$ and $t \prec s \Rightarrow t \mid u$.

Proof:

(1) and (2) are easily proved.

For (3): If $u = su'$ and $u = tu''$ and $s \mid t$, then $s = vis'$ and $t = vjt'$ for some sequences v, s', t' and distinct integers i, j (by Lemma 3·1). Hence $u = vis'u'$ and so $u \mid t$, contrary to the assumption that $u \prec t$.

In terms of components, this lemma implies that

$\underline{U}_p$ in $\underline{V}_q$ and $\underline{V}_q$ in $\underline{W}_r \Rightarrow \underline{U}_p$ in $\underline{W}_r$, by (2);

If $\underline{U}_p$ is in $\underline{V}_q$ and $\underline{W}_r$, then $\underline{V}_q$ is not disjoint from $\underline{W}_r$, by (3);

If $\underline{U}_p$ is in $\underline{V}_q$ and $\underline{V}_q$ is disjoint from $\underline{W}_r$, then $\underline{U}_p$ is disjoint from $\underline{W}_r$.

Note that if, in Lemma 3·1, s and t are positions, then $h_1 = k_1 = o$, and so u must also be a position if $s \mid t$.

Lemma 3·3

Two formulae cannot both occur at the same position in X;

i. e. $U \subset_p X$ and $V \subset_p X \Rightarrow U = V$.

Proof:

Induction on the length of p is used.

When p has just one member: p must be o, and so the deduction of "$U \subset_p X$" using Def. 3·3 could not have used clause (ii), because

(ii) adds a non-zero member to the position each time it is used. Hence U must be X. Similarly V = X.

When p = qi for some integer i: the deduction of "$U \subset_p X$" must have ended with an application of clause (ii), so X must contain a Formula $\phi(X_1,\ldots,X_m)$ at position q, with $U = X_i$ and $i \leqslant m$. Likewise for V there must be some $\psi(Y_1,\ldots,Y_n)$ at position q in X, with $V = Y_i$. By the induction-hypothesis applied to q, $\phi(X_1,\ldots,X_m) = \psi(Y_1,\ldots,Y_n)$. Hence by Def. 3·1(b); $\phi = \psi$, m = n and $X_j = Y_j$ for j = 1...m. Therefore $V = X_i = U$.

<u>Corollary 3·3</u> $\quad Y \subset_o X \Rightarrow Y = X$.

This follows from Lemma 3·3 because $X \subset_o X$ by Def. 3·3.

<u>Lemma 3·4</u>

If t is a possibly empty sequence of integers, and X contains V at position q, then

V contains U at position ot $\Leftrightarrow$ X contains U at position qt.

In short: If $V \subset_q X$, then $U \subset_{ot} V \Leftrightarrow U \subset_{qt} X$.

<u>Proof</u>:

Induction on the length of t is used.

When t is empty: $U \subset_q X \Leftrightarrow U = V$, by Lemma 3·3,

and $U = V \Leftrightarrow U \subset_o V$, by Corollary 3·3 and Def. 3·3(i).

When t = si for some s and i:

$U \subset_{qsi} X \Rightarrow$ clause (ii) is the clause of Def. 3·3 used last in the deduction of "$U \subset_{qsi} X$",

$\Rightarrow$ X contains a Formula $\phi(X_1,\ldots,X_m)$ at position qs and $U = X_i$ (and $i \leqslant m$).

$\Rightarrow \phi(X_1,\ldots,X_m) \subset_{os} V$, by the induction-hypothesis app. to s.

$\Rightarrow U \subset_{osi} V$ by Def 3·3(ii). That is, $U \subset_{ot} V$.

$U \subset_{osi} V \Rightarrow$ V contains a Formula $\phi(X_1,\ldots,X_m)$ at position os, and $U = X_i$ (and $i \leqslant m$).

$\Rightarrow \phi(X_1,\ldots,X_m) \subset_{qs} X$ by the induction-hypothesis,

$\Rightarrow U \subset_{qsi} X$, that is $U \subset_{qt} X$, completing the proof.

<u>Corollary 3·4</u>

If $\underline{U}_p$ and $\underline{V}_q$ are components of X and $\underline{U}_p$ is in $\underline{V}_q$, then $U \subset_{p-q} V$.

<u>Proof</u>:

$\underline{U}_p$ in $\underline{V}_q \Rightarrow \exists t$: p = qt, (and so p-q = ot)

$\Rightarrow U \subset_{ot} V$ by Lemma 3·4.

So p-q may be thought of as the position of $\underline{U}_p$ in $\underline{V}_q$.

Lemma 3·5

$$U \subset_{rjt} X \iff \exists \phi, X_1, \ldots, X_m : \phi(X_1, \ldots, X_m) \subset_r X \text{ and } U \subset_{ot} X_j \quad (\text{and } 1 \leq j \leq m).$$

Proof:

If $U \subset_{ot} X_j$ and $\phi(X_1, \ldots, X_m) \subset_r X$, then $X_j \subset_{rj} X$ by Def. 3·3, and so $U \subset_{rjt} X$ by Lemma 3·4.

The converse is proved by induction on the deduction of "$U \subset_{rjt} X$".

Basis: rjt cannot be o.

Induction-step: When there are ψ and $Y_1, \ldots, Y_n$ such that $\psi(Y_1, \ldots Y_n) \subset_q X$ and $rjt = qi$ and $U = Y_i$ (and $i \leq n$):

If t is empty, then q=r and i = j; hence $\psi(Y_1, \ldots, Y_n) \subset_r X$ and $U \subset_o Y_j$ by Def. 3·3(i). This is the result.

If t is not empty, the last member of t must be i; say t = si.

Hence q = rjs. By the induction-hypothesis applied to q and $\psi(Y_1, \ldots, Y_n)$, X must contain some Formula $\phi(X_1, \ldots, X_m)$ at position r, and $\psi(Y_1, \ldots, Y_n) \subset_{os} X_j$ (and $j \leq m$). Therefore $Y_i \subset_{osi} X_j$, that is $U \subset_{osi} X_j$.

Corollary 3·5

(1): If $1 \leq j \leq m$ and U occurs in X_j at position ot, then U occurs in $\phi(X_1, \ldots, X_m)$ at position ojt. (From the first part of the proof.)

(2): If $U \subset_p X$ and $p < r$, then X contains some Formula $\phi(X_1, \ldots, X_m)$ at position r and one of $X_1, \ldots, X_m$ contains U.

Proof of (2):

If p = rs for some non-empty s, then p = rjt, where j is the first member of s. Lemma 3·5 now gives the result.

Lemma 3·6

If $U \subset_p X$, $V \subset_q X$ and $p \mid q$, so that p = ris and q = rjt for some s, t and distinct integers i and j, then X contains some Formula $\phi(X_1, \ldots, X_m)$ at position r, with $U \subset_{os} X_i$ and $V \subset_{ot} X_j$. $\begin{cases} \text{and} \\ i \leq m \\ \& \ j \leq m. \end{cases}$

Proof:

If p = ris and q = rjt, then by Lemma 3·5 there exist ϕ, $X_1, \ldots, X_m$ such that $\phi(X_1, \ldots, X_m) \subset_r X$ and $U \subset_{os} X_i$. Also there exist ψ, $Y_1, \ldots Y_n$ such that $\psi(Y_1, \ldots, Y_n) \subset_r X$ and $V \subset_{ot} Y_j$. By Lemma 3·3, $\phi(X_1, \ldots, X_m) = \psi(Y_1, \ldots, Y_n)$ and so by def. 3·1(b), $\phi = \psi$, m = n and $X_k = Y_k$ for k= 1...m. Hence $V \subset_{ot} X_j$, as required.

Lemma 3·7

If $\underline{U}_p$ and $\underline{V}_q$ are components of X and $\underline{U}_p$ is in $\underline{V}_q$, then either $\underline{U}_p = \underline{V}_q$, or there exist ϕ, $X_1, \ldots, X_m$ such that $V = \phi(X_1, \ldots, X_m)$ and $\underline{U}_p$ is in one of the components $\underline{X}_{1_{qi}}, \ldots, \underline{X}_{m_{qm}}$.

Proof:

First note that if $V = \phi(X_1,\ldots,X_m)$, then for $i = 1\ldots m$, $X_i \subset_{qi} X$, so $\underline{X_i}_{qi}$ is a component of X.

Since $\underline{U}_p$ is in $\underline{V}_q$, either $p = q$ or $p \prec q$.

If $p = q$, then $\underline{U}_p = \underline{V}_q$ by Lemma 3·3.

If $p \prec q$, then $p = qt$ for some non-empty t; hence $p = qis$ for some i and (perhaps empty) s. Therefore by Lemma 3·5, there exist ϕ, $X_1,\ldots,X_m$ such that $\phi(X_1,\ldots,X_m) \subset_q X$. By Lemma 3·3, $\phi(X_1,\ldots,X_m) = V$. $\underline{U}_p$ is in $\underline{X_i}_{qi}$ because $p \prec qi$.

Corollary 3·7

(1): If $\underline{U}_p$ and $\underline{\phi(X_1,\ldots,X_m)}_q$ are components of X and $\underline{U}_p$ is in $\underline{\phi(X_1,\ldots,X_m)}_q$, then either $\underline{U}_p = \underline{\phi(X_1,\ldots,X_m)}_q$ or $\underline{U}_p$ is in an $\underline{X_i}_{qi}$.

{Hence if U occurs in $\phi(X_1,\ldots,X_m)$, then either $U = \phi(X_1,\ldots,X_m)$ or U occurs in X_i for some i. (with $1 \leq i \leq m$)}

(2): If U occurs in an atom X, then U = X and the position of U in X must be o.

(3): If $U \subset_p X$, $V \subset_q X$ and V is an atom, then $p \not\prec q$.

(4): If atoms occur at two distinct positions p and q in a Formula, p must be disjoint from q.

Proofs:

For (1), use Lemma 3·7 and the fact that a Formula can be expressed as $\phi(X_1,\ldots,X_m)$ in only one way, by Def. 3·1(b). The part in brackets follows by putting q = o in the first part, and using Corollary 3·4 to show that U occurs in X_i.

For (3): if $p \prec q$, then $\underline{U}_p$ is in $\underline{V}_q$, and hence by Lemma 3·7 and Def. 3·1(a), p = q, contradicting the assumption that $p \prec q$.

For (2): if $U \subset_p X$, then by (3) with q = o and V = X; $p \not\prec o$. Hence p = o, since the first member of p is o. By Corollary 3·3, U = X.

(4) follows from (3) and the definition of "disjoint".

Lemma 3·8

$$X \subset_p X \quad \Rightarrow \quad p = o.$$

Proof:

Induction on the definition of X is used.

When X is an atom: Corollary 3·7(2) gives the result.

When X is $\phi(X_1,\ldots,X_m)$: If $p \neq o$, then by the second part of Corollary 3·7(1), $X \subset_q X_i$ for some q and i (with $1 \leq i \leq m$). That is, $\phi(X_1,\ldots,X_m) \subset_q X_i$. Therefore $X_i \subset_{qi} X_i$ by Def. 3·3, and so by the induction-hypothesis, qi = o, which is impossible.

Corollary 3·8

If U occurs at distinct positions p and q in a Formula, then $p \mid q$.

Proof:

If $p \prec q$, then $U \subset_{p-q} U$ by Corollary 3·4, and hence p-q = o, by Lemma 3·8. Hence p = q, which is false. Similarly $q \not\prec p$.

Replacement

It may help the reader in understanding the next few proofs and some in Chapter 4 if he sometimes ignores the positions and reads "$\left\{\frac{V}{U}\right\}X$" for "$\left\{\frac{V}{U}p\right\}X$".

Lemma 3·9

Definition 3·5 does define replacement uniquely, for all U, p and X.

Proof:

Use induction on the deduction of "$U \subset_p X$".

When U = X and p = o: only clause (i) of Def. 3·5 can apply.

When $U = X_i$, $p = qi$ and $\phi(X_1,\ldots,X_m) \subset_q X$ (and $i \leqslant m$): only clause (ii) can apply. If X contained another Formula $\psi(Y_1,\ldots,Y_n)$ at position q with $U = Y_i$ (and $i \leqslant n$), then $\phi(X_1,\ldots,X_m) = \psi(Y_1,\ldots,Y_n)$ by Lemma 3·3, and hence $\phi = \psi$, m = n and $X_k = Y_k$ for k= 1...m, by Def. 3·1(b). So there is only one possible way of applying (ii), and the result follows by applying the induction-hypothesis to $\phi(X_1,\ldots,X_m)$ and q.

Lemma 3·10

If X contains U at position p, then

(1): $\left\{\frac{V}{U}p\right\}X$ contains V at position p,

(2): $\left\{\frac{W}{V}p\right\}\left\{\frac{V}{U}p\right\}X = \left\{\frac{W}{U}p\right\}X$,

(3): $\left\{\frac{U}{U}p\right\}X = X$.

Proof:

(1), (2) and (3) are proved together by induction on the deduction of "$U \subset_p X$".

When U = X and p = o: $\left\{\frac{V}{U}o\right\}X = V$, containing V at position o.

$\left\{\frac{W}{V}o\right\}\left\{\frac{V}{U}o\right\}X = \left\{\frac{W}{V}o\right\}V = W = \left\{\frac{W}{U}o\right\}X$. (using Def 3·5(i))

Also $\left\{\frac{U}{U}o\right\}X = U = X$.

When $U = X_i$, $p = qi$, and $\phi(X_1,\ldots,X_m) \subset_q X$ (and $i \leqslant m$):

Define, for any Formula Z, "$\phi(\ldots Z\ldots)$" to mean $\phi(X'_1,\ldots,X'_m)$, where $X'_j = X_j$ if $j \neq i$, and $X'_i = Z$. So $\phi(\ldots U\ldots) = \phi(X_1,\ldots,X_m)$ because $U = X_i$.

By Def. 3·5, $\left\{\frac{V}{U}qi\right\}X = \left\{\frac{\phi(\ldots V\ldots)}{\phi(\ldots U\ldots)}q\right\}X$ which contains $\phi(\ldots V\ldots)$ at position p by the induction-hypothesis. Hence $V \subset_{qi} \left\{\frac{V}{U}qi\right\}X$ by Def 3·3(ii), giving (1).

If V = U, then $\phi(\ldots V\ldots) = \phi(\ldots U\ldots)$, and so by the induction-hypothesis, $\left\{\frac{\phi(\ldots V\ldots)}{\phi(\ldots U\ldots)}q\right\}X = X$. Hence (3).

For (2); $\left\{\frac{W}{V}qi\right\}\left\{\frac{V}{U}qi\right\}X = \left\{\frac{\phi(\ldots W\ldots)}{\phi(\ldots V\ldots)}q\right\}\left\{\frac{\phi(\ldots V\ldots)}{\phi(\ldots U\ldots)}q\right\}X$ by above,

$$= \left\{\frac{\phi(\ldots W\ldots)}{\phi(\ldots U\ldots)}q\right\}X \text{ by the induction-hypothesis,}$$

$$= \left\{\frac{W}{U}qi\right\}X \quad \text{by Def. 3·5.}$$

Note: in (2), both sides of the equation do exist; this will either be proved or obvious whenever an equation is asserted in the rest of this chapter.

Corollary 3·10

$$\left\{\frac{U}{V}p\right\}\left\{\frac{V}{U}p\right\}X = X.$$

Proof:

$$\left\{\frac{U}{V}p\right\}\left\{\frac{V}{U}p\right\}X = \left\{\frac{U}{U}p\right\}X \text{ by (2), and this is the same as X, by (3).}$$

Lemma 3·11

If X contains W at position q and W contains U at position ot,

then
$$\left\{\frac{V}{U}qt\right\}X = \left\{\frac{\left\{\frac{V}{U}ot\right\}W}{W}q\right\}X.$$

(Roughly speaking; replacing $\underline{U}_{qt}$ by V has the same effect as replacing $\underline{W}_q$ by $\left\{\frac{V}{U}ot\right\}W$.)

Proof:

By Lemma 3·4, $U \subset_{qt} X$, so $\left\{\frac{V}{U}qt\right\}X$ does exist. Now the equation will be proved by induction on the deduction of "$U \subset_{ot} W$".

When U = W and ot = o (i.e. t is empty):

$$\left\{\frac{\left\{\frac{V}{U}o\right\}W}{W}q\right\}X = \left\{\frac{\left\{\frac{V}{U}o\right\}U}{U}q\right\}X = \left\{\frac{V}{U}q\right\}X \quad \text{by Def. 3·5.}$$

When $U = X_i$ and ot = osi (i.e. t = si) and $\phi(X_1,\ldots,X_m) \subset_{os} W$ (and $i \leqslant m$): define "$\phi(\ldots Z\ldots)$" as on page 97, for any Z.

$$\left\{\frac{\left\{\frac{V}{U}osi\right\}W}{W}q\right\}X = \left\{\frac{\left\{\frac{\phi(\ldots V\ldots)}{\phi(\ldots U\ldots)}os\right\}W}{W}q\right\}X \quad \text{by Def. 3·5(ii),}$$

$$= \left\{\frac{\phi(\ldots V\ldots)}{\phi(\ldots U\ldots)}qs\right\}X \quad \text{by the induction-hypothesis applied to } \phi(\ldots U\ldots),$$

$$= \left\{\frac{V}{U}qsi\right\}X \quad \text{by Def. 3·5(ii).}$$

Corollary 3·11

(1): If $X = \phi(X_1,\ldots,X_m)$ and $U \subset_{ot} X_i$ for some i with $1 \leqslant i \leqslant m$,

then
$$\left\{\frac{V}{U}oit\right\}X = \phi(\ldots \left\{\frac{V}{U}ot\right\}X_i\ldots)$$

(2): If $Z \subset_q X$ and $U \subset_{ot} W$, then

$$\left\{\frac{V}{U}qt\right\}\left\{\frac{W}{Z}q\right\}X = \left\{\frac{\left\{\frac{V}{U}ot\right\}W}{Z}q\right\}X.$$

Proof:

(1): By Def. 3·3, $X_i \subset_{oi} X$. Therefore by Lemma 3·11,

$$\left\{\frac{V}{U}oit\right\}X = \left\{\frac{\left\{\frac{V}{U}ot\right\}X_i}{X_i}oi\right\}X \quad \text{(Here, q = oi.)}$$

$$= \left\{\frac{\phi(\ldots\left\{\frac{V}{U}ot\right\}X_i\ldots)}{\phi(\ldots X_i \ldots)}o\right\}X \quad \text{by Def. 3·5(ii).}$$

$$= \phi(\ldots \left\{\frac{V}{U}ot\right\}X_i\ldots) \quad \text{by Def. 3·5(i).}$$

(2): By Lemma 3·10(1), $W \subset_q \left\{\frac{W}{Z} q\right\} X$.

Therefore by Lemma 3·11, $\left\{\frac{V}{U} qt\right\}\left\{\frac{W}{Z} q\right\} X = \left\{\frac{\left\{\frac{V}{U} ot\right\} W}{W} q\right\}\left\{\frac{W}{Z} q\right\} X$

$$= \left\{\frac{\left\{\frac{V}{U} ot\right\} W}{Z} q\right\} X$$

by Lemma 3·10(2).

