Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών

Εφαρμογές της Λογικής στην Πληροφορική

(Λάμδα - Λογισμοί)

Γιώργος Κολέτσος
(koletsos@softlab.ntua.gr)

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχ. και Μηχ. Υπολογιστών

Ακαδημαϊκό έτος 2007–2008

Περιεχόμενα

Κεφάλαιο 1

Λάμδα λογισμός

1.1 Προκαταρκτικά

Η έννοια της σύναρτησης.

Είναι κεντρική έννοια στα Μαθηματικά και στην Πληροφορική. Μπορεί να νοηθεί ως ένας «κανόνας» που συνδέει κάθε αντικείμενο *όρισμα* με την *τιμή* της συνάρτησης γι' αυτό το όρισμα. Συνήθως στα Μαθηματικά κάθε συνάρτηση f συνδέεται με ένα (ορισμένο από πριν) σύνολο επιτρεπτών ορισμάτων $\mathbf{A}$, το οποίο αποκαλείται *το πεδίο ορισμού της f*, και με ένα σύνολο $\mathbf{B}$, το οποίο αποτελείται από όλες τις τιμές που μπορεί μια συνάρτηση να πάρει για όλες τις δυνατές τιμές των ορισμάτων της και το οποίο καλείται *το πεδίο τιμών της f*. Γράφουμε τότε f: $\mathbf{A} \to \mathbf{B}$. Συνήθως τα αντικείμενα στο σύνολο $\mathbf{A}$ είναι απλά αντικείμενα (π.χ. αριθμοί), δεν είναι δηλαδή συναρτήσεις. Τίποτα όμως δεν αποκλείει τα αντικείμενα στο $\mathbf{A}$ να είναι και συναρτήσεις. Για παράδειγμα, η έκφραση $\int_0^1 f(x)dx$, όταν το πεδίο των ορισμάτων είναι ολοκληρώσιμες πραγματικές συναρτήσεις που ορίζονται στο [0,1], ορίζει μία συνάρτηση με ορίσματα συναρτήσεις και τιμές πραγματικούς αριθμούς.

Είναι δυνατόν μια συνάρτηση f να «εφαρμόζεται» στον εαυτό της; Είναι δηλαδή δυνατόν ένα από τα δυνατά ορίσματα της f να είναι η ίδια η f; Αν θεωρήσουμε ότι το σύνολο ορισμάτων της f έχει οριστεί *πριν* από τον ορισμό της f, για προφανείς λόγους, αυτό είναι αδύνατο. Μπορούμε όμως να φανταστούμε ότι η συνάρτηση ορίζεται *αρχικά* ως ένας κανόνας (απεικόνισης) και (μόνον) *εκ των υστέρων* προσδιορίζονται, με βάση αυτόν τον κανόνα, τα αντικείμενα στα οποία η συνάρτηση μπορεί να «εφαρμοστεί». Αυτό μπορεί να φαντάζει ως μία απομάκρυνση από την κλασική, καθιερωμένη άποψη για τη συνάρτηση, αλλά στη σύγχρονη, κυρίως πληροφορική, πρακτική είναι σύνηθες π.χ. ένα πρόγραμμα που «καλεί» τον εαυτό του και υπολογίζει μία τιμή ή ένα άλλο πρόγραμμα. Η χαρακτηριστικότερη περίπτωση είναι η *ταυτοτική* συνάρτηση $\mathbb{I}$. Ο κανόνας ορισμού αυτής της συνάρτησης είναι ότι το $(\mathbb{I}\,x)$[1] είναι το x. Οπότε τίποτε δεν αποκλείει την $\mathbb{I}$ να εφαρμοστεί στον εαυτό της, οπότε το $(\mathbb{I}\,\mathbb{I})$ είναι το $\mathbb{I}$.

Ως άλλο παράδειγμα, αν θεωρήσουμε ότι η $\mathbb{H}$ ορίζεται ώστε $(\mathbb{H}\,x)$ να είναι το για κάθε x, τότε το $(\mathbb{H}\,\mathbb{H})$ είναι το .

Στα ως άνω παραδείγματα τα πεδία ορισμού των συναρτήσεων και $\mathbb{H}$ αποτελούνται από όλα τα αντικείμενα.

Έκταση και Ένταση.

Πότε είναι δύο συναρτήσεις ίδιες; Π.χ. είναι οι συναρτήσεις $f(x) = 2 * x$ και $g(x) = x + x$ (όπου x αριθμός) ίδιες;

Η άμεση (συνολοθεωρητική) απάντηση είναι ότι δύο συναρτήσεις f και g είναι ίδιες όταν έχουν το ίδιο πεδίο οριμσού και όταν για κάθε x που ανήκει σ'αυτό το $(f\,x)$ είναι ίδιο με το $(g\,x)$. Αυτή η άποψη είναι η άποψη της ισότητας των συναρτήσεων ως προς την *έκταση*.

[1]Αν f η συνάρτηση και x ένα όρισμά της, γράφουμε ως $(f\,x)$ την τιμή της συνάρτησης γι'αυτό το όρισμα.