Lemma 3·12

If U and Z occur in X at disjoint positions p and q respectively, then Z occurs at position q in $\left\{\frac{V}{U} p\right\} X$, and

$$\left\{\frac{W}{Z} q\right\}\left\{\frac{V}{U} p\right\} X = \left\{\frac{V}{U} p\right\}\left\{\frac{W}{Z} q\right\} X.$$

That is, roughly, replacing $\underline{U}_p$ does not affect $\underline{Z}_q$, and the order in which the two replacements are done does not affect their result.

Proof:

By Lemma 3·1 there exist r, s, t, i, j such that p = ris, q = rjt and $i \neq j$; by Lemma 3·6 there exist ϕ, $X_1, \ldots, X_m$ such that $\phi(X_1, \ldots, X_m) \subset_r X$, $U \subset_{os} X_i$ and $Z \subset_{ot} X_j$ (and $i \leq m$ and $j \leq m$).

For any Formulae Y_1 and Y_2, define "$\phi(..Y_1 \ldots Y_2..)$" to denote $\phi(X_1', \ldots, X_m')$ where $X_i' = Y_1$, $X_j' = Y_2$ and $X_k' = X_k$ for all k distinct from i and j.

Case 1: When r = o: then by Corollary 3·3, $\phi(X_1, \ldots, X_m) = X$.

Therefore $\left\{\frac{V}{U} p\right\} X = \left\{\frac{V}{U} ois\right\} X = \phi(.. \left\{\frac{V}{U} os\right\} X_i \ldots X_j ..)$

by Corollary 3·11(1).

By Corollary 3·5(1), $Z \subset_{ojt} \phi(.. \left\{\frac{V}{U} os\right\} X_i \ldots X_j ..)$, satisfying the first part of the theorem. Similarly $U \subset_p \left\{\frac{W}{Z} q\right\} X$, so $\left\{\frac{V}{U} p\right\}\left\{\frac{W}{Z} q\right\} X$ does exist.

$$\left\{\frac{W}{Z} q\right\}\left\{\frac{V}{U} p\right\} X = \left\{\frac{W}{Z} ojt\right\} \phi(.. \left\{\frac{V}{U} os\right\} X_i \ldots X_j ..)$$

$$= \phi(.. \left\{\frac{V}{U} os\right\} X_i \ldots \left\{\frac{W}{Z} ot\right\} X_j ..) \quad \text{by Corollary 3·11(1).}$$

$$= \left\{\frac{V}{U} p\right\}\left\{\frac{W}{Z} q\right\} X, \quad \text{using Corollary 3·11 twice, as above.}$$

Case 2: When r contains more than one member: define Y to be $\phi(X_1, \ldots, X_m)$. Then $U \subset_{ois} Y$ and $Z \subset_{ojt} Y$ by Corollary 3·5(1); define p' = ois and q' = ojt. Applying Case 1 to p', q', U, Z and Y gives $Z \subset_{q'} \left\{\frac{V}{U} p'\right\} Y$, $\left\{\frac{W}{Z} q'\right\}\left\{\frac{V}{U} p'\right\} Y = \left\{\frac{V}{U} p'\right\}\left\{\frac{W}{Z} q'\right\} Y$;

also $U \subset_{p'} \left\{\frac{W}{Z} q'\right\} Y$.

By Lemma 3·11, $\left\{\frac{V}{U} p\right\} X = \left\{\frac{\left\{\frac{V}{U} p'\right\} Y}{Y} r\right\} X$. Hence $\left\{\frac{V}{U} p'\right\} Y \subset_r \left\{\frac{V}{U} p\right\} X$, by Lemma 3·10(1). So by Lemma 3·4, $Z \subset_{rjt} \left\{\frac{V}{U} p\right\} X$; that is $Z \subset_q \left\{\frac{V}{U} p\right\} X$. Similarly $U \subset_p \left\{\frac{W}{Z} q\right\} X$, so both Formulae in the equation in Lemma 3·12 do exist. Define Y^* to be $\left\{\frac{V}{U} p'\right\} Y$.

$\left\{\frac{W}{Z} q\right\}\left\{\frac{V}{U} p\right\} X = \left\{\frac{W}{Z} q\right\}\left\{\frac{Y^*}{Y} r\right\} X$ by above,

$$= \left\{ \frac{\left\{\frac{W}{Z}q\right\} Y^*}{Y} r \right\} X \quad \text{by Corollary 3·11(2),}$$

$$= \left\{ \frac{\left\{\frac{V}{U}p'\right\}\left\{\frac{W}{Z}q'\right\} Y}{Y} r \right\} X \quad \text{by above,}$$

$$= \left\{\frac{V}{U}p\right\}\left\{\frac{W}{Z}q\right\}X, \text{ using Lemma 3·11 and Corollary 3·11(2) as above.}$$

Lemma 3·13

If W occurs in $\left\{\frac{V}{U}p\right\}X$ at position q and $q \mid p$, then W occurs in X at position q.

Proof:

By Lemma 3·12 applied to $\left\{\frac{V}{U}p\right\}X$: $W \subset_q \left\{\frac{U}{V}p\right\}\left\{\frac{V}{U}q\right\}X$, which is the same as X by Corollary 3·10.

Relations defined by Replacement

Suppose that a relation r (it will always be obvious whether "r" denotes a relation or a position) is defined from a given set of ordered pairs as follows:

$X \; r \; Y$ iff $Y = \left\{\frac{V}{U}p\right\}X$ for some pair (U,V) in the given set, with $U \subset_p X$.

All the relations in Chapter 4 will be of this type.

Lemma 3·14

Suppose $X \subset_p Z$ and $W \subset_p Z'$: then

(1): $X \; r \; Y \Rightarrow Z \; r \left\{\frac{Y}{X}p\right\}Z$ and $\left\{\frac{X}{W}p\right\}Z' \; r \left\{\frac{Y}{W}p\right\}Z'$,

(2): $X \geqslant_r Y \Rightarrow Z \geqslant_r \left\{\frac{Y}{X}p\right\}Z$ and $\left\{\frac{X}{W}p\right\}Z' \geqslant_r \left\{\frac{Y}{W}p\right\}Z'$,

(3): $X \sim_r Y \Rightarrow Z \sim_r \left\{\frac{Y}{X}p\right\}Z$ and $\left\{\frac{X}{W}p\right\}Z' \sim_r \left\{\frac{Y}{W}p\right\}Z'$.

Proof:

(1): If $Y = \left\{\frac{V}{U}ot\right\}X$, for some member (U,V) of the given set and some position ot, then by Lemma 3·11, $\left\{\frac{Y}{X}p\right\}Z = \left\{\frac{V}{U}pt\right\}Z$, and the first part of the conclusion follows by the definition of r. For the second part; $X \subset_p \left\{\frac{X}{W}p\right\}Z'$ by Lemma 3·10(1), so by the first part, $\left\{\frac{X}{W}p\right\}Z' \; r \left\{\frac{Y}{X}p\right\}\left\{\frac{X}{W}p\right\}Z' = \left\{\frac{Y}{W}p\right\}Z'$ by Lemma 3·10(2).

(2): By induction on n; $X = X_0 \; r \; X_1 \; r \ldots r \; X_n \Rightarrow Z \geqslant_r \left\{\frac{X_n}{X}p\right\}Z$.
Basis: when n = 0, then $Z = \left\{\frac{X_n}{X}p\right\}Z$ by Lemma 3·10(3).
Induction-step: when n > 0, then $\left\{\frac{X_{n-1}}{X}p\right\}Z \; r \left\{\frac{X_n}{X}p\right\}Z$ by the second part of (1). Therefore $Z \geqslant_r \left\{\frac{X_n}{X}p\right\}Z$ by the induction-hypothesis and the transitivity of $\geqslant_r$. The second part of the conclusion is proved as for (1).

(3): By (1), $X \sim_{1r} Y \Rightarrow Z \sim_{1r} \left\{\frac{Y}{X}p\right\}Z$ and $\left\{\frac{X}{W}p\right\}Z' \sim_{1r} \left\{\frac{Y}{W}p\right\}Z'$,

and (3) follows from this as did (2) from (1).

In the next chapter Lemmas 3·1 to 3·9 will often be used without explicit mention, though applications of the more complicated corollaries and of Lemmas 3·10 to 3·14 will usually be indicated.

CHAPTER 4

λ-conversion

Theorem 2·1 will be applied here to prove the Church-Rosser Theorem for αβ-contraction, which will then be extended by Theorem 1·2 to cover Curry's newer form of contraction. To make sure that Theorem 2·1 really does apply to αβ-contraction, the results in this chapter will be proved in detail, even though most of them are just slight modifications of those in Chapters 3 and 4 of [5]. Because of this the proof of (A1),...,(A6), (D^7) and (D^8) for αβ-contraction will actually be longer than the derivation of (CR) from these properties.

λ-formulae have been defined in Def. 0·1 and further described in Chapter 3. The "constants" mentioned in Def. 0·1 are used in various applications of the λ-system; for example Church and Rosser used a constant, δ, in a way to be explained later.

In this chapter, capital letters M, N, U, V, W, X, Y and Z will denote arbitrary λ-formulae and v, w, x, y and z denote variables, unless otherwise stated. Also "formula" here will mean "λ-formula". For ease of reading, some parentheses will be omitted from formulae or parts of formulae; the outermost pair will usually be left off, and if X_1, X_2, X_3 are λ-formulae, "$X_1\ X_2\ X_3$" will be used to denote $((X_1\ X_2)\ X_3)$. Similarly "$X_1\ X_2\ X_3 \ldots X_n$" will denote $(..((X_1\ X_2)\ X_3)\ \ldots .X_n)$. Also "$(\lambda x\ X)$" may be written as "$\lambda x.\ X$". For example, "$x\ (\lambda x.\ yz)\ v\ w$" denotes $(((x\ (\lambda x\ (yz)))\ v)\ w)$.

When it plays no great part in the reasoning, the position subscript may be omitted from the symbol for a component or occurrence. For instance, $\underline{U}_p$ may be referred to as "the component $\underline{U}$", or "$\underline{U}_p$ is in $\underline{V}_q$" may be shortened to "$\underline{U}$ is in $\underline{V}$", when there is only one occurrence of U (and one of V) under consideration.

A variable x is <u>bound in</u> U iff there exist Y and q such that $(\lambda x\ Y) \subset_q U$; any occurrences of x in $\underline{(\lambda x\ Y)}_q$ are said to be <u>bound</u>. If there are occurrences of x in U which are not bound, x is said to <u>occur free</u> in U (or <u>be free</u> in U), and the occurrences in question are <u>free occurrences</u>. It can easily be shown that a variable v is free in (X Y) iff it is free in X or free in Y; and that v is free in (λx Y) iff it is free in Y and distinct from x.

A component $\underline{V}_p$ of a formula U is said to be <u>x-bound</u> iff there exist Z and q such that $(\lambda x\ Z) \subset_q U$ (and hence $Z \subset_{q1} U$) and $\underline{V}_p$ is in $\underline{Z}_{q1}$. } I.E. in scope of a λx.

Substitution of formulae for free variables is the same as in Definition 0·3. From Definition 3·1(a) and (b) (which hold for λ-formulae) by induction on the definition of X, $[N/_x]X$ can be shown to have a unique value for each N, x and X.

Define the <u>rank</u> of a λ-formula as follows:

$$\begin{cases} \text{The rank of any atom is 0;} \\ \text{If the rank of X is m and the rank of Y is n, then the rank} \\ \text{of (XY) is m+n+1;} \\ \text{If the rank of X is m, then the rank of } (\lambda x\ X) \text{ is m+1, for all x.} \end{cases}$$

<u>Lemma 4·1</u>

(1): $[x/_x]Y = Y$ for all x and Y.

(2): If x is not free in Y, then $[N/_x]Y = Y$.

(3): If w is any atom, then $[w/_x]Y$ has the same rank as Y.

(4): v is free in $[N/_x]Y \iff \begin{cases} \text{v is free in Y and } v \neq x, \\ \text{or x is free in Y and v is free in N.} \end{cases}$

These are proved in [5] as Theorem 1(a) and (b), page 95, and Lemmas 1 and 2, page 96. (3) is the reason why "rank" is a useful concept, as will be seen in the proof of Lemma 4·7.

<u>Lemma 4·2</u>

If $\underline{x}_{p_1}, \ldots, \underline{x}_{p_n}$ are the free occurrences of x in Y, and clause (iiic) of def. 0·3 is not used in evaluating $[N/_x]Y$, then

$$[N/_x]Y = \left\{\frac{N}{x}p_1\right\} \cdots \left\{\frac{N}{x}p_n\right\}Y.$$

<u>Proof</u> by induction on the definition of Y: (the cases correspond to Def 0·3)

(i): (a) When Y = x: then n = 1 and $p_1 = o$, and

$$[N/_x]x = N = \left\{\frac{N}{x}o\right\}x.$$

(b) When Y is an atom distinct from x: then there are no free occurrences of x in Y.

(ii): When Y = (UV) and the result is true for U and V:

Each $\underline{x}_{p_i}$ must be either in $\underline{U}_{o1}$ or in $\underline{V}_{o2}$ by Corollary 3·7(1); suppose $\underline{x}_{p_1},\ldots,\underline{x}_{p_m}$ are in $\underline{U}_{o1}$ and $\underline{x}_{p_{m+1}},\ldots,\underline{x}_{p_n}$ are in $\underline{V}_{o2}$. Therefore by Corollary 3·4, $\underline{x}_{p_1-o1},\ldots,\underline{x}_{p_m-o1}$ are the free occurrences of x in U, and $\underline{x}_{p_{m+1}-o2},\ldots,\underline{x}_{p_n-o2}$ are the free occurrences in V.

Then $\left[{}^{N}/_{x}\right](UV) = \left(\left[{}^{N}/_{x}\right]U \ \left[{}^{N}/_{x}\right]V\right)$ by Def. 0·3(ii),

$$= \left(\left\{\frac{N}{x}p_1-o1\right\}\cdots\left\{\frac{N}{x}p_m-o1\right\}U \quad \left\{\frac{N}{x}p_{m+1}-o2\right\}\cdots\left\{\frac{N}{x}p_n-o2\right\}V\right)$$

by the induction-hypothesis.

$$= \left\{\frac{N}{x}p_1\right\}\cdots\left\{\frac{N}{x}p_n\right\}(UV),$$ by Corollary 3·11(1), used n times.

(iii):(a) When $Y = (\lambda x\ U)$: then x is not free in Y.

(b) When $Y = (\lambda y\ U)$, $y \neq x$ and either y is not free in N or x is not free in U:

$\left[{}^{N}/_{x}\right]Y = (\lambda y\ \left[{}^{N}/_{x}\right]U)$ by Def. 0·3(iiib), and the induction-step is like (ii) above, except that now each $\underline{x}_{p_i}$ must be in $\underline{U}_{o1}$.

(c) When $Y = (\lambda y\ U)$, $y \neq x$ and y is free in N and x is free in U: then Def. 0·3(iiic) would be used in evaluating $\left[{}^{N}/_{x}\right]Y$, contrary to the assumption.

<u>Note</u>: If clause (iiic) of Def. 0·3 were used in evaluating $\left[{}^{N}/_{x}\right]Y$, then there would be a variable which was both free in N and bound in Y, so Lemma 4·2 applies to N, x, Y if no variable free in N is bound in Y.

<u>Lemma 4·3</u>

If clause (iiic) of Def. 0·3 is not used to evaluate $\left[{}^{y}/_{x}\right]X$, then v is bound in X iff v is bound in $\left[{}^{y}/_{x}\right]X$.

<u>Proof</u>:

Induction on the definition of X is used, the proof being arranged in cases to correspond to Def. 0·1.

(i): When X is an atom: v cannot be bound in X or $\left[{}^{y}/_{x}\right]X$.

(ii): When $X = (X_1\ X_2)$:

v is bound in X $\Leftrightarrow$ for some Z, $(\lambda v\ Z)$ occurs in $(X_1\ X_2)$

$\Leftrightarrow$ for some Z, $(\lambda v\ Z)$ occurs in X_1 or in X_2, (using Corollary 3·7(1).)

$\Leftrightarrow$ v is bound in $\left[{}^{y}/_{x}\right]X_1$ or in $\left[{}^{y}/_{x}\right]X_2$, by the induction-hypothesis,

$\Leftrightarrow$ v is bound in $\left[{}^{y}/_{x}\right]X$.

(iii): When X is $(\lambda w\ X_1)$:

(a): When $w = x$: By Def. 0·3(iiia), $\left[{}^{y}/_{x}\right]X = X$.

(b): When $w \neq x$, and either $w \neq y$ or x is not free in X_1:

$\left[{}^{y}/_{x}\right]X = (\lambda w\ \left[{}^{y}/_{x}\right]X_1)$, and hence

v is bound in X $\Leftrightarrow$ $v = w$ or v is bound in X_1,

$\Leftrightarrow$ $v = w$ or v is bound in $\left[{}^{y}/_{x}\right]X_1$, by the induction-hypothesis;

$\Leftrightarrow$ v is bound in $\left[{}^{y}/_{x}\right]X$.

(c): When $w \neq x$, $w = y$, and x is free in X_1:

Def. 0·3(iiic) would be used in evaluating $\left[{}^{y}/_{x}\right]X$.

Lemma 4·4

If $U \subset_q X$, no variable is both free in N and bound in X, and $\underline{U}_q$ is not x-bound;

then (1): $\left[{}^{N}/_{x}\right]U \subset_q \left[{}^{N}/_{x}\right]X$

and (2): $\left[{}^{N}/_{x}\right]\left\{\frac{V}{U}q\right\}X = \left\{\frac{\left[{}^{N}/_{x}\right]V}{\left[{}^{N}/_{x}\right]U}q\right\}\left[{}^{N}/_{x}\right]X.$

Proof:

Since $\underline{U}_q$ is not x-bound, the free occurrences $\underline{x}_{ot_1},\ldots,\underline{x}_{ot_m}$ $(0 \leq m)$ of x in U correspond to free occurrences $\underline{x}_{qt_1},\ldots,\underline{x}_{qt_m}$ of x in X. Suppose $\underline{x}_{p_1},\ldots,\underline{x}_{p_n}$ are all the free occurrences of x in X. By Lemma 4·2 and the Note on page 109,

$$\left[{}^{N}/_{x}\right]X = \left\{\frac{N}{x}p_1\right\}\cdots\left\{\frac{N}{x}p_n\right\}X.$$

By Corollary 3·7(4), $p_1,\ldots,p_n$ are mutually disjoint, so by Lemma 3·12, the order of replacement of $\underline{x}_{p_1},\ldots,\underline{x}_{p_n}$ does not affect the result. Hence $\underline{x}_{qt_1},\ldots,\underline{x}_{qt_m}$ may be assumed to be the first occurrences in the list $\underline{x}_{p_1},\ldots,\underline{x}_{p_n}$; that is, $p_i = qt_i$ for $i = 1\ldots m$. Therefore

$$\left[{}^{N}/_{x}\right]X = \left\{\frac{N}{x}qt_1\right\}\cdots\left\{\frac{N}{x}qt_m\right\}X^*$$

where X^* is defined to be $\left\{\frac{N}{x}p_{m+1}\right\}\cdots\left\{\frac{N}{x}p_n\right\}X$.