Είναι δυνατόν όμως να θεωρήσουμε ότι δύο συναρτήσεις f και g μπορεί να είναι ίδιες ως προς την έκταση άλλα να μην είναι ίδιες όσον αφορά τον τρόπο με τον οποίο υπολογίζουν τις τιμές τους. Κάτω από αυτή τη θεώρηση οι συναρτήσεις νοούνται ως συναρτήσεις ως προς την *ένταση*. Π.χ. οι συναρτήσεις $f(x) = 2 * x$ και $g(x) = x + x$ ενώ είναι ίδιες ως προς την έκταση δεν μπορούν να θεωρηθούν ίδιες ως προς την ένταση, μια και ο τρόπος που υπολογίζονται οι τιμές τους είναι διαφορετικός.

Θα πρέπει στα διάφορα (υπολογιστικά) πλαίσια και με διάφορα κριτήρια να αποφασίζουμε πότε δύο συναρτήσεις είναι ίδιες ως προς την ένταση (ισότητα ως προς την ένταση).

Συναρτήσεις πολλών μεταβλητών.

Η μέχρι τώρα σιωπηρή παραδοχή είναι ότι οι συναρτήσεις μας είναι συναρτήσεις μιας μεταβλητής. Είναι βέβαια επιθυμητό να έχουμε στη διάθεσή μας και την έννοια, για κάθε φυσικό n, της συνάρτησης n μεταβλητών. Αυτό μπορούμε να το κάνουμε χωρίς να αποστούμε από την παραδοχή μας ότι οι συναρτήσεις μας είναι συναρτήσεις μιας μεταβλητής. Η ιδέα οφείλεται στον Schönfinkel [Schönfinkel,1924] αλλά ονομάζεται «currying» από τον H. B. Curry που την εισήγαγε και αυτός ανεξάρτητα. Όταν π.χ. το $n = 2$, δηλαδή όταν θέλουμε η f να είναι συνάρτηση δύο μεταβλητών, τότε μπορούμε να θεωρήσουμε ότι για αντικείμενα x και y η τιμή $f(x, y)$ είναι η $((f\,x)\,y)$, δηλαδή η συνάρτηση δύο μεταβλητών μπορεί να θεωρηθεί ως συνάρτηση μιας μεταβλητής της οποίας οι τιμές είναι συναρτήσεις μίας μεταβλητής. Και αυτό μπορεί να επεκταθεί σε οποιοδήποτε n.

Αφαίρεση.

Είναι αναγκαίο να διαχωρίζουμε μεταξύ ενός συμβόλου ή έκφρασης που δηλώνει μια συνάρτηση και μιας έκφρασης που περιέχει μια μεταβλητή και δηλώνει με αμφίβολο τρόπο κάποια τιμή της συνάρτησης. Αυτή η διάκριση συσκοτίζεται στη συνήθη γλώσσα των μαθηματικών.

Όταν λέμε π.χ. ότι «$x^2 + 1$ είναι μεγαλύτερο από το 1000» διατυπώνουμε κάτι το οποίο δεν έχει νόημα παρά μόνον αν το x πάρει την τιμή ενός συγκεκριμένου αριθμού. Ενώ όταν λέμε ότι «x^2+1 είναι μία πρωτογενής αναδρομική συνάρτηση», διατυπώνουμε κάτι οριστικό, κάτι που δεν εξαρτάται από τον προσδιορισμό του x, δηλαδή εδώ το x επέχει θέση φαινομενικής ή δεσμευμένης μεταβλητής. Η διαφορά λοιπόν είναι ότι την πρώτη περίπτωση η έκφραση $x^2 + 1$ χρησιμοποιείται ως διφορούμενη ή μεταβλητή δήλωση ενός φυσικού αριθμού ενώ στη δεύτερη μιας συγκεκριμένης συνάρτησης. Γι' αυτό στη δεύτερη περίπτωση θα παριστάνουμε τη συνάρτηση που αντιστοιχεί στην έκφραση $x^2 + 1$ ως $(\lambda x.\, x^2 + 1)$ (λ-αφαίρεση).

Το νόημα μίας τέτοιας γραφής (λ-αφαίρεσης) είναι ότι όταν η συνάρτηση $\lambda x.\, x^2+1$ εφαρμοστεί σε ένα συγκεκριμένο όρισμα, έστω 3, τότε η τιμή της συνάρτησης θα παραχθεί από την «μεταβλητή» έκφραση $x^2 + 1$ όπου όμως το x αντικαθίσταται με 3, δηλαδή

$$((\lambda x.\, x^2+1)\,3) \quad = \quad 3^2+1 \quad (= \quad 10)$$

Θα προχωρήσουμε τώρα στον ορισμό του συστήματος του καθαρού (χωρίς τύπους) λ-λογισμού.