Using Corollary 3·7(3), $p_{m+1},\ldots,p_n$ are all disjoint from q. $\left\{\text{because } \underline{x}_{p_{m+1}},\ldots,\underline{x}_{p_n} \text{ are not in } \underline{u}_q\right\}$ Therefore by

Lemma 3·12, $U \subset_q X^*$. By Lemma 3·11 used m times,

$$\left\{\frac{N}{x}qt_1\right\}\cdots\left\{\frac{N}{x}qt_m\right\}X^* = \left\{\frac{\left\{\frac{N}{x}ot_1\right\}\cdots\left\{\frac{N}{x}ot_m\right\}U}{U}q\right\}X^*,$$

$$= \left\{\frac{\left[{}^{N}/_{x}\right]U}{U}q\right\}X^* \text{ by Lemma 4·2, since if clause}$$

(iiic) of Def. 0·3 were used in evaluating $\left[{}^{N}/_{x}\right]U$, it would be used in evaluating $\left[{}^{N}/_{x}\right]X$. By the above and Lemma 3·10(1), $\left[{}^{N}/_{x}\right]U \subset_q \left[{}^{N}/_{x}\right]X$, proving (1).

For (2), note first that in $\left\{\frac{V}{U}q\right\}X$, the free occurrences of x are $\underline{x}_{p_{m+1}},\ldots,\underline{x}_{p_n}$ together with any that are in $\underline{V}_q$, since $\underline{V}_q$ is not x-bound.

If $\underline{V}_q$ were x-bound in $\left\{\frac{V}{U}q\right\}X$, then $\underline{V}_q$ would be in some $\underline{Z}_{p1}$ with $\underline{(\lambda x\ Z)}_p$ a component of $\left\{\frac{V}{U}q\right\}X$. By Corollary 3·10, $X = \left\{\frac{U}{V}q\right\}\left\{\frac{V}{U}q\right\}X$, so by Lemma 3·11,

$$X = \left\{\frac{\left\{\frac{U}{V}q-p\right\}(\lambda x\ Z)}{(\lambda x\ Z)}p\right\}\left\{\frac{V}{U}q\right\}X = \left\{\frac{\left(\lambda x\ \left\{\frac{U}{V}q-p1\right\}Z\right)}{(\lambda x\ Z)}p\right\}\left\{\frac{V}{U}q\right\}X \text{ by}$$

Corollary 3·11(1). Hence $\underline{U}_q$ would be x-bound in X, contrary to the assumption.

Hence $\left[{}^{N}/_{x}\right]\left\{\frac{V}{U}q\right\}X = \left\{\frac{\left[{}^{N}/_{x}\right]V}{V}q\right\}\left\{\frac{N}{x}p_{m+1}\right\}\cdots\left\{\frac{N}{x}p_n\right\}\left\{\frac{V}{U}q\right\}X$, as in the above proof of (1), but with "V" and "$\left\{\frac{V}{U}q\right\}X$" instead of "U" and "X".

$$= \left\{\frac{\left[{}^{N}/_{x}\right]V}{V}q\right\}\left\{\frac{V}{U}q\right\}\left\{\frac{N}{x}p_{m+1}\right\}\cdots\left\{\frac{N}{x}p_n\right\}X \text{ by Lemma 3·12.}$$

$$= \left\{\frac{[N/_x]V}{U}q\right\} X^*, \text{ by Lemma } 3\cdot10(2),$$

$$= \left\{\frac{[N/_x]V}{[N/_x]U}q\right\}\left\{\frac{[N/_x]U}{U}q\right\} X^*, \text{ by Lemma } 3\cdot10(2),$$

$$= \left\{\frac{[N/_x]V}{[N/_x]U}q\right\}[N/_x]X \quad \text{by the proof of (1).}$$

If x is not free in some of X, U, V, $\left\{\frac{V}{U}q\right\}X$, then some of the replacements in the preceding proof do not happen, but the main line of reasoning is the same.

Conversion

The definitions in the introduction can now be re-stated in the language of Chapter 3.

Definition 4·1 α- and β-contraction

$$X \ \alpha \ Y \quad \text{iff} \quad \begin{cases} \text{there exist } p, x \text{ and } M \text{ such that } (\lambda x\ M) \subset_p X, \\ \text{and } \ Y = \left\{\dfrac{(\lambda y\ [y/_x]M)}{(\lambda x\ M)}p\right\}X \ \text{ for some } y \text{ distinct} \\ \text{from } x \text{ and not free in } M. \end{cases}$$

$$X \ \beta \ Y \quad \text{iff} \quad \begin{cases} \text{there exist } p, x, M \text{ and } N \text{ such that} \\ ((\lambda x\ M)\ N) \subset_p X \ \text{ and } \ Y = \left\{\dfrac{[N/_x]M}{((\lambda x\ M)\ N)}p\right\}X. \end{cases}$$

In effect, α-contraction is simply changing bound variables (see later), and out of several alternatives in the literature, I have used the definition from [5] so as to be able to use some of Curry and Feys' results.

Any formula of the form $((\lambda x\ M)\ N)$ will be called a <u>β-redex</u>. (Curry and Feys in [5] use the word "redex" to denote a component, not just a formula.) The corresponding $[N/_x]M$ is called its <u>contractum</u>; each β-redex has a unique contractum, but for α-contraction, each $(\lambda x\ M)$ may be replaced by any one of an infinite set of formulae, depending on the choice of y.

Another fact which promises to cause trouble is that (D_β) is not true. That is, there exist U, X and Y such that although U β X and U β Y, there is no Z such that $X \geqslant_\beta Z$ and $Y \geqslant_\beta Z$ —— see the example overleaf.

Example: $\underline{U = (\lambda x.\ (\lambda y\ (\lambda x.\ xy))\ x)\ y}$ (and $x \neq y$)

Replacing $\underline{U}$ by

$[^y/_x](\lambda y\ (\lambda x.\ xy))\ x$

$= (\lambda y\ (\lambda x.\ xy))\ y;$

$\underline{X = (\lambda y\ (\lambda x.\ xy))\ y}$

The only possible β-contraction in X is the replacement of X by

$[^y/_y](\lambda x.\ xy),$

$= \underline{(\lambda x.\ xy)};$

Replacing $\underline{(\lambda y\ (\lambda x.\ xy))\ x}$ in U by $[^x/_y](\lambda x.\ xy)$

$= \lambda z.[^x/_y][^z/_x](xy)$ by Def. 4·3(iiic),

$= (\lambda z.\ zx);$

$\underline{Y = (\lambda x.\ (\lambda z.\ zx))\ y}$

The only possible β-contraction in Y is the replacement of Y by

$[^y/_x](\lambda z.\ zx),$

$= \underline{(\lambda z.\ zy)}.$

These two end-formulae are distinct and cannot be β-contracted, though either can be α-contracted to the other, so a good way of proving (CR) seems to be to deal with classes of α-equivalent formulae instead of the formulae themselves. This appears to be in effect what is done in [5] and [7], and is intuitively satisfying too, since α-equivalent formulae have identical interpretations.

Before going on with this line of argument, some lemmas

on substitution and α-contraction are needed. First of all, a relation α_o is defined which can be used instead of α.

Definition 4·2 α_o-contraction

$$X\ \alpha_o\ Y \text{ iff } \begin{cases} Y = \left\{\dfrac{(\lambda y\ [^y/_x]M)}{(\lambda x\ M)}\ p\right\} X \text{ for some } p, M, x \text{ and } y \\ \text{such that } y \neq x,\ y \text{ is neither free nor bound} \\ \text{in } M, \text{ and } x \text{ is not bound in } M. \end{cases}$$

Since y is not bound in M, clause (iiic) of Def. 4·3 is not used in evaluating $[^y/_x]M$; so by Lemma 4·2, α_o-contraction is a simple change of a bound variable. The "x is not bound in M" clause simplifies later proofs, and Lemma 4·7 will show $\sim_{\alpha_o}$ to be the same as $\sim_\alpha$.

Lemma 4·5

If $X \sim_\alpha Y$, then the same variables are free in X as are free in Y.

Proof:

If y is not free in M, and $y \neq x$:

v is free in $(\lambda y\ [^y/_x]M)$ $\Leftrightarrow$ $v \neq y$ and v is free in M and $v \neq x$, by Lemma 4·1(4),

$\Leftrightarrow$ v is free in $(\lambda x\ M)$, since y is not free in M.

The Lemma follows fairly easily from this.

Lemma 4·6

If r is any one of the relations α, $\geqslant_\alpha$, $\sim_\alpha$, α_o, $\geqslant_{\alpha_o}$, $\sim_{\alpha_o}$, β, $\geqslant_\beta$, or $\sim_\beta$, then by Lemma 3·14,

$$X \; r \; Y \implies (XZ) \; r \; (YZ) \text{ and } (ZX) \; r \; (ZY) \text{ and } (\lambda x \; X) \; r \; (\lambda x \; Y)$$

for all Z and x.

Lemma 4·7

$$X \sim_\alpha Y \iff X \sim_{\alpha_o} Y.$$

Proof:

Obviously $X \; \alpha_o Y \implies X \; \alpha \; Y$, so it is enough to prove that $X \; \alpha \; Y \implies X \sim_{\alpha_o} Y$, and this would be true if for all M and x,

$$(\lambda x \; M) \sim_{\alpha_o} (\lambda y \; [^y/_x]M) \quad . \; . \; . \; . \; . \; . \; . \; . \; . \; . \quad (I)$$

whenever $y \neq x$ and y is not free in M.

Now to every M, x, y such that $y \neq x$ and y is not free in M, there will be shown to correspond a formula N in which y is neither free nor bound, and in which x is not bound, such that

$$M \sim_{\alpha_o} N \text{ and } [^y/_x]N \sim_{\alpha_o} [^y/_x]M.$$

Hence (I), because

$(\lambda x \; M) \sim_{\alpha_o} (\lambda x \; N)$ by Lemma 4·6 and the definition of N,

$\alpha_o \; (\lambda y \; [^y/_x]N)$ by the definition of α_o,

$\sim_{\alpha_o} (\lambda y \; [^y/_x]M)$ by Lemma 4·6, since $[^y/_x]N \sim_{\alpha_o} [^y/_x]M$.

The existence of N is proved by induction on the rank of M, the proof

being laid out in cases to correspond to Def. 0·3.

(i): When M is an atom:

Since y is not free in M and no variable can be bound in M, let N = M.

(ii): When M is $(M_1 \; M_2)$ and N_i corresponds to M_i for i = 1 and 2:

Let $N = (N_1 \; N_2)$, giving

$$\begin{aligned} M = (M_1 \; M_2) &\sim_{\alpha_o} (N_1 \; M_2) \text{ by Lemma 4·6, since } M_1 \sim_{\alpha_o} N_1; \\ &\sim_{\alpha_o} (N_1 \; N_2) \text{ by Lemma 4·6, since } M_2 \sim_{\alpha_o} N_2; \\ &= N. \end{aligned}$$

$$\text{and } [^y/_x]N = \left([^y/_x]N_1 \;\; [^y/_x]N_2\right) \sim_{\alpha_o} \left([^y/_x]M_1 \;\; [^y/_x]M_2\right) \text{ by Lemma 4·6} = [^y/_x]M.$$

Also by the induction-hypothesis, y is neither free nor bound in $(N_1 \; N_2)$ and x is not bound in $(N_1 \; N_2)$.

(iii): When M is $(\lambda v \; M_1)$ and N_1 corresponds to M_1:

(a): When v = x:

Let $N = (\lambda w \; [^w/_x]N_1)$, where w is any variable distinct from x and y, and is neither free nor bound in N_1. Therefore x is not bound in N and y is neither free nor bound in N, by Lemmas 4·3 and 4·1(4).

Now $M = (\lambda x\, M_1) \sim_{\alpha_0} (\lambda x\, N_1)\ \alpha_0\ (\lambda w\, [^w/_x]N_1) = N$.

Therefore $M \sim_{\alpha_0} N$.

Hence $M \sim_{\alpha} N$ and so x is not free in N, by Lemma 4·5.

Therefore by Lemma 4·1(2),

$$[^y/_x]N = N \sim_{\alpha_0} M = [^y/_x]M.$$

(b): Firstly —— when $v \neq x$ and $v \neq y$:

Let $N = (\lambda v\, N_1)$. Then $M = (\lambda v\, M_1) \sim_{\alpha_0} (\lambda v\, N_1) = N$, using Lemma 4·6 and the definition of N_1.

Also $[^y/_x]N = (\lambda v\, [^y/_x]N_1)$ by Def. 0·3(iiib),

$\sim_{\alpha_0} (\lambda v\, [^y/_x]M_1)$ by Lemma 4·6 and the definition of N_1,

$= [^y/_x]M$ by Def. 0·3(iiib).

Since v is distinct from x and y; x is not bound in N and y is neither free nor bound in N.

Secondly —— when $v \neq x$ and $v = y$ and x is not free in M_1:

Let $N = (\lambda w\, [^w/_y]N_1)$, where w is distinct from x and y, and is neither free nor bound in N_1. Then as in case (a), x is not bound in N and y is neither free nor bound in N. By Lemma 4·6 and the definition of N_1; $M = (\lambda y\, M_1) \sim_{\alpha_0} (\lambda y\, N_1)\ \alpha_0\ (\lambda w\, [^w/_y]N_1) = N$. Since x is not free in M, $[^y/_x]M = M \sim_{\alpha_0} N = [^y/_x]N$ as in case (a).

(c): When $v \neq x$, $v = y$ and x is free in M_1:

Then $M = (\lambda y\, M_1)$ and $[^y/_x]M = (\lambda z\, [^y/_x][^z/_y]M_1)$, where $z \neq y$ and z is not free in M_1.

By the induction-hypothesis applied to y, z and M_1, there exists a formula W in which z is neither free nor bound, and y is not bound, such that $M_1 \sim_{\alpha_0} W$ and $[^z/_y]W \sim_{\alpha_0} [^z/_y]M_1$. Therefore

$M = (\lambda y\, M_1) \sim_{\alpha_0} (\lambda y\, W)\ \alpha_0\ (\lambda z\, [^z/_y]W) \sim_{\alpha_0} (\lambda z\, [^z/_y]M_1)$ . . . . . (II)

Now applying the induction-hypothesis to $[^z/_y]M_1$, which has the same rank as M_1 by Lemma 4·1(3), there exists N^* in which y is neither free nor bound, and x is not bound, such that

$$[^z/_y]M_1 \sim_{\alpha_0} N^* \text{ and } [^y/_x]N^* \sim_{\alpha_0} [^y/_x][^z/_y]M_1.$$

Let N be $(\lambda z\, N^*)$. $z \neq x$, since x is free in M_1 and z is not. Hence x is not bound in N, and y is neither free nor bound in N.

$N = (\lambda z\, N^*) \sim_{\alpha_0} (\lambda z\, [^z/_y]M_1)$ by the definition of N^*,

$\sim_{\alpha_0} M$ by (II) above.

Also $[^y/_x]N = (\lambda z\, [^y/_x]N^*)$ because $z \neq y$ and $z \neq x$,

$\sim_{\alpha_0} (\lambda z\, [^y/_x][^z/_y]M_1)$ by above,

$= [^y/_x]M$ as required.

From this lemma and Lemma 4·2 can be seen that in Lemma 4·5, not only are the same variables free in X as are free in Y, but the positions of their free occurrences are the same in X as in Y. To

prove this, it is enough to deduce it when $X = (\lambda x\ M)$ and $Y = (\lambda y [^y/_x]M)$ with y neither free nor bound in M and x not bound in M. But in this case the result follows by Lemmas 4·2 and 3·12, since the occurrences of any variable free in X must be disjoint from the occurrences of x.

Lemma 4·8

$$X\ \alpha_o\ Y \iff Y\ \alpha_o\ X.$$

Proof:

It suffices to show that $(\lambda y\ [^y/_x]M)\ \alpha_o\ (\lambda x\ M)$ for all x, M and y such that $y \neq x$, y is neither free nor bound in M, and x is not bound in M.

By Lemma 4·1(4), x is not free in $[^y/_x]M$; also x and y are not bound in $[^y/_x]M$, by Lemma 4·3.

Therefore $(\lambda y\ [^y/_x]M)\ \alpha_o\ (\lambda x\ [^x/_y][^y/_x]M)$. . . . . .(I)

If the free occurrences of x in M are $\underline{x}_{p_1}, \ldots, \underline{x}_{p_n}$, then the free occurrences of y in $[^y/_x]M$ are $\underline{y}_{p_1}, \ldots, \underline{y}_{p_n}$, by Lemmas 4·2 and 3·10(1).

Hence $[^x/_y][^y/_x]M = \left\{\frac{x}{y}p_1\right\} \cdots \left\{\frac{x}{y}p_n\right\}\left\{\frac{y}{x}p_1\right\} \cdots \left\{\frac{y}{x}p_n\right\} M$ by Lemma 4·2,

$= \left\{\frac{x}{y}p_1\right\}\left\{\frac{y}{x}p_1\right\} \cdots \left\{\frac{x}{y}p_n\right\}\left\{\frac{y}{x}p_n\right\} M$ by Lemma 3·12,

$= M$ by Corollary 3·10.

The result follows from this and (I) above.

Corollary 4·8

$$X \sim_\alpha Y \iff X \geqslant_\alpha Y.$$

Proof:

$X \geqslant_\alpha Y \Rightarrow X \sim_\alpha Y.$

Also $X \sim_{\alpha_o} Y \Rightarrow X\ \alpha_o\ Y$ or $Y\ \alpha_o\ X$,

$\Rightarrow X\ \alpha_o\ Y$ by Lemma 4·8.

Hence $X \sim_{\alpha_o} Y \Rightarrow X \geqslant_{\alpha_o} Y.$

Therefore $X \sim_\alpha Y \Rightarrow X \sim_{\alpha_o} Y$ by Lemma 4·7,

$\Rightarrow X \geqslant_{\alpha_o} Y \Rightarrow X \geqslant_\alpha Y.$

In future, $\sim_{\alpha_o}$ will be used interchangeably with $\sim_\alpha$.

η- and δ-contraction

In [18], Curry introduced a relation called η, defined as follows.

Definition 4·3

$$X\ \eta\ Y \text{ iff } \begin{cases} \text{there exist } M, x \text{ and } p \text{ with } x \text{ not free in } M, \\ \text{such that } (\lambda x\ (Mx)) \subset_p X, \text{ and} \\ Y = \left\{\frac{M}{(\lambda x\ (Mx))}p\right\}X. \end{cases}$$

The idea is that $(\lambda x\ (Mx))$ represents the function whose value at x is (Mx), which is the value at x of the function represented by M. Thus the functions represented by M and $(\lambda x\ (Mx))$ always have the same values.

Any formula of the form $(\lambda x\ (Mx))$ with x not free in M is called an <u>η-redex</u>, and the corresponding M is its <u>contractum</u>.

A fourth relation, δ, has been used by Church in a system of logic based on λ-conversion. (See [6].) He included a constant called "δ" amongst the atoms in the definition of λ-formulae, and then defined the relation thus:

<u>Definition 4·4</u>

$$X\ \delta\ Y \quad \text{iff} \quad \begin{cases} \text{there exist M, N and p such that } ((\delta\ M)\ N) \subset_p X, \\ \text{and } Y = \left\{\dfrac{\lambda v.\ (\lambda w.\ v\ (vw))}{((\delta\ M)\ N)}\,p\right\}X \text{ if } M \sim_\alpha N, \\ \text{but } Y = \left\{\dfrac{\lambda v.\ (\lambda w.\ (vw))}{((\delta\ M)\ N)}\,p\right\}X \text{ if } M \not\sim_\alpha N. \\ \text{Also neither M nor N contains any free variable,} \\ \text{any other formula of the form } ((\delta\ U)\ V) \text{ in which} \\ \text{no variables are free, or any } \beta\text{- or } \eta\text{-redex.} \end{cases}$$

v and w are certain chosen distinct variables, independent of X, Y and p. Note that "δ" denotes both the relation and the constant,

but this should not cause confusion.

Actually Church replaced <u>$((\delta\ M)\ N)$</u> by $(\lambda v.\ (\lambda w.\ v\ (vw)))$ only when M = N, but this is not an essential difference from Def. 4·4. In his system of logic, $(\lambda v.\ (\lambda w.\ v\ (vw)))$ represents truth and $(\lambda v.\ (\lambda w.\ (vw)))$ falsehood; a formula X being true if and only if $X \sim_{\alpha\beta\delta} (\lambda v.\ (\lambda w.\ v\ (vw)))$. For further details, see [6]: note that Church did not use η-contraction.

S. C. Kleene in [9] uses a generalized form of δ-conversion, which he calls "α-conversion". (See pages 283 – 4) To include this conversion as well as δ, Definition 4·4 is generalized as follows.

<u>Definition 4·5</u>

Certain formulae are called "δ'-redexes"; these contain no other β-, η- or δ'-redexes, and no variables occur free in them. No δ'-redex may have the form $(\lambda x\ M)$ or $((\lambda x\ M)\ N)$. With each δ'-redex is associated a contractum in which no variables are free, such that the contracta of any two α-equivalent δ'-redexes are α-equivalent.

$$X\ \delta'\ Y \quad \text{iff} \quad \begin{cases} \text{there exist p and a } \delta'\text{-redex U such that} \\ U \subset_p X \text{ and } Y = \left\{\dfrac{V}{U}\,p\right\}X, \text{ where V is the} \\ \text{contractum of U.} \end{cases}$$

The above conditions are satisfied by δ and by Kleene's generalization.

From Definitions 4·1, 4·3 and 4·5, no formula can be two sorts of redex at once, and no variable is a redex.

α-equivalence classes

An α-equivalence class (or just "a class" for short) is a non-empty set of λ-formulae such that any two of its members are α-equivalent, and any formula α-equivalent to a member is also a member.

Letters $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, $\mathcal{U}$ and $\mathcal{V}$ will denote α-equivalence classes, and the class containing X as a member will be called "$\bar{X}$", for all X.

It can be shown that no two distinct classes have members in common, and that if X is an atom, X must be the only member of $\bar{X}$. Also $\bar{X} = \bar{Y} \iff X \sim_\alpha Y$.

Definition 4·6 β-, η- and δ'-contraction of classes

$\mathcal{X}\ \beta\ \mathcal{Y}$ iff there exist $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ such that $X\ \beta\ Y$.

$\mathcal{X}\ \eta\ \mathcal{Y}$ iff there exist $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ such that $X\ \eta\ Y$.

$\mathcal{X}\ \delta'\ \mathcal{Y}$ iff there exist $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ such that $X\ \delta'\ Y$.

The Church-Rosser property

Let "r" denote any of the relations β, η, δ', βη or βηδ'.

Then $X \sim_{\alpha r} Y \Rightarrow \bar{X} \sim_r \bar{Y}$, because $X\ \alpha r\ Y \Rightarrow X\ \alpha\ Y$ or $X\ r\ Y$,

$\Rightarrow \bar{X} = \bar{Y}$ or $\bar{X}\ r\ \bar{Y}$,

$\Rightarrow \bar{X}\ \underline{r}\ \bar{Y}$.

Also $\mathcal{X} \geqslant_r \mathcal{Y} \Rightarrow \exists X,Y\colon\ X \in \mathcal{X},\ Y \in \mathcal{Y}$ and $X \geqslant_{\alpha r} Y$.

Proof: If $\mathcal{X}_0\ r\ \mathcal{X}_1\ r \ldots r\ \mathcal{X}_n$, then for $i = 1 \ldots n$, there exist $X_{i-1} \in \mathcal{X}_{i-1}$ and $Y_i \in \mathcal{X}_i$ such that $X_{i-1}\ r\ Y_i$. Then $X_0\ r\ Y_1 \sim_\alpha X_1\ r\ Y_2 \sim_\alpha X_2\ r \ldots \sim_\alpha X_{n-1}\ r\ Y_n$, which implies $X_0 \geqslant_{\alpha r} Y_n$, using Corollary 4·8.

Hence if the Church-Rosser property were true for the relation "r" among classes, it could be proved for "αr" and formulae as follows.

$$X \sim_{\alpha r} Y \Rightarrow \bar{X} \sim_r \bar{Y},$$

$$\Rightarrow \exists \mathcal{Z}\colon\ \bar{X} \geqslant_r \mathcal{Z} \text{ and } \bar{Y} \geqslant_r \mathcal{Z},$$

$$\Rightarrow \exists Z_1, Z_2, X', Y'\colon \begin{cases} X' \in \bar{X}, & Z_1 \in \mathcal{Z}, \\ Z_2 \in \mathcal{Z}, & Y' \in \bar{Y}, \text{ and} \\ X' \geqslant_{\alpha r} Z_1 \text{ and } Y' \geqslant_{\alpha r} Z_2. \end{cases}$$

$$\Rightarrow \quad X \geqslant_\alpha X' \geqslant_{\alpha r} Z_1 \geqslant_\alpha Z_2$$

and $Y \geqslant_\alpha Y' \geqslant_{\alpha r} Z_2$, using Corollary 4·8.

In the rest of the chapter, letters P, Q, R will denote redexes (β, η or δ') and the contractum of any redex R will be called "$\gamma(R)$". By a note just after Def. 4·5, R can only be one sort of redex, so $\gamma(R)$ is uniquely determined by R.

To apply Chapters 1 and 2 to the relation $\beta\eta\delta'$ among classes, a cell is defined to be any ordered pair $(p, \mathcal{X})$ for which some member of $\mathcal{X}$ contains a redex at position p. The cell is a β-, η- or δ'-cell according as this redex is a β-, η- or δ'-redex. p is called the cell's position. The start of the cell $(p, \mathcal{X})$ is $\mathcal{X}$, and its end is $\overline{\left\{\frac{\gamma(P)}{P}p\right\}X}$, for any $X \in \mathcal{X}$ with a redex P at position p. ~~Lemma 4·13 will show that this~~ end is independent of X.

By Lemma 3·2, the conditions (B1), (B2) and (B3) mentioned at the end of Chapter 2 are satisfied. Also if the positions of two co-initial cells are identical, then the cells themselves are identical.

All that should remain now is to define residuals as in Def. 2·1 and prove properties (A6), (D^7) and (D^8). Unfortunately (D^8) is not true for $\beta\eta$-cells with the most convenient definition of residuals (see [5], page 119), so the Church-Rosser property will be derived according to the following plan.

(1): Define residuals and prove (D^7) for $\beta\eta\delta'$-cells.

(2): Prove (A6) and (D^8) for β-cells only. Hence (CR_β), by the end of Chapter 2.

(3): Prove (D^2) — see Chapter 1 — with β ~~as "r" and~~ $\eta\delta'$ as "s".

(4): Prove ($D^1_{\eta\delta'}$); hence ($CR_{\eta\delta'}$) by Theorem 1·1.

(5): ($CR_{\beta\eta\delta'}$) follows from (2), (3) and (4) by Theorem 1·2.

Actually this method turns out to be nearly as short as testing $\beta\eta\delta'$-cells for (D^8) would be, so the lack of ($D^8_{\beta\eta}$) is no great hindrance. It might be possible to change the definition of residuals or cells to give ($D^8_{\beta\eta}$), but I have not managed to do so.

Before the main proof of ($CR_{\beta\eta\delta'}$) there are a few more lemmas.

<u>Lemma 4·9</u>

(1): If $x \neq y$ and y is not free in M, then

$$[M/x][N/y]X \sim_\alpha \left[[M/x]N/y\right][M/x]X.$$

(2): If x is not free in X, then

$$[M/x][N/y]X \sim_\alpha \left[[M/x]N/y\right]X.$$

<u>Proof</u>:

These are Theorem 2c of [5], page 95; noting that in (2) above, $\left[[M/x]N/y\right]X = \left[[M/x]N/y\right][M/x]X$ by Lemma 4·1(2). Also note that in [5], the condition "$x \neq y$" seems to have been missed out of the statement of Theorem $2c_1$. (It <u>is</u> necessary there.)

Lemma 4·10

$$X \sim_a Y \quad \Rightarrow \quad [M/_x]X \sim_a [M/_x]Y.$$

Proof:

This is Theorem 2a, page 95 in [5].

Lemma 4·11

$$M \sim_a N \quad \Rightarrow \quad [M/_x]X \sim_a [N/_x]X.$$

Proof:

If any variables free in M are bound in X, α_0-contractions in X can change these variables to new ones, giving a formula Y such that $X \sim_a Y$ and no variable free in M is bound in Y. Hence Def 0·3(iiic) is not used in evaluating $[M/_x]Y$, nor in evaluating $[N/_x]Y$, since the variables free in N are the same as those free in M.

Suppose $\underline{x}_{p_1}, \ldots, \underline{x}_{p_n}$ are the free occurrences (if any) of x in Y.

Then $[M/_x]Y = \left\{\frac{M}{x}p_1\right\} \cdots \left\{\frac{M}{x}p_n\right\}Y$ by Lemma 4·2,

$\sim_a \left\{\frac{N}{x}p_1\right\} \cdots \left\{\frac{N}{x}p_n\right\}Y$ by Lemma 3·14 used n times.

$= [N/_x]Y$ by Lemma 4·2.

By Lemma 4·10 and the above, $[M/_x]X \sim_a [M/_x]Y \sim_a [N/_x]Y \sim_a [N/_x]X$.

If x is not free in Y, then $[M/_x]X = X = [N/_x]X$, since by Lemma 4·5, x is not free in X.

Lemma 4·12

(1): If P is a β-, η- or δ'-redex and no variable free in N or x is bound in P, then $[N/_x]P$ is a redex of the same sort as P, and $\gamma([N/_x]P) \sim_a [N/_x]\gamma(P)$.

(2): If P is a β-, η- or δ'-redex and $P \sim_a Q$, then Q is a redex of the same sort as P, and $\gamma(Q) \sim_a \gamma(P)$.

Proof of (1):

When P is a δ'-redex:

No variables are free in either P or $\gamma(P)$; hence $[N/_x]P = P$ and $[N/_x]\gamma(P) = \gamma(P)$. Therefore $\gamma([N/_x]P) = \gamma(P) = [N/_x]\gamma(P)$.

When P is a β-redex, $((\lambda v\ U)\ V)$:

Then v cannot be free in N or x, and so $[N/_x]P = ((\lambda v\ [N/_x]U)\ [N/_x]V)$ by Def. 0·3(ii) and (iiib), since $v \neq x$. Hence $[N/_x]P$ is a β-redex.

Therefore $\gamma([N/_x]P) = \left[[N/_x]V/_v\right][N/_x]U$

$\sim_a [N/_x][V/_v]U$ by Lemma 4·9(1),

$= [N/_x]\gamma(P)$.

When P is an η-redex $(\lambda v\ (Uv))$ with v not free in U:

$[N/_x]P = (\lambda v\ ([N/_x]U\ \ v))$ and v is not free in $[N/_x]U$, by Lemma 4·1(4). Hence $[N/_x]P$ is an η-redex.

$\gamma([N/_x]P) = [N/_x]U = [N/_x]\gamma(P)$, completing the proof of (1).

Proof of (2):

For δ'-redexes, (2) is part of definition 4·5. For β- and η-redexes, it is enough to prove the result when $P \; a \; Q$.

When P is a β-redex, $((\lambda v\ U)\ V)$:

Suppose $Q = \left\{\frac{(\lambda y\ [y/x]M)}{(\lambda x\ M)}r\right\}P$, with $y \neq x$ and y not free in M.

If $\underline{(\lambda x\ M)}$ is in $\underline{U}$ or $\underline{V}$, then $Q = ((\lambda v\ U^*)\ V^*)$ where $U \underline{a} U^*$ and $V \underline{a} V^*$. Then

$$\begin{aligned} \gamma(Q) &= [V^*/v]U^* \\ &\sim_a [V/v]U^* \quad \text{by Lemma 4·11,} \\ &\sim_a [V/v]U \quad \text{by Lemma 4·10,} \\ &= \gamma(P). \end{aligned}$$

The only other possibility is that $\underline{(\lambda x\ M)}$ may be the same as $\underline{(\lambda v\ U)}$, in which case $P = ((\lambda x\ M)\ V)$, $\gamma(P) = [V/x]M$ and $Q = ((\lambda y\ [y/x]M)\ V)$.

Then

$$\begin{aligned} \gamma(Q) &= [V/y][y/x]M \\ &\sim_a \left[[V/y]y/x\right]M \quad \text{by Lemma 4·9(2), since y is not free in M;} \\ &= [V/x]M \\ &= \gamma(P). \end{aligned}$$

When P is an η-redex $(\lambda v\ (U v))$, with v not free in U:

Again suppose $Q = \left\{\frac{(\lambda y\ [y/x]M)}{(\lambda x\ M)}r\right\}P$, with $y \neq x$ and y not free in M.

If $\underline{(\lambda x\ M)}$ is in $\underline{U}$, then $Q = (\lambda v\ (U^* v))$ where $U \; a \; U^*$ and so v is not free in U^*. Therefore Q is an η-redex and $\gamma(Q) = U^* \sim_a U = \gamma(P)$. The only other possibility is for $\underline{(\lambda x\ M)}$ to be the same as $\underline{P}$. Then

$v = x$, $M = (U v)$ and $Q = (\lambda y\ [y/v](U v)) = (\lambda y\ ([y/v]U\ \ y)) = (\lambda y\ (U y))$ since v is not free in U.

Since y is not free in M, which is the same as $(U v)$, y cannot be free in U. Hence Q is an η-redex. $\gamma(Q) = U = \gamma(P)$, completing the proof of (2).

Lemma 4·13

If $X \sim_a Y$ and P is a β-, η- or δ'-redex occurring at position p in X, then at position p in Y there occurs a redex Q of the same sort as P, and $\left\{\frac{\gamma(P)}{P}p\right\}X \sim_a \left\{\frac{\gamma(Q)}{Q}p\right\}Y$.

Hence the end, $\overline{\left\{\frac{\gamma(P)}{P}p\right\}X}$, of the cell $(p, \mathcal{X})$ on page 127 is independent of X, because if X and X' are members of $\mathcal{X}$ with $P \subset_p X$ and $P' \subset_p X'$, then $\overline{\left\{\frac{\gamma(P)}{P}p\right\}X} = \overline{\left\{\frac{\gamma(P')}{P'}p\right\}X'}$.

Proof of the Lemma:

It is enough to prove the result when $X \; a_o \; Y$.

Suppose $Y = \left\{\frac{(\lambda y\ [y/x]M)}{(\lambda x\ M)}r\right\}X$, with $y \neq x$, y neither free nor bound in M, and x not bound in M.

Case (I): When $\underline{(\lambda x\ M)}_r \mid \underline{P}_p$:

Lemma 3·12 implies that $P \subset_p Y$ and $\left\{\frac{\gamma(P)}{P}p\right\}Y = \left\{\frac{(\lambda y\ [y/x]M)}{(\lambda x\ M)}r\right\}\left\{\frac{\gamma(P)}{P}p\right\}X$,

which is α-equivalent to $\left\{\frac{\gamma(P)}{P}p\right\}X$. Let Q be P.

<u>Case (II)</u>: When $\underline{(\lambda x\ M)}_r$ is in $\underline{P}_p$:

Lemma 3·11 shows that $Y = \left\{\frac{Q}{P}p\right\}X$, where Q is $\left\{\frac{(\lambda y\ [^y/_x]M)}{(\lambda x\ M)}r-p\right\}P$.

Then $Q \sim_\alpha P$, and so by Lemma 4·12(2), Q is a redex of the same sort as P and $\gamma(Q) \sim_\alpha \gamma(P)$.

$$\text{Therefore } \left\{\frac{\gamma(Q)}{Q}p\right\}Y = \left\{\frac{\gamma(Q)}{Q}p\right\}\left\{\frac{Q}{P}p\right\}X$$

$$= \left\{\frac{\gamma(Q)}{P}p\right\}X \quad \text{by Lemma 3·10,}$$

$$\sim_\alpha \left\{\frac{\gamma(P)}{P}p\right\}X \quad \text{by Lemma 3·14.}$$

<u>Case (III)</u>: When $\underline{P}_p$ is in and distinct from $\underline{(\lambda x\ M)}_r$:

$\underline{P}_p$ must therefore be in $\underline{M}_r$; that is, p = rit and $P \subset_{ot} M$ for some t. Therefore $[^y/_x]P \subset_{ot} [^y/_x]M$ by Lemma 4·4(1), since x is not bound in M and so no component of M can be x-bound.

Therefore $[^y/_x]P \subset_{oit} (\lambda y\ [^y/_x]M)$;

hence $[^y/_x]P \subset_{rit} Y$ by Lemma 3·4, since $(\lambda y\ [^y/_x]M) \subset_r Y$.

Let Q be $[^y/_x]P$; then $Q \subset_p Y$ since rit = p. By Lemma 4·12(1) with "N" being y, Q must be a redex of the same sort as P, and $\gamma(Q) \sim_\alpha [^y/_x]\gamma(P)$.

$$\text{Therefore } \left\{\frac{\gamma(Q)}{Q}ot\right\}[^y/_x]M \sim_\alpha \left\{\frac{[^y/_x]\gamma(P)}{Q}ot\right\}[^y/_x]M \quad \text{by Lemma 3·14,}$$

$$= [^y/_x]\left\{\frac{\gamma(P)}{P}ot\right\}M \quad \text{by Lemma 4·4(2)}$$

since $Q = [^y/_x]P$.

Now for any z; z free in $\gamma(P) \Rightarrow$ z free in P.

<u>Proof</u>: If P is a δ'-redex, then no variables are free in P or $\gamma(P)$.

If P is an η-redex $(\lambda v\ (Uv))$, then

z free in P $\Leftrightarrow$ z free in U and $z \neq v$

$\Leftrightarrow$ z free in U $\{$which is $\gamma(P)\}$, since v is not free in U.