Ορισμός 1.1 *Το σύνολο Λ των λ-όρων είναι το σύνολο των εκφράσεων που σχηματίζεται ξεκινώντας από ένα άπειρο σύνολο μεταβλητών $V = \{v, v', v'', \ldots\}$ (αριθμήσιμο σύνολο) με τη χρήση των τελεστών της εφαρμογής και της λ-αφαίρεσης. Ο γενικευμένος ορισμός είναι ο εξής:*

$$\begin{array}{lcl} x \in V & \Rightarrow & x \in \Lambda \\ M, N \in \Lambda & \Rightarrow & (M\,N) \in \Lambda \\ M \in \Lambda, x \in V & \Rightarrow & (\lambda x.\, M) \in \Lambda \end{array}$$

ή χρησιμοποιώντας αφηρημένη σύνταξη μπορούμε να γράψουμε:

$$
\begin{array}{lcl}
V & ::= & v \mid V' \\
\Lambda & ::= & V \mid (\Lambda\,\Lambda) \mid (\lambda V.\,\Lambda)
\end{array}
$$

Κάθε όρος της μορφής $(M\,N)$ *θα λέγεται* εφαρμογή *(του* M *στο* N*)* *ενώ κάθε όρος της μορφής* $(\lambda x.\,M)$ *θα λέγεται* λ-αφαίρεση *(στο* x*).*

Παράδειγμα 1.1 Οι κάτωθι εκφράσεις είναι λ-όροι:

$$
\begin{array}{l}
v \\
(v\,v'') \\
(\lambda v.\,(v\,v'')) \\
((\lambda v.\,(v\,v''))\,v') \\
((\lambda v'.\,((\lambda v.\,(v\,v''))\,v'))v''')
\end{array}
$$

■

Συμβολισμοί:

1. Τα $x, y, z, \ldots$ θα δηλώνουν τυχαίες μεταβλητές (μεταμεταβλητές). Τα $M, N, L, \ldots$ θα δηλώνουν τυχαίους λ-όρους.

2. Γράφουμε $F\,M_1\,M_2\,\ldots\,M_n$ αντί του πλήρους $(\cdots((F\,M_1)\,M_2)\,\ldots\,M_n)$.

   [προσεταιρισμός από αριστερά στις εφαρμογές]

   Γράφουμε $\lambda x_1 x_2 \ldots x_n.\,M$ ή $\lambda x_1 \lambda x_2 \cdots \lambda x_n.M$ αντί του $(\lambda x_1.\,(\lambda x_2.\,(\cdots(\lambda x_n.\,M)\cdots)))$

   [προσεταιρισμός από δεξιά στις λ-αφαιρέσεις]

3. Οι εξωτερικές παρενθέσεις δεν αναγράφονται.

Παράδειγμα 1.2 Οι όροι του παραδείγματος 1.1 γράφονται με βάση τις παραπάνω συνθήκες:

$$v$$
$$v\,v''$$
$$\lambda v.\,v\,v''$$
$$(\lambda v.\,v\,v'')\,v'$$
$$(\lambda v'.\,(\lambda v.\,v\,v'')\,v')v'''$$

■

Παρατήρηση: Ο τρόπος με τον οποίο έχουν οριστεί οι λ-όροι δίνει *μοναδική αναγνωσιμότητα*, δηλαδή κάθε όρος t είναι ένα και μόνον ένα από τα ακόλουθα:

1. μια μεταβλητή ($t = x$ για κάποιο x),
2. μια εφαρμογή, όπου υπάρχουν μοναδικά M και N ώστε $t = (M\,N)$,
3. μια λ-αφαίρεση, όπου υπάρχουν μοναδικά x και N ώστε $t = (\lambda x.\,N)$.

Για τη γραφή των όρων θα προτιμούμε τις απλουστεύσεις που περιγράψαμε παραπάνω αλλά και επιπλέον κάθε γραφή που θα υποδεικνύεται από την απλότητα ή από τη σαφήνεια και η οποία δε θα οδηγεί σε λάθος ανάγνωση του όρου.

Ελεύθερες και δεσμευμένες μεταβλητές.

Όταν σχηματίζεται ο όρος $\lambda x.\,M$ ο τελεστής λx *δεσμεύει* τη μεταβλητή x στον όρο M. Για παράδειγμα, λέμε ότι στον όρο $\lambda x.\,y\,x$ η x είναι *δεσμευμένη* ενώ η y *ελεύθερη* μεταβλητή. Η αντικατάσταση $[x := N]$ εκτελείται μόνο στις ελεύθερες εμφανίσεις της x. Π.χ.

$$y\,x\,(\lambda x.\,x)[x := N] \;\; = \;\; y\,N\,(\lambda x.\,x)$$

Το φαινόμενο των ελεύθερων και δεσμευμένων μεταβλητών εμφανίζεται γενικότερα στα Μαθηματικά, για παράδειγμα στην παράσταση

$$\sum_{x=1}^{3} x + y$$

η x είναι δεσμευμένη μεταβλητή και η y ελεύθερη. Δεν έχει νόημα να αντικαταστήσουμε τη x με κάποιο αριθμό, έχει όμως νόημα να αντικαταστήσουμε την y με π.χ. το 5 αποκτώντας την παράσταση $\sum_{x=1}^{3} x + 5$.

Για λόγους «συντακτικής υγιεινής» θα θεωρούμε ότι οι μεταβλητές που είναι δεσμευμένες σ'έναν όρο θα είναι διαφορετικές από τις ελεύθερες μεταβλητές. Για παράδειγμα, δε θα επιτρέπουμε όρους της μορφής $z\,x\,(\lambda x.\,x)$. Αυτό το επιτυγχάνουμε με τη μετονομασία των δεσμευμένων μεταβλητών, π.χ. ο όρος $\lambda x.\,x$ μπορεί να γίνει $\lambda y.\,y$. Σημειωτέον ότι οι όροι $\lambda x.\,x$ και $\lambda y.\,y$ δρουν κατά τον ίδιο ακριβώς τρόπο, δηλαδή δηλώνουν τον ίδιο αλγόριθμο:

$$(\lambda x.\,x)\,a \quad = \quad a \quad = \quad (\lambda y.\,y)\,a$$

Συμβολισμός: $M \equiv_\alpha N$ ή απλώς $M \equiv N$ σημαίνει ότι οι όροι M και N είτε είναι ίδιοι ή ότι ο ένας μπορεί να αποκτηθεί από τον άλλο με τη μετονομασία των δεσμευμένων μεταβλητών. Για παράδειγμα

$$\begin{array}{rcl}(\lambda x.\,x)\,z & \equiv & (\lambda y.\,y)\,z \\ (\lambda x.\,x)\,z & \equiv & (\lambda x.\,x)\,z \\ (\lambda x.\,x)\,z & \not\equiv & (\lambda x.\,y)\,z\end{array}$$

Ορισμός 1.2 *Ακολουθούν κάποιοι σημαντικοί ορισμοί:*

1. *Το σύνολο των* ελεύθερων μεταβλητών *του λ-όρου M (συμβολίζεται με $\boldsymbol{FV}(M)$) ορίζεται επαγωγικά ως:*

$$\begin{array}{lcl}\boldsymbol{FV}(x) & = & \{\,x\,\} \\ \boldsymbol{FV}(M\,N) & = & \boldsymbol{FV}(M) \cup \boldsymbol{FV}(N) \\ \boldsymbol{FV}(\lambda x.\,M) & = & \boldsymbol{FV}(M) - \{\,x\,\}\end{array}$$

2. *Ο M είναι κλειστός λ-όρος (ή συνδυαστής) αν $\boldsymbol{FV}(M) = \emptyset$. Το σύνολο των κλειστών λ-όρων συμβολίζεται με Λ^0.*

3. *Το αποτέλεσμα της αντικατάστασης (των ελεύθερων εμφανίσεων) του x από το N στον όρο M, συμβολίζεται με $M[x := N]$, ορίζεται ως ακολούθως (θεωρούμε $x \neq y$):*

   - $x[x := N] \equiv N$
   - $y[x := N] \equiv y$
   - $(P\,Q)[x := N] \equiv (P[x := N])(Q[x := N])$
   - $(\lambda y.\, P)[x := N] \equiv \lambda y.\ (P[x := N])$
   - $(\lambda x.\, P)[x := N] \equiv \lambda x.\ P$

<u>Παρατήρηση</u>:Για παράδειγμα στον λ-όρο $y\,(\lambda xy.\, x\,y\,z)$ οι y και z εμφανίζονται ως ελεύθερες μεταβλητές, διότι η πρώτη εμφάνιση της y είναι ελεύθερη καθώς και η μοναδική εμφάνιση της z, ενώ οι x και y ως δεσμευμένες διότι η δεύτερη εμφάνιση της y είναι δεσμευμένη καθώς και η μοναδική εμφάνιση της x. Ο όρος $\lambda xy.\, x\,x\,y$ είναι κλείστος.

Τα ονόματα των κλειστών μεταβλητών σε έναν όρο θα επιλέγονται πάντα ώστε να διαφέρουν από τα ονόματα των ελεύθερων μεταβλητών. Άρα γράφουμε $y\,(\lambda xy'.\, x\,y'\,z)$ για τον $y\,(\lambda xy.\, x\,y\,z)$. Η σύμβαση αυτή μπορεί να επεκταθεί και σε περισσότερους από έναν όρους. Αν π.χ. έχουμε τους όρους $M_1, M_2, \ldots M_n$ μπορούμε να φανταστούμε ότι όλες οι δεσμευμένες μεταβλητές που εμφανίζονται στους όρους αυτούς είναι διαφορετικές από τις ελεύθερες μεταβλητές αυτών των όρων. Αυτό βέβαια μπορεί να επιτευχθεί με μετονομασία των δεσμευμένων (και όχι βέβαια των ελεύθερων) μεταβλητών.

Άρα λοιπόν και στην περίπτωση της αντικατάστασης όταν σχηματίζουμε τον όρο $M[x := N]$ μπορούμε να φανταστούμε ότι αυτή η «σύμβαση των μεταβλητών» ισχύει για τους M και N έτσι ώστε πραγματοποιούμενης της αντικατάστασης καμμία ελεύθερη μεταβλητή του N δε μπορεί να δεσμευτεί (μετά την αντικατάσταση) από κάποιο λ-τελεστή του M. Π.χ. δεν μπορεί να υπάρξει $(\lambda x.\, x\, y)[y := x] = \lambda x.\, x\, x$ διότι αυτό πρέπει να γίνει $(\lambda x.\, x\, y)[y := x] = (\lambda z.\, z\, y)[y := x] = \lambda z.\, z\, x$.

Η «σύμβαση των μεταβλητών» επιτρέπει να ορίζουμε την αντικατάσταση στο λ-λογισμό χωρίς να λαμβάνουμε κάποια ειδική πρόνοια για τις ελεύθερες και δεσμευμένες μεταβλητές.