If P is a β-redex $((\lambda v\ U)\ V)$, then

$$\left.\begin{array}{l}\text{z free in } \gamma(P) \\ \text{(which is } [^V/_v]U)\end{array}\right\} \Leftrightarrow \left\{\begin{array}{l}\text{either z free in V and v free in U} \\ \text{or } z \neq v \text{ and z free in U}\end{array}\right.$$

$\Rightarrow$ z free in $((\lambda v\ U)\ V)$, which is P.

Hence y is not free in $\left\{\frac{\gamma(P)}{P}ot\right\}M$, which will be called "$M^*$".

<u>Proof</u>: If y were free in M^*, then y would have to be free in $\gamma(P)$, since y is not free in M. Hence y would be free in P, by above. <u>P</u> cannot be in any component of the form $\underline{(\lambda y\ Z)}$ because y is not bound in M. Therefore the free occurrences of y in P must be free in M, contrary to y not being free in M.

$$\left\{\frac{\gamma(P)}{P}p\right\}X = \left\{\frac{(\lambda x\ M^*)}{(\lambda x\ M)}r\right\}X \quad \text{by Lemma 3·11,}$$

$$\sim_\alpha \left\{\frac{(\lambda y\ [^y/_x]M^*)}{(\lambda x\ M)}r\right\}X, \text{ since y is not free in } M^*.$$

Then $\left\{\frac{\gamma(Q)}{Q}p\right\}Y = \left\{\frac{(\lambda y\ \left\{\frac{\gamma(Q)}{Q}ot\right\}[^y/_x]M)}{(\lambda y\ [^y/_x]M)}r\right\}Y$ by Lemma 3·11,

$$= \left\{\frac{(\lambda y\ \left\{\frac{\gamma(Q)}{Q}ot\right\}[^y/_x]M)}{(\lambda y\ [^y/_x]M)}r\right\}\left\{\frac{(\lambda y\ [^y/_x]M)}{(\lambda x\ M)}r\right\}X$$

$$= \left\{\frac{(\lambda y\ \left\{\frac{\gamma(Q)}{Q}ot\right\}[^y/_x]M)}{(\lambda x\ M)}r\right\}X \text{ by Lemma 3·10(2),}$$

$$\sim_\alpha \left\{\frac{(\lambda y\ [^y/_x]\left\{\frac{\gamma(P)}{P}ot\right\}M)}{(\lambda x\ M)}r\right\}X \text{ by the bottom of page 133,}$$

$$\sim_\alpha \left\{\frac{\gamma(P)}{P}p\right\}X \text{ by the previous page.}$$

Corollary 4·13

If in Lemma 4·13, $P = ((\lambda v\ U)\ V)$ and $Q = ((\lambda z\ U')\ V')$, and $\underline{v}_{p_1},\ldots,\underline{v}_{p_n}$ $(0 \leq n)$ are the free occurrences of v in U, then $\underline{z}_{p_1},\ldots,\underline{z}_{p_n}$ are the free occurrences of z in U'.

Proof:

In case (I) of the proof of Lemma 4·13, Q was chosen to be P, so the result is immediate.

In case (II), $Q = \left\{\frac{(\lambda y\ [^y/_x]M)}{(\lambda x\ M)}r\text{-}p\right\}P$. There are three possibilities: firstly $\underline{(\lambda x\ M)}$ may be in $\underline{V}$, in which case $V \alpha V'$, $z = v$ and $U' = U$, giving the result.

next, $\underline{(\lambda x\ M)}$ may be in $\underline{U}$, and so $z = v$ and $U \alpha U'$; the

result follows from a note just after Lemma 4·7.

thirdly, $\underline{(\lambda x\ M)}$ may be $\underline{(\lambda v\ U)}$, and so $Q = ((\lambda y\ [^y/_x]M)\ V)$; Lemma 4·2 shows that $[^y/_x]M = \left\{\frac{y}{x}p_1\right\}\cdots\left\{\frac{y}{x}p_n\right\}M$ if $n > 0$, and hence the free occurrences of y in $[^y/_x]M$ are $\underline{y}_{p_1},\ldots,\underline{y}_{p_n}$ as required. If $n = 0$, that is x is not free in M, then $[^y/_x]M = M$ and so y is not free in $[^y/_x]M$.

In case (III), $\underline{P}$ is in $\underline{M}$ and hence y is neither free nor bound i and x is not bound in P. $Q = [^y/_x]P = ((\lambda v\ [^y/_x]U)\ [^y/_x]V)$, and since v must be distinct from x and y, the free occurrences of v in $[^y/_x]U$ are the same as in U. (Using Lemmas 4·2 and 3·12.)

The first step in the plan of attack outlined on page 127 is to define residuals for β-, η- and δ'-cells; the proof of (D^7) will be included in this definition. For convenience a cell $(p, \mathcal{U})$ may simply be called "p", when the value of $\mathcal{U}$ is obvious from the context.

Definition of Residuals

If $(p, \mathcal{U})$ and $(q, \mathcal{U})$ are cells, the set $(p, \mathcal{U})/(q, \mathcal{U})$ (or "p/q" by the above abbreviation) of the residuals of $(p, \mathcal{U})$ with respect to $(q, \mathcal{U})$ is defined as follows. (Compare Def. 2·1.)

First of all choose any formula $U \in \mathcal{U}$ in which

(i): no variable is both free and bound,

(ii): no variable is bound twice; more precisely, if $\underline{(\lambda x\ Z)}_{r_1}$ and $\underline{(\lambda y\ V)}_{r_2}$ are distinct components of U, then $x \neq y$.

This choice is possible because, in any member U' of $\mathcal{U}$, each component of the form $\underline{(\lambda v\ W)}_r$ can be replaced by $(\lambda w\ [w/v]W)$, where w is distinct from all the other variables free or bound in U'. After a finite sequence of such replacements a formula U of the required type will be obtained.

If $((\lambda x\ M)\ N)$ occurs in U for some x, M and N, then x is bound in neither M nor N, and no variable is both free in N and bound in M, so Lemma 4·2 applies to $[N/x]M$.

Now suppose that P and Q are the redexes at positions

p and q respectively in U. Notice that the question of whether P (or Q) is a β-, η- or δ'-redex is independent of the particular member U of $\mathcal{U}$ that has been chosen, by Lemma 4·13. Also if P or Q is a β-redex $((\lambda x\ M)\ N)$, the positions of the free occurrences of x in M are independent of U, by Corollary 4·13. Using these facts, it will be seen that the residuals depend only on p, q and $\mathcal{U}$; the only reason for choosing U as above is to simplify the proof of (D^7).

<u>Case I</u> When $p = q$:

Define $p/q = \emptyset$. (D^7) is satisfied because Q must be the same as P by Lemma 3·3, and so $\gamma(Q) = \gamma(P)$.

<u>Case II</u> When $p \mid q$:

Define $p/q = \left(p, \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right)$. This is indeed a cell because by Lemma 3·12, $P \subset_p \left\{\frac{\gamma(Q)}{Q}q\right\}U$. It depends only on p, q and $\mathcal{U}$, and it is the same sort of cell as $(p, \mathcal{U})$.

To verify (D^7):

Interchanging p and q in the above shows that $q/p = \left(q, \overline{\left\{\frac{\gamma(P)}{P}p\right\}U}\right)$.

The end of $q + p/q$ is $\overline{\left\{\frac{\gamma(P)}{P}p\right\}\left\{\frac{\gamma(Q)}{Q}q\right\}U}$ which by Lemma 3·12 is the same as $\overline{\left\{\frac{\gamma(Q)}{Q}q\right\}\left\{\frac{\gamma(P)}{P}p\right\}U}$, which is the end of $p + q/p$.

Therefore $(p + q/p) \simeq (q + p/q)$ as required.

<u>Case III</u> When $q \prec p$:

By Corollary 3·4, Q must occur in P. Therefore P cannot be a δ'-redex, by Definition 4·5.

If P is a β-redex $((\lambda z\ W)\ V)$, then there are three possibilities, by Corollary 3·7(1).

(a): If $\underline{Q}_q$ is in $\underline{W}_{p11}$, define $P/_q = \left(p,\ \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right)$.

This is a β-cell because by Lemma 3·11, $\left\{\frac{\gamma(Q)}{Q}q\right\}U = \left\{\frac{((\lambda z\ \left\{\frac{\gamma(Q)}{Q}r\right\}W)\ V)}{P}p\right\}U$ where $r = q-p11$, and so there is a β-redex at position p in $\left\{\frac{\gamma(Q)}{Q}q\right\}U$.

(b): If $\underline{Q}_q$ is in $\underline{V}_{p2}$, define $P/_q = \left(p,\ \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right)$.

This is a β-cell because $\left\{\frac{\gamma(Q)}{Q}q\right\}U = \left\{\frac{((\lambda z\ W)\ \left\{\frac{\gamma(Q)}{Q}r\right\}V)}{P}p\right\}U$ where $r = q-p2$, and so there is a β-redex at position p in $\left\{\frac{\gamma(Q)}{Q}q\right\}U$.

(c): If $\underline{Q}_q = \underline{(\lambda z\ W)}_{p1}$, define $P/_q = \emptyset$.

Note that in this situation $Q = (\lambda z\ W)$ and so must be an η-redex. Therefore $W = (N\ z)$ for some N in which z is not free.

If P is an η-redex $(\lambda z\ (W\ z))$, then there are two possibilities.

(d): If $\underline{Q}_q$ is in $\underline{W}_{p11}$, define $P/_q = \left(p,\ \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right)$.

To show that this is an η-cell: by Lemma 3·11,

$\left\{\frac{\gamma(Q)}{Q}q\right\}U = \left\{\frac{(\lambda z\ (\left\{\frac{\gamma(Q)}{Q}r\right\}W\ \ z))}{P}p\right\}U$, where $r = q-p11$, so $\left\{\frac{\gamma(Q)}{Q}q\right\}U$ contains $(\lambda z\ (\ \left\{\frac{\gamma(Q)}{Q}r\right\}W\ \ z))$ at position p. This is an η-redex because if z were free in $\left\{\frac{\gamma(Q)}{Q}r\right\}W$, then z would be free in W, as in the proof of Lemma 4·13, on page 134.

(e): If $\underline{Q}_q = \underline{(Wz)}_{p1}$, define $P/_q = \emptyset$.

Note that when this happens, Q must be $(W\,z)$ and so must be a β-redex. Hence W must be $(\lambda x\ M)$ for some x and M.

The proof of (D^7) in Case III follows from that in Case IV by interchanging p and q.

<u>Case IV</u> When $p \prec q$:

Then P occurs in Q and there are five sub-cases as in Case III.

<u>Subcase (a)</u>: If $Q = ((\lambda x\ M)\ N)$ and $\underline{P}_p$ is in $\underline{M}_{q11}$, define $P/_q = \left(qt,\ \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right)$, where $ot = p-q11$; this depends only on p, q, $\mathcal{U}$.

To show that this is indeed a cell of the same sort as $(p, \mathcal{U})$:

By Corollary 3·4, $P \subset_{ot} M$. Hence by Lemma 4·4(1) and the choice of U, $[N/_x]P \subset_{ot} [N/_x]M$. Therefore $[N/_x]P \subset_{qt} \left\{\frac{[N/_x]M}{Q}q\right\}U$, by Lemmas 3·10(1) and 3·4. But $\left\{\frac{[N/_x]M}{Q}q\right\}U = \left\{\frac{\gamma(Q)}{Q}q\right\}U$ and

and by Lemma 4·12(1), $[{}^{N}/_{x}]P$ is a redex of the same sort as P, giving the result. Call $[{}^{N}/_{x}]P$: "R".

To verify (D^7):

By Lemma 4·12(1), $\gamma(R) \sim_a [{}^{N}/_{x}]\,\gamma(P)$.

Therefore $[{}^{N}/_{x}]\left\{\frac{\gamma(P)}{P}ot\right\}M = \left\{\frac{[{}^{N}/_{x}]\,\gamma(P)}{R}ot\right\}[{}^{N}/_{x}]M$ by Lemma 4·4(2),

$\sim_a \left\{\frac{\gamma(R)}{R}ot\right\}[{}^{N}/_{x}]M$ by above.

The reduction $q+{}^{P}\!\!\swarrow_{q}$ first replaces $\underline{Q}_q$ by $\gamma(Q)$ which is $[{}^{N}/_{x}]M$, and then replaces $\underline{R}_{qt}$ by $\gamma(R)$, so the end of $q+{}^{P}\!\!\swarrow_{q}$ is

$\overline{\left\{\frac{\gamma(R)}{R}qt\right\}\left\{\frac{[{}^{N}/_{x}]M}{Q}q\right\}U}$, which is $\overline{\left\{\frac{\left\{\frac{\gamma(R)}{R}ot\right\}[{}^{N}/_{x}]M}{Q}q\right\}U}$ by Corollary 3·11(2).

Also ${}^{q}/_{p} = \left(q,\ \overline{\left\{\frac{\gamma(P)}{P}p\right\}U}\right)$ by Case III, and the redex at position q in $\left\{\frac{\gamma(P)}{P}p\right\}U$ is $((\lambda x\ M^*)\ N)$, where $M^* = \left\{\frac{\gamma(P)}{P}ot\right\}M$.

So $p+{}^{q}\!\!\swarrow_{p}$ first replaces $\underline{P}_p$ by $\gamma(P)$ and then $((\lambda x\ M^*)\ N)$ by $[{}^{N}/_{x}]M^*$.

Hence the end of $p+{}^{q}\!\!\swarrow_{p}$ is $\overline{\left\{\frac{[{}^{N}/_{x}]M^*}{((\lambda x\ M^*)\ N)}q\right\}\left\{\frac{\gamma(P)}{P}p\right\}U}$

$= \overline{\left\{\frac{[{}^{N}/_{x}]M^*}{((\lambda x\ M^*)\ N)}q\right\}\left\{\frac{((\lambda x\ M^*)\ N)}{Q}q\right\}U}$ by Lemma 3·11,

$= \overline{\left\{\frac{[{}^{N}/_{x}]M^*}{Q}q\right\}U}$ by Lemma 3·10(2).

$= \overline{\left\{\frac{\left\{\frac{\gamma(R)}{R}ot\right\}[{}^{N}/_{x}]M}{Q}q\right\}U}$ by above.

This is the same as the end of $q+{}^{P}\!\!\swarrow_{q}$.

<u>Subcase (b)</u>: If $Q = ((\lambda x\ M)\ N)$ and $\underline{P}_p$ is in $\underline{N}_{q2}$, define

${}^{P}/_{q} = \left\{\left(qs_1t,\ \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right),\ \ldots,\ \left(qs_nt,\ \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}\right)\right\}$, where $ot = p-q2$ and $os_1,\ldots,os_n$ $(0 \leqslant n)$ are the positions of the free occurrences of x in M. Then by a previous convention, ${}^{P}/_{q} = \emptyset$ if there are no free occurrences of x in M. By a note at the start of the definition, ${}^{P}/_{q}$ is independent of the choice of U.

To show that the members of ${}^{P}/_{q}$ are cells of the same sort as $(p, \mathcal{U})$:

$\gamma(Q) = [{}^{N}/_{x}]M = \left\{\frac{N}{x}os_1\right\}\ldots\left\{\frac{N}{x}os_n\right\}M$ by Lemma 4·2. Therefore N occurs in $\gamma(Q)$ at positions $os_1,\ldots,os_n$, and so P occurs in $\gamma(Q)$ at positions $os_1t,\ \ldots,\ os_nt$ by Lemma 3·4. Hence P occurs in $\left\{\frac{\gamma(Q)}{Q}q\right\}U$ at positions $qs_1t,\ \ldots,\ qs_nt$, giving the result.

To verify (D^7):

Since all the residuals' positions $qs_1t,\ \ldots,\ qs_nt$ are mutually disjoint, an MCD of ${}^{P}/_{q}$ can be formed by replacing each $\underline{P}_{qs_it}$ in turn by $\gamma(P)$. (Using the third part of Remark 6 in Chapter 2, and the fact that by Case I, ${}^{qs_it}/_{qs_jt} = qs_it$ whenever $i \neq j$.) Define $P\!\!\swarrow_{q}$ to be this MCD.

Hence the end of $q+{}^{P}\!\!\swarrow_{q}$ is $\overline{\left\{\frac{\gamma(P)}{P}qs_nt\right\}\ldots\left\{\frac{\gamma(P)}{P}qs_1t\right\}\left\{\frac{[{}^{N}/_{x}]M}{Q}q\right\}U}$

$= \overline{\left\{\frac{\left\{\frac{\gamma(P)}{P}os_nt\right\}\ldots\left\{\frac{\gamma(P)}{P}os_1t\right\}[{}^{N}/_{x}]M}{Q}q\right\}U}$

by Corollary 3·11(2) used n times.

Now $\left\{\frac{\gamma(P)}{P} os_n t\right\} \ldots \left\{\frac{\gamma(P)}{P} os_1 t\right\} \left[{}^{N}/_{x}\right] M$

$= \left\{\frac{\gamma(P)}{P} os_n t\right\} \ldots \left\{\frac{\gamma(P)}{P} os_1 t\right\} \left\{\frac{N}{x} os_n\right\} \ldots \left\{\frac{N}{x} os_1\right\} M$ by Lemma 4·2,

$= \left\{\frac{\gamma(P)}{P} os_n t\right\} \left\{\frac{N}{x} os_n\right\} \ldots \left\{\frac{\gamma(P)}{P} os_1 t\right\} \left\{\frac{N}{x} os_1\right\} M$ by Lemma 3·12,

$= \left\{\frac{N^*}{x} os_n\right\} \ldots \left\{\frac{N^*}{x} os_1\right\} M$ where $N^* = \left\{\frac{\gamma(P)}{P} ot\right\} N$, by Corollary 3·11(2),

$= \left[{}^{N^*}/_{x}\right] M$ by Lemma 4·2, since if any variable bound in M were free in N^*, it would be free in N, by part of the proof of Lemma 4·13, on p.134.

Therefore the end of $q+{}^{p}/_{q}$ is $\overline{\left\{\frac{\left[{}^{N^*}/_{x}\right] M}{Q} q\right\} U}$.

By Case III, ${}^{q}/_{p} = \left(q, \overline{\left\{\frac{\gamma(P)}{P} p\right\} U}\right)$ and the redex at position q in $\left\{\frac{\gamma(P)}{P} p\right\} U$ is $((\lambda x\ M)\ N^*)$.

So the end of $p+{}^{q}/_{p}$ is $\overline{\left\{\frac{\left[{}^{N^*}/_{x}\right] M}{((\lambda x\ M)\ N^*)} q\right\} \left\{\frac{\gamma(P)}{P} p\right\} U}$

$= \overline{\left\{\frac{\left[{}^{N^*}/_{x}\right] M}{((\lambda x\ M)\ N^*)} q\right\} \left\{\frac{((\lambda x\ M)\ N^*)}{Q} q\right\} U}$ by Lemma 3·11,

$= \overline{\left\{\frac{\left[{}^{N^*}/_{x}\right] M}{Q} q\right\} U}$ which is the end of $q+{}^{p}/_{q}$.