Και για να μην υπάρχει παρεξήγηση, λ-όροι είναι μόνο οι εκφράσεις (συμβολοσειρές) που σχηματίζονται με βάση τον ορισμό 1.1. Οι ταυτίσεις, μέσω της σχέσης $\equiv$, γίνονται εκ των υστέρων, αφού δημιουργηθούν οι όροι και επίσης η «σύμβαση των μεταβλητών» θα ικανοποιείται μετά την αντικατάσταση κάποιων όρων με ισοδύναμούς τους.

Πρόταση 1.1 (Λήμμα αντικατάστασης – Substitution lemma) *Έστω $M, N, L \in \Lambda$. Υποθέτουμε ότι $x \neq y$ και $x \notin \boldsymbol{FV}(L)$. Τότε*

$$M[x := N][y := L] \quad \equiv \quad M[y := L][x := N[y := L]]$$

Απόδειξη: Με επαγωγή στον όρο M.

Παρατηρήσεις:

1. Ταυτίσαμε τους όρους που διαφέρουν μόνον ως προς τα ονόματα των δεσμευμένων μεταβλητών τους. Μία εναλλακτική και πιο ακριβής μαθηματικά προσέγγιση θα ήταν να ορίζαμε ως προόρους (pre-terms) αυτά που τώρα ορίσαμε ως όρους και μετά να ορίζαμε με συστηματικό και ακριβή τρόπο μία σχέση ισοδυναμίας, την α-ισοδυναμία. Μέσω αυτής της προσέγγισης

θα θεωρούσαμε ως όρους τις κλάσεις ισοδυναμίας (δηλαδή ταύτιση των α-ισοδύναμων προόρων). Προτιμήσαμε να έχουμε τις ταυτίσεις στο συντακτικό επίπεδο. Αυτές οι ταυτίσεις γίνονται στο μυαλό μας και όχι στα χαρτιά.

2. Στο επίπεδο γραφής των όρων θα πρέπει, όταν κάνουμε αντικαταστάσεις, να ικανοποιούμε την (επεκτεταμένη) «σύμβαση μεταβλητών». Π.χ. αν έχουμε τους όρους $\lambda x.\, M$ και N οι οποίοι ο καθένας ξεχωριστά ικανοποιεί τη «σύμβαση μεταβλητών» τότε αν θεωρήσουμε τον $(\lambda x.\, M)\, N$ και θέλουμε να τον αναγάγουμε (με β-αναγωγή [βλ. πιο κάτω]) θα πρέπει να φροντίσουμε ώστε καμμία ελεύθερη μεταβλητή του N δεν είναι δεσμευμένη στον $\lambda x.\, M$. Π.χ. έστω $\omega \equiv \lambda x.\, x\, x$ και $\mathbb{J} \equiv \lambda yz.\, y\, z$. Τότε οι διαδοχικές αναγωγές είναι:

$$\begin{array}{rcl} \omega\, \mathbb{J} & \equiv & (\lambda x.\, x\, x)(\lambda yz.\, y\, z) \\ & =\beta & (\lambda yz.\, y\, z)(\lambda yz.\, y\, z) \\ & =\beta & \lambda z.\, (\lambda yz.\, y\, z)\, z \\ & \equiv & \lambda z.\, (\lambda yz'.\, y\, z')\, z \\ & =\beta & \lambda zz'.\, z\, z' \\ & \equiv & \lambda yz.\, y\, z \\ & \equiv & \mathbb{J} \end{array}$$

Αναγωγή.

Ορίζουμε τη σχέση της αναγωγής στους λ-όρους.

Ορισμός 1.3 *$\rightarrow_\beta$ είναι η μικρότερη διμελής σχέση στο Λ ώστε να ισχύει ότι*

$$(\lambda x.\, P)\, Q \quad \rightarrow_\beta \quad P[x := Q]$$

και η οποία είναι κλειστή για τους ακόλουθους κανόνες:

$$
\begin{array}{lll}
P \to_\beta P' & \Rightarrow \quad \forall x \in V: & \lambda x.\, P \to_\beta \lambda x.\, P' \\
P \to_\beta P' & \Rightarrow \quad \forall Z \in \Lambda: & P\, Z \to_\beta P'\, Z \\
P \to_\beta P' & \Rightarrow \quad \forall Z \in \Lambda: & Z\, P \to_\beta Z\, P'
\end{array}
$$

Ένας όρος της μορφής $(\lambda x.\, P)\, Q$ ονομάζεται *β-redex* και ο $P[x := Q]$ ονομάζεται το *β-contractum* του.

Ένας όρος M είναι μία *β-κανονική μορφή* εάν δεν υπάρχει όρος N ώστε $M \to_\beta N$.