If x is not free in M, some of the above replacements do not happen, but the main line of reasoning is the same.

<u>Subcase (c)</u>: If $Q = ((\lambda x\ M)\ N)$ and $\underline{P}_p = \underline{(\lambda x\ M)}_{q1}$, define ${}^{p}/_{q} = \emptyset$. This is independent of U.

By Case III(c), ${}^{q}/_{p} = \emptyset$, so to verify (D^7) it must be proved

that $\overline{\left\{\frac{\gamma(P)}{P} p\right\} U} = \overline{\left\{\frac{\gamma(Q)}{Q} q\right\} U}$. $p = q1$ because $\underline{P}_p = \underline{(\lambda x\ M)}_{q1}$,

so by Lemma 3·11, $\left\{\frac{\gamma(P)}{P} p\right\} U = \left\{\frac{\left\{\frac{\gamma(P)}{P} o1\right\} Q}{Q} q\right\} U$. Hence (D^7) will be satisfied if $\left\{\frac{\gamma(P)}{P} o1\right\} Q = \gamma(Q)$.

But $P = (\lambda x\ M)$ and so must be an η-redex; hence $M = (V\ x)$ for some V in which x is not free. Therefore $Q = ((\lambda x\ (V x))\ N)$ and $\gamma(Q) = \left[{}^{N}/_{x}\right](V\ x) = (\left[{}^{N}/_{x}\right] V\ \ N) = (V\ N)$ since x is not free in V.

$\gamma(P) = V$, so $\left\{\frac{\gamma(P)}{P} o1\right\} Q = \left\{\frac{V}{(\lambda x\ (V x))} o1\right\} ((\lambda x\ (V x))\ N)$

$= (V\ N)$

$= \gamma(Q)$ as required.

Subcase (d): If $Q = (\lambda x\ (M x))$ and $\underline{P}_p$ is in $\underline{M}_{q11}$, define ${}^{p}/_{q} = \left(qt, \overline{\left\{\frac{\gamma(Q)}{Q} q\right\} U}\right)$, where $ot = p-q11$. This depends only on p, q, $\mathcal{U}$.

It is a cell because $\left\{\frac{\gamma(Q)}{Q} q\right\} U = \left\{\frac{M}{Q} q\right\} U$ which contains M at position q, and hence contains P at position qt. (Since $P \subset_{ot} M$ by Corollary 3·4.) This also shows that ${}^{p}/_{q}$ is the same sort of cell as $(p, \mathcal{U})$.

To verify (D^7):

The end of $q+{}^{p}/_{q}$ is $\overline{\left\{\frac{\gamma(P)}{P} qt\right\} \left\{\frac{\gamma(Q)}{Q} q\right\} U}$

$= \overline{\left\{\frac{\gamma(P)}{P} qt\right\} \left\{\frac{M}{Q} q\right\} U}$

$= \overline{\left\{\frac{M^*}{Q}q\right\}U}$ by Corollary 3·11(2), where $M^* = \left\{\frac{\gamma(P)}{P}ot\right\}M$.

By Case III, ${}^{q}/_{p} = \left(q, \overline{\left\{\frac{\gamma(P)}{P}p\right\}U}\right)$, and the redex at position q in $\left\{\frac{\gamma(P)}{P}p\right\}U$ is $(\lambda x\ (M^*x))$.

Therefore the end of $p+{}^{q}/_{p}$ is $\overline{\left\{\frac{M^*}{(\lambda x\ (M^*x))}q\right\}\left\{\frac{\gamma(P)}{P}p\right\}U}$

$$= \overline{\left\{\frac{M^*}{(\lambda x\ (M^*x))}q\right\}\left\{\frac{(\lambda x\ (M^*x))}{Q}q\right\}U}$$

by Lemma 3·11;

$$= \overline{\left\{\frac{M^*}{Q}q\right\}U}, \text{ which is the end of } q+{}^{P}/_{q}.$$

<u>Subcase (e)</u>: If $Q = (\lambda x\ (M\ x))$ and $\underline{P}_p = \underline{(M\ x)}_{q1}$, define ${}^{P}/_{q} = \emptyset$. This is independent of the chosen U. Since ${}^{q}/_{p} = \emptyset$ by Case III, (D^7) follows if it is shown that

$$\overline{\left\{\frac{\gamma(P)}{P}p\right\}U} = \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}.$$

Similarly to Subcase (c), it is enough to show that $\left\{\frac{\gamma(P)}{P}o1\right\}Q \sim_\alpha \gamma(Q)$.

$P = (M\ x)$ and so P must be a β-redex. Therefore $M = (\lambda y\ V)$ for some y and V, and hence $Q = (\lambda x\ ((\lambda y\ V)\ x))$. Then $\gamma(Q) = (\lambda y\ V)$.

P is $((\lambda y\ V)\ x)$, so $\gamma(P) = [{}^{x}/_{y}]V$.

Therefore $\left\{\frac{\gamma(P)}{P}o1\right\}Q = \left\{\frac{[{}^{x}/_{y}]V}{(M\ x)}o1\right\}(\lambda x\ (M\ x)) = (\lambda x\ [{}^{x}/_{y}]V)$.

So (D^7) would follow if $(\lambda y\ V) \sim_\alpha (\lambda x\ [{}^{x}/_{y}]V)$. But $x \neq y$ since no variable is bound twice in U, and x is not free in V because otherwise x would be free in M, contrary to the fact that Q is an

η-redex. Hence $(\lambda y\ V)\ \alpha\ (\lambda x\ [{}^{x}/_{y}]V)$, giving (D^7) and completing the definition of residuals.

For future use, note that if $(p,\mathcal{U})$ and $(q,\mathcal{U})$ are both β-cells, then the positions of the members of ${}^{P}/_{q}$ are actually independent of $\mathcal{U}$ in all cases except IV(b) $\{$where $s_1,\ldots,s_n$ are involved$\}$.

It can be seen that no cell has more than one residual with respect to an η- or δ'-cell. Hence

$$(D^1_{\eta\delta'}):\quad \mathcal{U}\,\eta\delta'\,\mathcal{X} \text{ and } \mathcal{U}\,\eta\delta'\,\mathcal{Y} \Rightarrow \exists\mathcal{Z}:\ \mathcal{X}\ \underline{\eta\delta'}\ \mathcal{Z} \text{ and } \mathcal{Y}\ \underline{\eta\delta'}\ \mathcal{Z}.$$

Also, for the same reason,

$$\mathcal{U}\,\beta\,\mathcal{X} \text{ and } \mathcal{U}\,\eta\delta'\,\mathcal{Y} \Rightarrow \exists\mathcal{Z}:\ \mathcal{X} \geqslant_{\eta\delta'} \mathcal{Z} \text{ and } \mathcal{Y}\ \underline{\beta}\ \mathcal{Z}.$$

This is (D^2) with β as "r" and $\eta\delta'$ as "s".

Parts (1), (3) and (4) of the plan on page 127 have now been proved, and only (2) remains. To prove (2), ignore all δ'- and η-cells in the definition of residuals. Then the property (B4) that was mentioned at the end of Chapter 2 is satisfied, because in Case III, $[{}^{P}/_{q}]$ is only empty when q or p is an η-cell.

<u>Proof of (A6)</u>

Suppose there are β-cells $(p_1,\mathcal{U}),\ldots,(p_m,\mathcal{U})$, $(q,\mathcal{U})$ such that $p_i \prec q$ for $i = 1\ldots m$, and choose U to be any member of $\mathcal{U}$.

Then β-redexes $P_1,\ldots,P_m,Q$ must occur in U at positions $p_1,\ldots,p_m$ and q respectively. Hence $P_i \subset_{p_i - q} Q$ for i= 1...m, by Corollary 3·4.

Suppose $Q = ((\lambda x\ M)\ N)$: then each $\underline{P}_{p_i}$ is either in $\underline{M}_{q11}$ or in $\underline{N}_{q2}$; that is, each p_i is either $q11t_i$ or $q2t_i$ for some t_i.

If no p_i has the form $q2t_i$, then choose k such that p_k is minimal in $\{p_1,\ldots,p_m\}$; i.e. $i \neq k \Rightarrow p_i \not< p_k$.

Now $qt_i < qt_k \Rightarrow t_i < t_k \Rightarrow q11t_i < q11t_k \Rightarrow p_i < p_k$, so $i \neq k \Rightarrow qt_i \not< qt_k$.

By Case IV of the definition of residuals, each $p_i/_q$ has only one member and its position is qt_i. Hence $p_k/_q$ is minimal in $\{p_1/_q,\ldots,p_m/_q\}$, as required.

If some p_i has the form $q2t_i$, then suppose that

$$\begin{cases} p_i = q2t_i \text{ for } i= 1\ldots h, \text{ for some } h \text{ with } 1 \leqslant h \leqslant m, \\ p_j = q11t_j \text{ for } j= h+1\ldots m, \text{ if } m > h. \end{cases}$$

Choose k such that p_k is minimal in $\{p_1,\ldots,p_h\}$; that is,

$$i \neq k \text{ and } i \leqslant h \Rightarrow p_i \not< p_k.$$

Suppose that $\underline{x}_{os_1},\ldots,\underline{x}_{os_n}$ are the free occurrences of x in M; then for i= 1...h, the positions of the members of $p_i/_q$ are $\{qs_1t_i,\ldots,qs_nt_i\}$ by Case IV(b). Also for j= (h+1)...m, the position of the single member of $p_j/_q$ is qt_j, by Case IV(a).

Now $p_i/_q \not\subset p_k/_q$ if $i \leqslant h$ and $i \neq k$.

> Proof: Otherwise, one of $\{qs_1t_i,\ldots,qs_nt_i\}$ would be an extension of one of $\{qs_1t_k,\ldots,qs_nt_k\}$ (suppose it is an extension of qs_1t_k). Therefore, since $s_1,\ldots,s_n$ are mutually disjoint, it must be qs_1t_i that is the extension of qs_1t_k. Hence t_i is an extension of t_k, and so p_i is an extension of p_k, contrary to the choice of k.

Also $p_j/_q \not\subset p_k/_q$ if $j > h$.

> Proof: Otherwise qt_j would be an extension of one of $\{qs_1t_k,\ldots,qs_nt_k\}$. Suppose it is an extension of qs_1t_k. Hence ot_j is an extension of os_1t_k, and so it is an extension of os_1. Then since $P \subset_{ot_j} M$ and $x \subset_{os_1} M$, P must occur in x, which is impossible.

Hence the cell $(p_k, \mathcal{U})$ satisfies the requirements of (A6).

Now it only remains to prove (D^8) for β-cells; using (B4) and the end of Chapter 2, only the cases mentioned on page 81 need be considered. Then if $(p,\mathcal{U})$, $(q,\mathcal{U})$ and $(r,\mathcal{U})$ are β-cells, $r/_{(p+q/_p)}$ need only be proved identical to $r/_{(q+p/_q)}$ when

$p < q$ and $r < q$ and $r/_q \not\subset p/_q$, and either $p \mid r$ or $p < r$.

{Actually the conclusion of (D^8) is true for β-cells in all cases, as is shown in [5].} Suppose that U is any member of $\mathcal{U}$, in which no variable is both free and bound, and no variable is bound twice. Suppose also that Q = ((λx M) N) is the redex at position q in U, and R and P are the redexes at positions r and p respectively. For convenience, define $\mathcal{X} = \overline{\left\{\frac{\gamma(P)}{P}p\right\}U}$, which is the end of the cell $(p, \mathcal{U})$, and $\mathcal{Y} = \overline{\left\{\frac{\gamma(Q)}{Q}q\right\}U}$, which is the end of the cell $(q, \mathcal{U})$. Let $\underline{x}_{os_1}, \ldots, \underline{x}_{os_n}$ $(0 \leqslant n)$ be the free occurrences of x in M.

The members of ${}^{r}/_{p+q}/_{p}$ are co-initial with the members of ${}^{r}/_{q+p}/_{q}$, because $p+{}^{q}/_{p} \simeq q+{}^{p}/_{q}$. Since two co-initial cells with the same position must be identical, (D^8) will follow if it is shown that the set of positions of the members of ${}^{r}/_{p+q}/_{p}$ is the same as the set of positions of the members of ${}^{r}/_{q+p}/_{q}$.

Proof of (D^8)

Case 1 When $p < q$, $r < q$, ${}^{r}/_{q} \not\leq {}^{p}/_{q}$, and $p \mid r$:

Then $\underline{R}_r$ is either in $\underline{M}_{q11}$ or in $\underline{N}_{q2}$; that is r = q11t or r = q2t, for some t.

Subcase (a): When r = q11t:

$(r, \mathcal{U})/_{(q, \mathcal{U})} = (qt, \mathcal{Y})$ by Case IV(a) of the definition of residuals.

$(r, \mathcal{U})/_{(p, \mathcal{U})} = (r, \mathcal{X})$ by Case II.

$(q, \mathcal{U})/_{(p, \mathcal{U})} = (q, \mathcal{X})$ by Case III.

Therefore ${}^{r}/_{p+q}/_{p} = {}^{(r/p)}/_{(q/p)} = {}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$ by above. By Case IV(a) applied to r, q and $\mathcal{X}$ (since r = q11t), ${}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$ has only one member and its position is qt. Hence ${}^{r}/_{p+q}/_{p}$ has just one member, with position qt.

Now $\underline{P}_p$ is either in $\underline{M}_{q11}$ or in $\underline{N}_{q2}$; that is, either p = q11s or p = q2s, for some s.

When p = q11s:

Then $(p, \mathcal{U})/_{(q, \mathcal{U})} = (qs, \mathcal{Y})$ by Case IV(a).

Therefore ${}^{r}/_{q+p}/_{q} = {}^{(r/q)}/_{(p/q)} = {}^{(qt,\mathcal{Y})}/_{(qs,\mathcal{Y})}$, which is one cell with position qt, by Case II, since qt | qs.

qt | qs because $p \mid r \Rightarrow q11t \mid q11s$
$\Rightarrow t \mid s$
$\Rightarrow qt \mid qs$.

Hence ${}^{r}/_{q+p}/_{q}$ has just one member, with position qt, satisfying (D^8) since qt is the position of the one member of ${}^{r}/_{p+q}/_{p}$.

When p = q2s:

Then $(p, \mathcal{U})/_{(q, \mathcal{U})} = \{(qs_1s, \mathcal{Y}), \ldots, (qs_ns, \mathcal{Y})\}$ by Case IV(b).

Now ${}^{r}/_{q+p}/_{q} = {}^{(r/q)}/_{(p/q)} = {}^{(qt,\mathcal{Y})}/_{(p/q)}$.

For i= 1...n, either $qs_i s \mid qt$ or $qs_i s \prec qt$.

> Proof: $R \subset_{ot} M$ and $x \subset_{os_i} M$, so by Corollary 3·7(3), either $s_i \mid t$ or $s_i \prec t$. Therefore $qs_i s \mid qt$ or $qs_i s \prec qt$.

Hence ${}^{(qt,\mathcal{Y})}/_{(p/q)}$ is one cell with position qt, by Lemma 2·4 on page 79. (Since ${}^{p}/_{q}$ is a development of $\{(qs_1 s,\mathcal{Y}),\ldots,(qs_n s,\mathcal{Y})\}$.)
Therefore ${}^{r}/_{q+p}/_{q}$ is one cell with position qt, as required.

Subcase (b): When r = q2t:

${}^{(r,\mathcal{U})}/_{(q,\mathcal{U})} = \{(qs_1 t,\mathcal{Y}),\ldots,(qs_n t,\mathcal{Y})\}$ by Case IV(b).

${}^{(r,\mathcal{U})}/_{(p,\mathcal{U})} = (r,\mathcal{X})$ by Case II.

${}^{(q,\mathcal{U})}/_{(p,\mathcal{U})} = (q,\mathcal{X})$ By Case III.

Therefore ${}^{r}/_{p+q}/_{p} = {}^{(r/p)}/_{(q/p)} = {}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$.

To evaluate ${}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$:

$p \prec q$, therefore $\mathcal{X} = \overline{\left\{\frac{\gamma(P)}{P}p\right\}U} = \overline{\left\{\frac{\left\{\frac{\gamma(P)}{P}p-q\right\}Q}{Q}q\right\}U}$.

Hence the redex at position q in the member $\left\{\frac{\gamma(P)}{P}p\right\}U$ of $\mathcal{X}$ is $\left\{\frac{\gamma(P)}{P}p-q\right\}Q$.
Suppose it is $((\lambda y\, M^*)\, N^*)$ for some y, M^*, N^*. If the free occurrences of y in M^* can be proved to have positions $os_1,\ldots,os_n$, then by Case IV(b), since r = q2t, ${}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$ will be a set of cells with

positions $qs_1 t,\ldots,qs_n t$.

Now $\underline{P}_p$ is either in $\underline{M}_{q11}$ or in $\underline{N}_{q2}$; that is p = q11s or p = q2s, for some s.

When p = q11s:

Then $\left\{\frac{\gamma(P)}{P}p-q\right\}Q = ((\lambda x\, M^*)\, N)$, where M^* is $\left\{\frac{\gamma(P)}{P}os\right\}M$. In this case the previously-mentioned N^* and y are N and x respectively.

Now $os \mid os_i$ for i= 1...n.

> Proof: If, for some i, not $os \mid os_i$; then by Corollary 3·7(3) $os_i \prec os$, since $x \subset_{os_i} M$ and $P \subset_{os} M$.
> Therefore $qs_i t \prec qs$. But ${}^{(p,\mathcal{U})}/_{(q,\mathcal{U})}$ is one cell with position qs, by Case IV(a), and the positions of the members of ${}^{(r,\mathcal{U})}/_{(q,\mathcal{U})}$ are $qs_1 t,\ldots,qs_n t$ by the previous page, so there is a member of ${}^{r}/_{q}$ whose position is $qs_i t$, which is an extension of the position of the sole member of ${}^{p}/_{q}$. This contradicts the assumption that ${}^{r}/_{q} \not\subset {}^{p}/_{q}$.

Hence by Lemma 3·12, $\underline{x}_{os_1},\ldots,\underline{x}_{os_n}$ are free occurrences of x in M^*.
But x is not free in P.

> Proof: If $\underline{x}_{ou}$ were a free occurrence of x in P, then $\underline{x}_{osu}$ would be an occurrence in M. It could not be one of the free occurrences in M, because not $os \mid osu$. Therefore x would have to be bound in M, and hence bound twice in U, contrary to the choice of U.

Therefore by a result in the proof of Lemma 4·13, x is not free in $\gamma(P)$, and so $\underline{x}_{os_1},\ldots,\underline{x}_{os_n}$ are the only free occurrences of x in M^*. Hence from the bottom of page 151, $(r,\mathcal{X})/(q,\mathcal{X})$ $\left\{\text{which equals } {}^{r}/_{p+q}/_{p}\right\}$ is a set of cells with positions $qs_1t,\ldots,qs_nt$.

$$ {}^{r}/_{q+p}/_{q} = {}^{(r}/_{q})/_{(p}/_{q)} = \left\{(qs_1t,\mathcal{Y}),\ldots,(qs_nt,\mathcal{Y})\right\}/_{(p}/_{q)}. $$

$$ = \left\{(qs_1t,\mathcal{Y}),\ldots,(qs_nt,\mathcal{Y})\right\}/_{(qs,\mathcal{Y})} \text{ by Case IV(a).} $$

For i= 1...n, $qs \mid qs_it$, since $os \mid os_i$. Therefore by Case II, $(qs_it,\mathcal{Y})/_{(qs,\mathcal{Y})}$ is one cell with position qs_it. Hence ${}^{r}/_{q+p}/_{q}$ is a set of cells with positions $qs_1t,\ldots,qs_nt$, which are the same as the positions of the cells in ${}^{r}/_{p+q}/_{p}$.

When p = q2s:

Then $\left\{\frac{\gamma(P)}{P}\right\}Q = ((\lambda x\ M)\ N^*)$, where N^* is $\left\{\frac{\gamma(P)}{P}os\right\}N$. In this case the M^* and y mentioned on p.151 are M and x respectively. Therefore $(r,\mathcal{X})/_{(q,\mathcal{X})}$ $\left\{\text{which equals } {}^{r}/_{p+q}/_{p}\right\}$ is a set of cells with positions $qs_1t,\ldots,qs_nt$, by the bottom of page 151.

As above, ${}^{r}/_{q+p}/_{q} = \left\{(qs_1t,\mathcal{Y}),\ldots,(qs_nt,\mathcal{Y})\right\}/_{(P}/_{q)}$

$(p,\mathcal{U})/_{(q,\mathcal{U})} = \left\{(qs_1s,\mathcal{Y}),\ldots,(qs_ns,\mathcal{Y})\right\}$ by Case IV(b).

Also for i= 1...n, $qs_is \mid qs_jt$ for j= 1...n.

Proof: $p \mid r$ and p = q2s and r = q2t; hence $s \mid t$. So if

j = i, then $qs_is \mid qs_jt$. If $j \neq i$, then $s_j \mid s_i$ because atoms occur at both positions os_j and os_i in M. Hence $qs_jt \mid qs_is$.

So by Lemma 2·4, $(qs_it,\mathcal{Y})/_{(p}/_{q)}$ is one cell with position qs_it, for i= 1...n. Hence ${}^{r}/_{q+p}/_{q}$ is a set of cells with positions $qs_1t,\ldots,qs_nt$, which are the same as the positions of the members of ${}^{r}/_{p+q}/_{p}$.

Case 2 When $p < q$, $r < q$, ${}^{r}/_{q} \not\leq {}^{p}/_{q}$, and $p < r$:

Let os = p-r.

$(q,\mathcal{U})/_{(p,\mathcal{U})} = (q,\mathcal{X})$ by Case III.

$(r,\mathcal{U})/_{(p,\mathcal{U})} = (r,\mathcal{X})$ by Case III.

Now $\underline{R}_r$ may be either in $\underline{M}_{q11}$ or in $\underline{N}_{q2}$; that is r = q11t or r = q2t, for some t.

Subcase (a): When r = q11t:

Then $(r,\mathcal{U})/_{(q,\mathcal{U})} = (qt,\mathcal{Y})$ by Case IV(a). Also p = rs = q11ts, so by Case IV(a) again, $(p,\mathcal{U})/_{(q,\mathcal{U})} = (qts,\mathcal{Y})$.

Therefore ${}^{r}/_{q+p}/_{q} = {}^{(r}/_{q})/_{(p}/_{q)} = (qt,\mathcal{Y})/_{(qts,\mathcal{Y})}$ which is one cell with position qt by Case III, since $qts < qt$.

${}^{r}/_{p+q}/_{p} = {}^{(r}/_{p})/_{(q}/_{p)} = (r,\mathcal{X})/_{(q,\mathcal{X})}$ which is one cell with position qt,

by Case IV(a). Hence ${}^{r}/_{p+q}/_{p} = {}^{r}/_{q+p}/_{q}$.

<u>Subcase (b)</u>: When $r = q2t$:

Then ${}^{(r,\mathcal{U})}/_{(q,\mathcal{U})} = \{(qs_1t,\mathcal{Y}),\ldots,(qs_nt,\mathcal{Y})\}$ by Case IV(b).

$p = rs = q2ts$, so ${}^{(p,\mathcal{U})}/_{(q,\mathcal{U})} = \{(qs_1ts,\mathcal{Y}),\ldots,(qs_nts,\mathcal{Y})\}$, by Case IV(b).

Hence ${}^{r}/_{q+p}/_{q} = {}^{(r/q)}/_{(p/q)} = \{(qs_1t,\mathcal{Y}),\ldots,(qs_nt,\mathcal{Y})\}/_{(p/q)}$.

Now for $i = 1\ldots n$ and $j = 1\ldots n$, either $qs_jts \mid qs_it$ or $qs_jts \prec qs_it$.

> <u>Proof</u>: If $j = i$, then $qs_jts \prec qs_it$. If $j \neq i$, then $s_j \mid s_i$ and so $qs_jts \mid qs_it$.

Therefore by Lemma 2·4, since ${}^{p}/_{q}$ is an MCD of $\{(qs_1ts,\mathcal{Y}),\ldots,(qs_nts,\mathcal{Y})\}$, ${}^{r}/_{q+p}/_{q}$ is a set of cells with positions $qs_1t,\ldots,qs_nt$.

$${}^{r}/_{p+q}/_{p} = {}^{(r/p)}/_{(q/p)} = {}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}.$$

To evaluate this:

$$\mathcal{X} = \overline{\left\{\frac{\mathcal{Y}(P)}{P}p\right\}U} = \overline{\left\{\frac{\left\{\frac{\mathcal{Y}(P)}{P}p{-}q\right\}Q}{Q}q\right\}U} = \overline{\left\{\frac{((\lambda x\ M)\ N^*)}{Q}q\right\}U}, \text{ where } N^* = \left\{\frac{\mathcal{Y}(P)}{P}ots\right\}N.$$

So the redex at position q in $\left\{\frac{\mathcal{Y}(P)}{P}p\right\}U$ must be $((\lambda x\ M)\ N^*)$. The free occurrences of x in $\overline{M}$ are $\underline{x}_{os_1},\ldots,\underline{x}_{os_n}$, and $r = q2t$, so by Case IV(b), ${}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$ is a set of cells whose positions are $qs_1t,\ldots,qs_nt$. Since ${}^{r}/_{p+q}/_{p} = {}^{(r,\mathcal{X})}/_{(q,\mathcal{X})}$ and the members of ${}^{r}/_{q+p}/_{q}$ also

have positions $qs_1t,\ldots,qs_nt$, ${}^{r}/_{p+q}/_{p}$ must be the same as ${}^{r}/_{q+p}/_{q}$, completing the proof of (D^8).

By (5) on page 128, the Church-Rosser property has now been proved for $\beta\eta\delta'$-contraction of classes, and hence for $\alpha\beta\eta\delta'$-contraction of formulae, by page 126.

CHAPTER 5

Some Applications of Theorem 1·1

The Church-Rosser property turns up in several other theories besides λ-conversion; this chapter gives a few such examples. The results are not new, though the proof given here for the first example is an improvement over previous proofs, so only Example 1 will be discussed in detail.

EXAMPLE 1

Here all page-references will be to [12], unless otherwise stated.

In the course of [12], Kleene defines partial recursive functions of natural numbers in two ways, as follows.

Definition 5·1 Inductive definition by "Schemes"

See pages 42 and 45 of [12]. In this definition, letters x, y, z will denote arbitrary natural numbers and "x'" denote the successor of x. "X = Y" will mean that either X+Y both undefined, or X+Y both defined and are equal ~~if X and Y are both defined, then they are equal.~~ ϕ will be a function of natural numbers, and n the number of its

argument-places.}

(I): If $\phi(x) = x'$ for all x, then ϕ is partial recursive.

(II): If, for some natural number c, $\phi(x_1,\ldots,x_n) = c$ for all $x_1,\ldots,x_n$, then ϕ is partial recursive.

(III): If, for some i with $1 \leq i \leq n$, $\phi(x_1,\ldots,x_n) = x_i$ for all $x_1,\ldots,x_n$, then ϕ is partial recursive.

(IV): If θ, $\chi_1,\ldots,\chi_m$ are partial recursive functions and $\phi(x_1,\ldots,x_n) = \theta(\chi_1(x_1,\ldots,x_n), \ldots, \chi_m(x_1,\ldots,x_n))$ for all $x_1,\ldots,x_n$, then ϕ is partial recursive.

(V): If χ is a partial recursive function, and

$$\text{either} \begin{cases} \phi(0) = c \text{ for some natural number } c, \\ \text{and } \phi(y') = \chi(y, \phi(y)) \text{ for all } y \end{cases}$$

$$\text{or} \begin{cases} \text{there is a partial recursive function } \psi \text{ such that} \\ \text{for all } x_2,\ldots,x_n \text{ and } y; \\ \phi(0,x_2,\ldots,x_n) = \psi(x_2,\ldots,x_n) \text{ and} \\ \phi(y',x_2,\ldots,x_n) = \chi(y, \phi(y,x_2,\ldots,x_n), x_2,\ldots,x_n) \end{cases}$$

then ϕ is partial recursive.

(VI): If ρ is a partial recursive function, and for some function σ

$$\begin{cases} \text{for all } x_1,\ldots,x_n, y \text{ and } z; \\ \sigma(0, x_1,\ldots,x_n,y) = y, \\ \sigma(z',x_1,\ldots,x_n,y) = \sigma(\rho(x_1,\ldots,x_n,y'), x_1,\ldots,x_n,y') \text{ and} \\ \phi(x_1,\ldots,x_n) = \sigma(\rho(x_1,\ldots,x_n,0), x_1,\ldots,x_n,0) \end{cases}$$

then ϕ is partial recursive.

{(VI) is the alternative scheme given on page 45 for the "least-number operator", μ, without the restriction that for all $x_1,\ldots,x_n$ there must exist y such that $\rho(x_1,\ldots,x_n,y) = 0$ —— see pages 46 and 51 for comment.}

Definition 5·2 Systems of equations

See pages 43 - 44 and 50 - 51.

Kleene describes a formal system, more or less as follows. Terms are formulae in the sense of Chapter 3:

(i) The atoms consist of an infinite amount of variables, and one "numeral" for each natural number. {In this discussion numerals will not be distinguished from their corresponding numbers.} If n is the numeral corresponding to the number k, then n' is the numeral corresponding to the successor of k.

(ii) If X is a term, then so is X'.

(iii) There are certain things called "function-symbols": if $X_1,\ldots,X_k$ are terms and f is a function-symbol, then $f(X_1,\ldots,X_k)$ is a term.

Positions and replacement can be defined as in Chapter 3, and since there are no bound variables here, substitution can be defined by the conclusion of Lemmas 4·2 and 4·1(2). In the rest of this example, letters m, n, h, i, j, k will denote numerals or natural numbers; x, y, z will

denote variables, and X, Y, Z, U, V, M, N, P, Q will denote terms. ϕ, χ, ψ will denote functions of natural numbers, and f, g, function-letters.

In the formal system there is a symbol "=", with which are associated the following transformation-rules:

(1): From the expression "X = Y", obtain the expression "$\left[{}^{n_1}/_{x_1}\right]\ldots\left[{}^{n_h}/_{x_h}\right]X = \left[{}^{n_1}/_{x_1}\right]\ldots\left[{}^{n_h}/_{x_h}\right]Y$", where $x_1,\ldots,x_h$ are all the variables occurring in X, Y, and $n_1,\ldots,n_h$ are any numerals.

(2): From the expressions "X = Y" and "$f(n_1,\ldots,n_k) = m$", obtain the expression "$X = \left\{\frac{m}{f(n_1,\ldots,n_k)}p\right\}Y$", if Y contains $f(n_1,\ldots,n_k)$ at position p.

A formal equation is any expression of the form "X = Y". If E is a set of formal equations, then "$E \vdash_{1,2} X = Y$" means that the formal equation "X = Y" can be obtained from members of E by a finite number of applications of rules (1) and (2). A finite set, E, of formal equations defines ϕ recursively iff there exists a function-symbol f such that $E \vdash_{1,2} f(i_1,\ldots,i_n) = m$ when and only when $\phi(i_1,\ldots,i_n) = m$.

ϕ is partial recursive iff there is a finite set of formal equations defining ϕ recursively.

The proof that any function ϕ which is partial recursive according to Def. 5·1 must also be partial recursive according to Def. 5·2 proceeds as follows.

If ϕ is partial recursive according to Def. 5·1, then there must be a deduction, using (I),...,(VI), of the fact that ϕ is partial recursive. Each step in this deduction is justified by one, two or three informal equations, and introduces a new function. (In fact, each instance of (VI) introduces two new functions.) The finite set of all equations involved in the deduction is transformed into a set, E, of formal equations by associating a distinct formal variable with each universally-quantified intuitive variable, and associating a distinct function-symbol with each function in the deduction. This is done in such a way that the symbol assigned to each newly-introduced function is distinct from the symbols assigned to the previously-occurring functions.

It can then be shown that E defines ϕ recursively; in other words,

(i): Whenever $\phi(i_1,\ldots,i_n) = m$, then $E \vdash_{1,2} f(i_1,\ldots,i_n) = m$,

(f being the function-symbol associated with ϕ.)

and (ii): Whenever $E \vdash_{1,2} f(i_1,\ldots,i_n) = m$, then $\phi(i_1,\ldots,i_n) = m$.

The proof of (ii) involves showing that

if $E \vdash_{1,2} f(i_1,\ldots,i_n) = m_1$ and $E \vdash_{1,2} f(i_1,\ldots,i_n) = m_2$, then $m_1 = m_2$.

(i.e. E is "consistent")

Kleene remarks on pages 54 - 55 that Def. 5·2 can be modified by replacing rule (2) by a more powerful rule, such as

(3) $\begin{cases} \text{From the expressions "X = Y" and "U = V", obtain} \\ \text{the expression "}X = \left\{\frac{V}{U}p\right\}Y\text{" if } U \subset_p Y, \\ \text{or the expression "}\left\{\frac{V}{U}p\right\}X = Y\text{" if } U \subset_p X. \end{cases}$

The place where this modified definition is actually used is [13] page 731, Def. 2b (to define general recursive functions), and the definition is extended to cover partial functions in [14], page 152.

The modified definition 5·2 is still equivalent to Def. 5·1, by a proof like that on the previous page, but in this case the proof of the consistency of E that Kleene quotes is non-finitary. He suggests that a constructive proof could be given by (I quote) " the type of argument used in the Church-Rosser consistency proof for λ-conversion, and in the Ackermann - von Neumann consistency proof for a certain part of number theory in terms of the Hilbert ε-symbol." This is what will be done here.

By the way, the remark just quoted suggests that the Ackermann - von Neumann result might be deducible from one of the theorems in Chapters 1 and 2; I have not yet followed up this suggestion.

Probably in Hilbert & Bernays "Grundlagen der Math."

Actually the literature contains several strengthened versions of rule (2), of which (3) is the most powerful: obviously the consistency of E with (3) implies the consistency of E with any weaker rule.

Proof of consistency of the previously-defined set E

(using rules 1 and 3)

Further results in J-J Levy 1976 filed as L.794

Define E' to be the union of E and the set of all formal equations of the form "$[^{n_1}/_{y_1}]\cdots[^{n_j}/_{y_j}]X = [^{n_1}/_{y_1}]\cdots[^{n_j}/_{y_j}]Y$", where "X = Y" is any member of E, $n_1,\ldots,n_j$ are any numerals, and $y_1,\ldots,y_j$ are any variables.

Define a relation r thus:

X r Y iff Y is $\{\frac{M}{P}p\}X$, for some member "P = M" of E'.

Finally define "$E \vdash_{1,3} X = Y$" to mean that "X = Y" can be obtained from members of E by rules 1 and 3.

Lemma 5·1

If $E \vdash_{1,3} X = Y$, then $X \sim_r Y$.

Proof:

It is enough to show that "$\sim_r$" has all the defining properties of "$\vdash_{1,3}$".

Basis: If "X = Y" is a member of E, then X r Y and hence $X \sim_r Y$.

Rule (1): To show that "$\sim_r$" satisfies rule (1); that is

$$X \sim_r Y \Rightarrow [^{n_1}/_{x_1}]\cdots[^{n_h}/_{x_h}]X \sim_r [^{n_1}/_{x_1}]\cdots[^{n_h}/_{x_h}]Y,$$

it is enough to show that for all X, Y, n and x,

$$X \text{ r } Y \Rightarrow [^n/_x]X \text{ r } [^n/_x]Y.$$

To prove the latter, suppose that Y is $\{\frac{M}{P}p\}X$, and "P = M" is a member of E'. Then by a result similar to Lemma 4·4(2), $[^n/_x]Y$ is $\left\{\frac{[^n/_x]M}{[^n/_x]P}p\right\}[^n/_x]X$. Since "P = M" is a member of E', so also is "$[^n/_x]P = [^n/_x]M$". Therefore $[^n/_x]X \text{ r } [^n/_x]Y$.

Rule (3): To show that "$\sim_r$" satisfies rule (3), that is

$$X \sim_r Y \text{ and } U \sim_r V \Rightarrow \begin{cases} X \sim_r \{\frac{V}{U}p\}Y & \text{if } U \subset_p Y, \\ \text{and } \{\frac{V}{U}p\}X \sim_r Y & \text{if } U \subset_p X; \end{cases}$$

note that if $U \sim_r V$ and $U \subset_p Y$, then $Y \sim_r \{\frac{V}{U}p\}Y$ by Lemma 3·14. Hence if $X \sim_r Y$, $U \sim_r V$ and $U \subset_p Y$, then $X \sim_r \{\frac{V}{U}p\}Y$ by the transitivity of $\sim_r$. Similarly if $U \subset_p X$, then $Y \sim_r X \sim_r \{\frac{V}{U}p\}X$.

Theorem 5·1

r possesses the Church-Rosser property.

Proof:

By Theorem 1·1, it is enough to prove

(D^1_r): U r X and U r Y $\Rightarrow$ $\exists Z$: X $\underline{r}$ Z and Y $\underline{r}$ Z.

If U r X and U r Y, then X is $\{\frac{M}{P}p\}U$ and Y is $\{\frac{N}{Q}q\}U$, for some

positions p, q and members "P = M" and "Q = N" of E'.

Case I: When $p \mid q$:

Let Z be $\left\{\frac{N}{Q}q\right\}X$, which is the same as $\left\{\frac{M}{P}p\right\}Y$ by Lemma 3·12.

Case II: When $q \prec p$:

Then P must contain Q and be distinct from Q. But from the form of the equations in Def. 5·1, P must be $g(v_1,\ldots,v_k)$, where g is a function-symbol, $v_2,\ldots,v_k$ are atoms and v_1 is either an atom or u' for some atom, u. Therefore Q must occur in one of $v_1,\ldots,v_k$, which is impossible because Q must have a form like that of P. Similarly $p \prec q$ is impossible.