Ορισμός 1.4 *Η έννοια του υποόρου ορίζεται ως εξής:*

1. *οι υποόροι του x είναι το x,*

2. *οι υποόροι του $(M\, N)$ είναι ο $(M\, N)$, οι υποόροι του M και οι υποόροι του N,*

3. *οι υποόροι του $(\lambda x.\, M)$ είναι ο $(\lambda x.\, M)$ καθώς και οι υποόροι του M.*

Πρόταση 1.2 *Ισχύει η ακόλουθη πρόταση:*

$$
M \to_\beta N \Leftrightarrow \begin{array}{l} \textit{Ακριβώς ένας υποόρος του } M \textit{ που είναι contractum} \\ \textit{έχει αντικατασταθεί με το redex του και προέκυψε ο } N. \end{array}
$$

<u>Απόδειξη:</u> Έστω red η σχέση μεταξύ δύο λ-όρων που ορίζεται από το δεύτερο σκέλος της ισοδυναμίας. Είναι φανερό ότι η σχέση red ικανοποιεί τις ιδιότητες της $\to_\beta$. Οπότε ισχύει $\to_\beta \subseteq red$, επειδή $\to_\beta$ είναι η μικρότερη τέτοια σχέση. Έστω τώρα $MredN$. Τότε υπάρχει υποόρος t του M της μορφής redex και t' του N ώστε ο N προέκυψε από τον M με την αντικατάσταση του t με το t', που είναι το contractum του t. Αλλά φανερά έχουμε $t \to_\beta t'$. Και επειδή η δημιουργία του όρου M (μαζί και του N) ακολουθεί τους κανόνες για

τους οποίους είναι κλειστή η $\rightarrow_\beta$, τελικά θα έχουμε και $M \rightarrow_\beta N$[2]. Οπότε $red \subseteq \rightarrow_\beta$, οπότε οι δύο σχέσεις ταυτίζονται.

Πόρισμα 1.1 *Ο όρος M είναι β-κανονική μορφή τότε και μόνον εάν δεν περιέχει (ως υποόρο) κανένα redex.*

Απόδειξη: Διότι αν περιείχε, τότε θα υπήρχε όρος N, σύμφωνα με την πρότασή 1.2, ώστε $M \rightarrow_\beta N$.

Η σχέση $\rightarrow_\beta$ μπορεί να θεωρηθεί για τους λ-όρους ως αναγωγή ενός βήματος, δηλαδή αν $M \rightarrow_\beta N$ τότε γίνεται η αναγωγή ενός redex στον M και προκύπτει ο N. Η διαδοχική εφαρμογή τέτοιων βημάτων ορίζει τη σχέση $\twoheadrightarrow_\beta$.

Ορισμός 1.5 *Η σχέση $\twoheadrightarrow_\beta$ είναι η μεταβατική και αυτοπαθής κλειστότητα της σχέσης $\rightarrow_\beta$. Δηλαδή είναι η μικρότερη διμελής σχέση στο Λ που είναι κλειστή για τους ακόλυθους κανόνες:*

$$\begin{array}{lcl} P \rightarrow_\beta P' & \Rightarrow & P \twoheadrightarrow_\beta P' \\ P \twoheadrightarrow_\beta P' \wedge P' \twoheadrightarrow_\beta P'' & \Rightarrow & P \twoheadrightarrow_\beta P'' \\ P \twoheadrightarrow_\beta P & & \end{array}$$

Πρόταση 1.3 *Ισχύει η ακόλουθη πρόταση:*

$$\begin{array}{ll} M \twoheadrightarrow_\beta N \Leftrightarrow & \textit{Είτε } M \equiv N \textit{ είτε υπάρχουν όροι } M_1, M_2, \ldots M_n \textit{ ώστε} \\ & M \equiv M_1 \textit{ και } N \equiv M_n \textit{ και για κάθε } i\ (1 \leq i \leq n-1), \\ & M_i \rightarrow_\beta M_{i+1}, \textit{ δηλαδή } M \rightarrow_\beta M_2 \rightarrow_\beta \cdots \rightarrow_\beta M_{n-1} \rightarrow_\beta N \end{array}$$

[2] Μπορούμε να αποδείξουμε με επαγωγή στο M ότι αν το N προκύπτει με την αντικατάσταση ενός redex που είναι υποόρος του M με το contractum του τότε $M \rightarrow_\beta N$.

Απόδειξη: Έστω R η σχέση που ορίζεται στο Λ μέσω του δεύτερου σκέλους της ισοδυναμίας. Είναι προφανές ότι R είναι αυτοπαθής, μεταβατική και περιέχει τη σχέση $\rightarrow_\beta$. Οπότε $\twoheadrightarrow_\beta \subseteq R$. Έστω τώρα MRN. Εάν $M \equiv N$ τότε $M \twoheadrightarrow_\beta N$, διότι η $\twoheadrightarrow_\beta$ είναι αυτοπαθής. Διαφορετικά, υπάρχουν $M \rightarrow_\beta M_2 \rightarrow_\beta \cdots \rightarrow_\beta M_{n-1} \rightarrow_\beta N$. Αλλά τότε $M \twoheadrightarrow_\beta M_2 \twoheadrightarrow_\beta \cdots \twoheadrightarrow_\beta M_{n-1} \twoheadrightarrow_\beta N$ και λόγω της μεταβατικότητας της $\twoheadrightarrow_\beta$ παίρνουμε $M \twoheadrightarrow_\beta N$. Οπότε $R \subseteq \twoheadrightarrow_\beta$.

Η αναγωγή ενός όρου είναι ο «υπολογισμός» του. Όταν στον όρο M υπάρχει ένα redex τότε «υπολογίζουμε» το redex αντικαθιστώντας το με το contractum του. Η μετάβαση δηλαδή από τον M στον N ($M \twoheadrightarrow_\beta N$) είναι μία διαδικασία υπολογισμού που μας οδηγεί από τον M στον N. Μπορούμε να θεωρήσουμε ότι οι M και N είναι «ίσοι» μια και έχουν προκύψει και οι δύο από διαδικασία εκτέλεσης υπολογισμών με την ίδια αφετηρία. Αυτή η έννοια γενικεύεται και στην περίπτωση της αναγωγής $\twoheadrightarrow_\beta$ δίνει τη β-ισότητα.

Ορισμός 1.6 *Η σχέση $=_\beta$ (β-ισότητα) είναι η μεταβατική, αυτοπαθής, συμμετρική κλειστότητα της σχέσης $\rightarrow_\beta$, δηλαδή η $=_\beta$ είναι η μικρότερη σχέση που είναι κλειστή για τους ακόλουθους κανόνες:*

$$
\begin{array}{lcl}
P \rightarrow_\beta P' & \Rightarrow & P =_\beta P' \\
P =_\beta P' \wedge P' =_\beta P'' & \Rightarrow & P =_\beta P'' \\
P =_\beta P & & \\
P =_\beta P' & \Rightarrow & P' =_\beta P
\end{array}
$$

Πρόταση 1.4 *Ισχύει η πρόταση:*

$$
\begin{array}{ll}
M =_\beta N \Leftrightarrow & \text{Υπάρχουν } M_1, M_2, \ldots M_n \text{ με } M \equiv M_1 \text{ και } N \equiv M_n \\
& \text{και για κάθε } i \ (1 \leq i \leq n-1) \text{ έχουν } M_i \twoheadrightarrow_\beta M_{i+1} \\
& \text{ή } M_{i+1} \twoheadrightarrow_\beta M_i
\end{array}
$$

Απόδειξη: Όπως και στις προηγούμενες περιπτώσεις.

Παράδειγμα 1.3 Ισχύουν τα παρακάτω:

$$\begin{array}{lcl}
(\lambda x.\, x\, x)\, \lambda z.\, z & \to_\beta & x\, x[x := \lambda z.\, z] \quad = \quad (\lambda z.\, z)\lambda y.\, y \\
(\lambda z.\, z)\, \lambda y.\, y & \to_\beta & z[z := \lambda y.\, y] \quad = \quad \lambda y.\, y \\
(\lambda x.\, x\, x)\, \lambda z.\, z & \twoheadrightarrow_\beta & \lambda y.\, y \\
(\lambda x.\, x)\, y\, z & =_\beta & y\, ((\lambda x.\, x)\, z) \\
& \text{διότι} & \overbrace{(\lambda x.\, x)\, y}^{\text{redex}}\ z \quad \to_\beta \quad y\, z \\
& \text{και} & y\ \underbrace{((\lambda x.\, x)\, z)}_{\text{redex}} \quad \to_\beta \quad y\, z
\end{array}$$

■

Κάποια επιπρόσθετα σχόλια.

Η απλή διαισθητική ερμηνεία των λ-όρων είναι ότι εκφράζουν συναρτήσεις και εφαρμογές συναρτήσεων σε μία καθαρή μορφή. Για παράδειγμα, ο λ-όρος

$$\mathbb{I} \;=\; \lambda x.\, x$$

εκφράζει την ταυτοτική συνάρτηση που περιγράφτηκε στην εισαγωγή (προκαταρκτικά). Βέβαια, ως όρος είναι μία τυπική έκφραση που γράφεται με τη χρήση συμβόλων ενός δεδομένου αλφαβήτου, τα σύμβολα λ, x, κ.λπ. Η διαφορά μεταξύ ενός όρου και της συνάρτησης που εκφράζει είναι ανάλογη αυτής που υπάρχει μεταξύ ενός προγράμματος που γράφεται σε μία γλώσσα και της συνάρτησης (δηλ. ένα σύνολο ζευγών) που υπολογίζει. Η συνάρτηση $\mathbb{H}$ που για κάθε αντικείμενο - όρισμα επιστρέφει την ταυτοτική συνάρτηση μπορεί να θεωρηθεί ότι εκφράζεται από τον όρο $K^* = \lambda y.\, \lambda x.\, x$ επειδή ακριβώς $K^*M =_\beta \lambda x.x \equiv \mathbb{I}$ Αυτό το φαινόμενο είναι βέβαια γνωστό από τον προγραμματισμό όπου μια συνάρτηση μπορεί να επιστρέφει ως αποτέλεσμα μια συνάρτηση.

Ο όρος $K = \lambda y.\, \lambda x.\, y$ δηλώνει τη συνάρτηση που σε κάθε όρισμα επιστρέφει τη συνάρτηση η οποία σε κάθε όρισμα επιστρέφει το προηγούμενο όρισμα, δηλαδή αν M είναι το όρισμα τότε $K\,M \to_\beta \lambda x.\,M$ και αν N ένα οποιοδήποτε όρισμα τότε $K\,M\,N \to_\beta (\lambda x.\,M)$ N $\to_\beta$ M.

Επίσης, μπορεί να θεωρηθεί ως μία συνάρτηση «2 μεταβλητών» (currying) όπου σε κάθε ζεύγος ορισμάτων επιστρέφεται το πρώτο όρισμα.