Case III: When p is the same as q:

Then P is the same as Q, and has the form $g(v_1,\ldots,v_k)$ as above. Suppose that P is $\left[{}^{m_1}/_{x_1}\right]\ldots\left[{}^{m_i}/_{x_i}\right]P_o$ and M is $\left[{}^{m_1}/_{x_1}\right]\ldots\left[{}^{m_i}/_{x_i}\right]M_o$ for some member "$P_o = M_o$" of E. (By definition of E')

Also suppose that for some member "$Q_o = N_o$" of E,

$$Q \text{ is } \left[{}^{n_1}/_{y_1}\right]\ldots\left[{}^{n_j}/_{y_j}\right]Q_o \text{ and } N \text{ is } \left[{}^{n_1}/_{y_1}\right]\ldots\left[{}^{n_j}/_{y_j}\right]N_o.$$

Since P is the same as Q; P_o must start with the same function-symbol as Q_o. Hence by the construction of E, the equations "$Q_o = N_o$" and "$P_o = M_o$" must both correspond to the same step in the deduction that ϕ is partial recursive. Hence by inspecting Def. 5·1, "$P_o = M_o$" can only be different from "$Q_o = N_o$" when for some atoms u, $v_2,\ldots,v_k$,

either P_o is $g(0, v_2,\ldots,v_k)$ and Q_o is $g(u', v_2,\ldots,v_k)$

or Q_o is $g(0, v_2,\ldots,v_k)$ and P_o is $g(u', v_2,\ldots,v_k)$.

In the former case, the formula at position oi in P must be 0, and the formula at position oi in Q cannot be an atom, which contradicts the fact that P is the same as Q. The other case is similar. Hence "$P_o = M_o$" is the same equation as "$Q_o = N_o$"; that is, P_o is Q_o and M_o is N_o.

To show that M is the same as N, notice that no variables occur in M_o which do not occur in P_o (by inspecting Def. 5·1). Hence in the expressions for P and M; $x_1,\ldots,x_i$ may be assumed to be all the variables occurring in P_o, and to include all the variables occurring in M_o. Similarly for $y_1,\ldots,y_j$, Q_o and N_o. Then since P_o equals Q_o, i must be the same as j, and for h= 1...i, y_h may be assumed equal to x_h. Since P equals Q; m_h must be the same as n_h for h= 1...i. Hence N is $\left[{}^{m_1}/_{x_1}\right]\ldots\left[{}^{m_i}/_{x_i}\right]N_o$, which is $\left[{}^{m_1}/_{x_1}\right]\ldots\left[{}^{m_i}/_{x_i}\right]M_o$, which is M.

Therefore X is the same as Y; let Z be X, completing the proof.

Now suppose that $E \vdash_{1,3} f(i_1,\ldots,i_n) = m_1$ and that $E \vdash_{1,3} f(i_1,\ldots,i_n) = m_2$. Then by Lemma 5·1, $m_1 \sim_r f(i_1,\ldots,i_n) \sim_r m_2$. Therefore there exists a term Z such that $m_1 \geqslant_r Z$ and $m_2 \geqslant_r Z$, by Theorem 5·1. If Z is not m_1 itself, then m_1 must contain the left-hand

term of a member of E', which is impossible, since m_1 is an atom. Therefore Z is m_1, and similarly Z is m_2. So m_1 is the same as m_2, proving the consistency of E.

The reasoning in this example can be extended to cover definitions of "partial recursive relative to a given set of functions". Also a similar argument can be used to give an alternative proof of Curry and Feys' consistency result for their theory of definition; see Theorem 1, page 67 and Theorem 4, page 123 of [5], and see page 122 of [5] for comment.

EXAMPLE 2

R. Harrop gives a method in [15] for (I quote) "obtaining for any propositional calculus L, which satisfies certain general conditions, associated calculi L' and L* whose decision-problems are equivalent to that of L". He says further that "L' and L* can always be taken as subsystems of positive implicational logic".

He has pointed out to me that an alternative proof of Lemma 6 in his paper might be given using Theorem 1·1. Such a proof is outlined in this example. I think that it can be modified to give Lemma 5 of [16] as well, but this will not be done here.

The formulae of L (here called "L-formulae") are defined with an infinite amount of variables as atoms; the nature of the constructors is irrelevant here. The formulae of L' and L* (here called "L^+-formulae") are defined with the same atoms as the L-formulae, but not necessarily the same constructors. In this example, letters x, y, z denote arbitrary variables, X, Y, Z, U, V denote arbitrary L-formulae, M, N, P, Q denote arbitrary L^+-formulae, and ϕ, ψ, denote arbitrary constructors with h and k argument-places respectively.

For any $n > 0$, and any L-formulae X, $Z_1,\ldots,Z_n$, $x_1,\ldots,x_n$, let "$\left[\frac{Z_1,\ldots,Z_n}{x_1,\ldots,x_n}\right] X$" denote the result of simultaneously substituting

Z_1 for x_1, . . . , Z_n for x_n in X. (This can be defined rigorously by induction on the definition of X, and it is assumed that $x_i = x_j \Rightarrow Z_i = Z_j$.)

"$Y = \mathcal{S}X$" is defined to mean that for some $n > 0$ and some $Z_1,\ldots,Z_n$, $x_1,\ldots,x_n$, $Y = \left[\frac{Z_1,\ldots,Z_n}{x_1,\ldots,x_n}\right]X$. It can be shown that

$$Z = \mathcal{S}Y \text{ and } Y = \mathcal{S}X \Rightarrow Z = \mathcal{S}X, \quad \ldots\ldots\ldots\ldots (I)$$

and that any simultaneous substitution can be carried out by a series of single-variable substitutions (which are defined by putting n = 1 on the previous page).

Similar definitions and results hold for L^+-formulae.

A mapping, T, from L-formulae to L^+-formulae is defined in [15]; its relevant features are

(T1): $T(x) = x$ for all variables, x.

(T2): For each constructor, ϕ;

$$T(\phi(X_1,\ldots,X_h)) = \left[\frac{T(X_1),\ldots,T(X_h)}{z_1,\ldots,z_h}\right]P_\phi$$

for some L^+-formula P_ϕ which is not an atom, and which contains no other variables besides $z_1,\ldots,z_h$.

(T3): $\left[\frac{M_1,\ldots,M_h}{z_1,\ldots,z_h}\right]P_\phi = \left[\frac{N_1,\ldots,N_k}{z_1,\ldots,z_k}\right]P_\psi \Rightarrow \phi = \psi$.

(T3) follows from the second part of Lemma 1(iii) in [15].

The term "$Y_i = \mathcal{S}X_i$ for i= 1...n, by a common substitution" means that for i= 1...n, $Y_i = \mathcal{S}X_i$ and the same formula is substituted for the same variable in each of $X_1,\ldots,X_n$. (Similarly for L^+-formulae.)

With a few changes in notation, Lemma 6 of [15] says: "Suppose $Q_1,\ldots,Q_n$ $(1 \leq n)$ are L^+-formulae such that for i= 1...n, $Q_i = \mathcal{S}T(X_i)$ for some X_i, by a common substitution. Suppose further that for i= 1...n, $Q_i = \mathcal{S}T(X_i')$, not necessarily by a common substitution. Then there exist $Z_1,\ldots,Z_n$ such that for i= 1...n,

(a): $Q_i = \mathcal{S}T(Z_i)$ by a common substitution,

(b): $Z_i = \mathcal{S}X_i$ by a common substitution,

(c): $Z_i = \mathcal{S}X_i'$."

This lemma will be dealt with here only in the case when n = 1; it can fairly easily be extended to its full generality by a device suggested by A. H. Lachlan.

For any L^+-formula Q, define $\mathcal{F}_Q$ to be the set of all L-formulae X for which $Q = \mathcal{S}T(X)$. Then when n = 1, the lemma says:

"If Q is any L^+-formula, and X and X' are members of $\mathcal{F}_Q$, then there exists $Z \in \mathcal{F}_Q$ such that $Z = \mathcal{S}X$ and $Z = \mathcal{S}X'$."

As the first step in proving the lemma, define a relation r as follows:

$$X \; r \; Y \quad \text{iff} \quad \begin{cases} Y = \left[\frac{V}{x}\right]X, \text{ for some } x \text{ occurring in } X, \\ \text{and either } V \text{ is a variable, or } V = \phi(x_1,\ldots,x_h) \\ \text{for some } \phi \text{ and distinct variables } x_1,\ldots,x_h \text{ not} \\ \text{occurring in } X. \end{cases}$$

Then $X \geqslant_r Y \iff Y = \mathcal{S}X$. . . . . (II)

$X \geqslant_r Y \implies Y = \mathcal{S}X$ by (I) and the definition of r.

Since a simultaneous substitution can always be carried out by a series of single-variable substitutions, the converse implication will follow if $Y = \left[\frac{Z}{x}\right]X \implies X \geqslant_r Y$.

This latter statement can be proved by induction on the definition of Z.

Define the relation r' thus:

$$X \; r' Y \quad \text{iff} \quad X \; r \; Y \text{ and } X \in \mathcal{F}_Q \text{ and } Y \in \mathcal{F}_Q.$$

Then r' possesses property (CR), which implies that if X and Y are members of $\mathcal{F}_Q$ and $X \sim_r Y$, there must exist $Z \in \mathcal{F}_Q$ such that $X \geqslant_r Z$ and $Y \geqslant_r Z$.

By Theorem 1·1, $(CR_{r'})$ follows from

$$(D^1_{r'}) \begin{cases} \text{If } U, X \text{ and } Y \text{ are members of } \mathcal{F}_Q, \text{ and } U \; r \; X \text{ and } U \; r \; Y, \\ \text{then there exists } Z \in \mathcal{F}_Q \text{ such that } X \; \underline{r} \; Z \text{ and } Y \; \underline{r} \; Z. \end{cases}$$

$(D^1_{r'})$ is proved by assuming that $X = \left[\frac{V}{x}\right]U$ and $Y = \left[\frac{W}{y}\right]U$,

where V and W have the forms required by the definition of r, and dealing with each possible case in turn.

Now any variable y is a member of $\mathcal{F}_Q$, since $Q = \left[\frac{Q}{y}\right]y = \left[\frac{Q}{y}\right]T(y)$. Also the formula X in the hypothesis of the Lemma is the same as $\left[\frac{X}{y}\right]y$; hence $X = \mathcal{S}y$, and so $y \geqslant_r X$ by (II). Similarly for the formula X' in the lemma, $y \geqslant_r X'$. Therefore $X \sim_r X'$, and so by the result on the previous page, there exists $Z \in \mathcal{F}_Q$ such that $X \geqslant_r Z$ and $X' \geqslant_r Z$. Hence by (II), $Z = \mathcal{S}X$ and $Z = \mathcal{S}X'$, proving the lemma when n = 1, and completing the example.

Other examples

In Axel Thue's paper "Probleme über veränderungen von Zeichenreihen nach gegeben Regeln" (Videnskabs-Selskabet Skrifter (KRISTIANIA) 1914) which is about replacements in finite sequences of symbols, he proves a lemma which can be deduced from Theorem 1·1.

In part of his paper Thue assumes that there is given a list of ordered pairs (A_i, B_i) (for i= 1...n) of finite sequences of symbols, and a rule allowing the replacement of an occurrence of any A_i in a symbol-sequence by the corresponding B_i. Further, if $i \neq j$, then occurrences of A_i and A_j in a symbol-sequence cannot overlap.

The lemma mentioned above says that if the sequences Y and Z can both be obtained from the sequence X by the replacement rule,

and neither Y nor Z contains any A_i, then Y = Z.

To deduce this from Theorem 1·1, the relation r is defined by

$$X \; r \; Y \quad \text{iff} \quad \begin{cases} X \text{ and } Y \text{ are symbol-sequences and } Y \text{ is the result} \\ \text{of replacing, for some } i, \text{ an occurrence of } A_i \text{ in } X \\ \text{by } B_i. \end{cases}$$

(D^1_r) can easily be proved, and (CR_r) follows. The lemma can then be proved by applying (CR_r) to Y and Z.

A less trivial application of Chapters 1 and 2 is the relation of "weak reduction" in combinatory logic. (See [5] and a remark in Def. 6·3 later.) The Church-Rosser property for this relation does not follow from Theorem 1·1, but can be deduced from Theorem 2·1.

The reader has probably noticed that in most of the quoted examples the Church-Rosser property is used to prove some sort of consistency result. To make this more precise, define (for any relation r) the object X to be <u>minimal</u> iff for all Y, $X \geqslant_r Y \implies Y = X$. Then the result which is required in most of the examples is

$$X \geqslant_r A \text{ and } X \geqslant_r B \text{ and } A, B \text{ minimal} \implies A = B.$$

Since this property is weaker than (CR_r), it might be interesting to see if it can be deduced from weakened forms of (A1),...,(A6), (D^7) and (D^8).

For further comment on the Church-Rosser property, see the first few pages of [1].

REFERENCES

[1]: M. H. A. Newman;

"On theories with a combinatorial definition of "Equivalence"";

Annals of Mathematics, Vol. 43 (1942), pp. 223 - 243.

[2]: H. B. Curry;

"A new proof of the Church-Rosser Theorem";

Proc. K. Nederl. Akad. Wetensch. series A, Vol. 55 (1952) pp.16 - 23.

[3]: D. E. Schroer;

Doctoral thesis; not yet published, as far as I know.

[4]: J. B. Rosser;

Review of [2]; Journal of Symbolic Logic Vol. 21(1956), p. 377.

[5]: H. B. Curry and R. Feys;

"Combinatory Logic", volume 1; North-Holland Publ. Co., 1958.

[6]: A. Church;

"The Calculi of Lambda-conversion"; Princeton Univ. Press, 1941.

[7]: A. Church and J. B. Rosser;

"Some properties of conversion";

Trans. American Math. Soc. Vol. 39 (1936), pp. 472 - 482.

[8]: P. Bernays;

Review of [7]; Journal of Symbolic Logic Vol. 1(1936), p. 74.

[9]: S. C. Kleene;

"λ-definable functionals of finite types";

Fundamenta Mathematicae Vol 50 (1961) pp. 281 - 303.

Reviewed by Kreisel in Zentralblatt für Math 100 (1963) P. 250

[10]: J. Ladrière;

"Le Théorème Fondamentale de Gentzen";

Revue Philosophique de Louvain, Vol 49 (1951), pp.357 - 384.

[11]: R. Péter;

"Über die Primitiv-Rekursivität den Aufbau von Formeln charakter--izierenden Wortfunktionen"

Acta Mathematica (Budapest), December 1963.

[12]: S. C. Kleene;

"Recursive predicates and quantifiers";

Trans. American Math. Soc. Vol. 46 (1943), pp. 41 - 72.

[13]: S. C. Kleene;

"General recursive functions of natural numbers";

Mathematische Annalen Vol. 112 (1936), pp. 727 - 742.

[14]: S. C. Kleene;

"On notation for ordinal numbers";

Journal of Symbolic Logic Vol. 3 (1938), pp. 150 - 155.

[15]: R. Harrop;

"A relativization procedure for propositional calculi, with an application to a generalized form of Post's Theorem".

Proc. London Math. Soc. Vol. 14 (1964) (not yet published)

[16]: R. Harrop;

"Some generalizations and applications of a relativization procedure for propositional calculi";

Pp. 10 - 39 of "Formal Systems and Recursive Functions", to be published by North-Holland Co., 1964.

[17]: H. B. Curry;

"Grundlagen der Kombinatorischen Logik";

American Journal of Maths. Vol. 52 (1930), pp. 509 - 536 and 789 - 834.

[18]: H. B. Curry;

"The consistency and completeness of the theory of combinators";

Journal of Symbolic Logic Vol. 6 (1941), pp. 54 - 61.

[19]: H. B. Curry
"On the definition of substitution, replacement & allied notions in an abstract formal system".
Revue Philosophique de Louvain, May 1952, pp. 251-269.

Some properties of relations used in Chapters 1 and 2.

Here r, s are arbitrary relations; U, X, Y are arbitrary objects.

(CR_r): $X \sim_r Y \Rightarrow \exists Z$: $X \geqslant_r Z$ and $Y \geqslant_r Z$.

(B_r): $U \geqslant_r X$ and $U \geqslant_r Y \Rightarrow \exists Z$: $X \geqslant_r Z$ and $Y \geqslant_r Z$.

(G_r): $U\ r\ X$ and $U \geqslant_r Y \Rightarrow \exists Z$: $X \geqslant_r Z$ and $Y \geqslant_r Z$.

(D_r): $U\ r\ X$ and $U\ r\ Y \Rightarrow \exists Z$: $X \geqslant_r Z$ and $Y \geqslant_r Z$.

(D^1_r): $U\ r\ X$ and $U\ r\ Y \Rightarrow \exists Z$: $X\ \underline{r}\ Z$ and $Y\ \underline{r}\ Z$.

(D^2): $U\ r\ X$ and $U\ s\ Y \Rightarrow \exists Z$: $X \geqslant_s Z$ and $Y\ \underline{r}\ Z$.

(D^3): $U\ r\ X$ and $U\ s\ Y \Rightarrow Y \geqslant_r X$ or $X \geqslant_s Y$.

(D^4): $U\ r\ X$ and $U\ s\ Y \Rightarrow \exists V$: $X\ \underline{r}\ V\ \underline{s}\ Y$.

(D^5): $U\ r\ X$ and $U\ s\ Y \Rightarrow \exists V$: $X\ \underline{s}\ V\ \underline{r}\ Y$.

The assumptions used in Theorem 2·1.

Here $x, y, z, y_1, \ldots, y_n$ are any mutually co-initial cells.

(A1): $x \not\subset x$; $x \subset y \Rightarrow y \not\subset x$.

(A2): $x \subset y$ and $y \subset z \Rightarrow x \subset z$.

(A3): If $x \not\subset y$, then ${}^{x}/_{y}$ has at most one member.

(A4): ${}^{x}/_{x} = \emptyset$.

(A5): $y_1 \not\subset x$ and $y_1 \not\subset y_2 \Rightarrow {}^{y_1}/_{x} \not\subset {}^{y_2}/_{x}$.

(A6): $y_i \subset x$ for $i = 1 \ldots n \Rightarrow \exists k$: $y_j \not\subset y_k$ and ${}^{y_j}/_{x} \not\subset {}^{y_k}/_{x}$ (if $j \neq k$).

(D^7): If x and y are co-initial, then $x + {}^{y}\!\surd_{x} \simeq y + {}^{x}\!\surd_{y}$, where ${}^{x}\!\surd_{y}$ and ${}^{y}\!\surd_{x}$ are MCDs of ${}^{x}/_{y}$ and ${}^{y}/_{x}$ respectively.

(D^8): If (D^7) is true, then ${}^{z}/_{x+{}^{y}\surd_{x}} = {}^{z}/_{y+{}^{x}\surd_{y}}$ in the following cases: (i): $z \not\subset x$ and $z \not\subset y$,

(ii): $y \subset x$, $z \subset x$, $z \not\subset y$ and ${}^{z}/_{x} \not\subset {}^{y}/_{x}$.