Η διαδικασία υπολογισμού τυποποιείται με τη β-αναγωγή. Δηλαδή, το redex που υπάρχει σε ένα όρο «υπολογίζεται» όταν το αντικαταστήσουμε με το contractum. Η σχέση $\twoheadrightarrow_\beta$ τυποποιεί τη διαδικασία ενός συνολικότερου υπολογισμού.

Επίσης, η σχέση $=_\beta$ «ταυτίζει» δύο όρους που διαισθητικά μπορούν να θεωρηθούν υπολογιστικά ισοδύναμοι, δηλαδή ισοδύναμοι ως προς την ένταση.

Ένας όρος μπορεί να ανάγεται και στον εαυτό του π.χ. αν $\omega = \lambda x.\,x\,x$. Τότε $\Omega = \omega\,\omega$ και έχουμε $\Omega = \omega\,\omega = (\lambda x.\,x\,x)\,\lambda x.\,x\,x \to_\beta \omega\,\omega = \Omega$. Οπότε

$$\Omega \to_\beta \Omega \to_\beta \Omega \to_\beta \Omega \to_\beta \ldots$$

Το Ω είναι ένα παράδειγμα όρου, όπου ένας υπολογισμός που έχει αφετηρία αυτόν τον όρο δεν τερματίζει ποτέ.

1.2 Το θεώρημα Church–Rosser

Κάθε όρος M μπορεί να περιέχει αρκετά (περισσότερα του ενός) από β-redex, π.χ. ο όρος

$$\mathbb{K}\,(\mathbb{I}\,\mathbb{I}) = \overbrace{\lambda y.\,\lambda x.\,y\,(\underbrace{(\lambda z.\,z)\,\lambda w.\,w}_{\text{redex}})}^{\text{redex}}$$

Μπορούμε να έχουμε $\mathbb{K}\,(\mathbb{I}\,\mathbb{I}) \to_\beta \lambda x.\,(\mathbb{I}\,\mathbb{I})$, αλλά και $\mathbb{K}\,(\mathbb{I}\,\mathbb{I}) \to_\beta \mathbb{I}$.

Οπότε με αφετηρία έναν όρο M μπορούμε να έχουμε διαφορετικά «μονοπάτια υπολογισμού» $M \twoheadrightarrow_\beta M_1$ και $M \twoheadrightarrow_\beta M_2$. Πώς σχετίζονται οι όροι M_1 και M_2; Το θεώρημα Church–Rosser λέει πως σ'αυτή την περίπτωση υπάρχει πάντοτε ένας (κοινός) όρος M_3, στον οποίο οι M_1 και M_2 μπορούν να συγκλίνουν, δηλαδή $M_1 \twoheadrightarrow_\beta M_3$ και $M_2 \twoheadrightarrow_\beta M_3$.

Θεώρημα 1.1 (Church–Rosser) *Εάν $M \twoheadrightarrow_\beta M_1$ και $M \twoheadrightarrow_\beta M_2$, τότε υπάρχει M_3 ώστε $M_1 \twoheadrightarrow_\beta M_3$ και $M_2 \twoheadrightarrow_\beta M_3$.*

Ορισμός 1.7 *Έστω $M \twoheadrightarrow_\beta N$ και N είναι β-κανονική μορφή. Τότε ο όρος N λέγεται β-κανονική μορφή του M.*

Πόρισμα 1.2 *Κάθε όρος μπορεί να έχει (αν έχει) μόνον μία κανονική μορφή.*

Απόδειξη: Αν M_1 και M_2 δύο κανονικές μορφές του M, τότε από το θεώρημα 1.1 θα υπήρχε όρος M_3 ώστε $M_1 \twoheadrightarrow_\beta M_3$ και $M_2 \twoheadrightarrow_\beta M_3$. Αλλά επειδή M_1 κανονική μορφή τότε $M_1 \equiv M_3$ και ομοίως $M_2 \equiv M_3$. Οπότε $M_1 \equiv M_2$.

Παρατήρηση: Δεν έχουν όλοι οι όροι κανονικές μορφές, π.χ. ο όρος Ω. Αν όμως υπάρχει, τότε θα είναι μοναδική. Αν φανταστούμε μία διαδικασία υπολογισμού (αναγωγή) της κανονικής μορφής τότε το θεώρημα Church–Rosser εξασφαλίζει ότι η κανονική μορφή που υπολογίζεται είναι ανεξάρτητη από τον τρόπο υπολογισμού. Το φαινόμενο είναι ανάλογο με τον υπολογισμό αριθμητικών-αλγεβρικών εκφράσεων στα μαθηματικά. Π.χ. όταν υπολογίζουμε την έκφραση $(5+3)*(4+7)*(11+3)$ το αποτέλεσμα θα είναι ανεξάρτητο από τη σειρά και από τον τρόπο που θα επιλέξουμε να την υπολογίσουμε.

Το θεώρημα Church–Rosser μας δίνει την δυνατότητα ενός χαρακτηρισμού της β-ισότητας.

Πόρισμα 1.3 *Ισχύει το παρακάτω:*

$$M =_\beta N \quad \Leftrightarrow \quad \textit{Υπάρχει όρος } L \textit{ ώστε } M \twoheadrightarrow_\beta L \textit{ και } N \twoheadrightarrow_\beta L.$$

Απόδειξη:
($\Leftarrow$) Προφανές από πρόταση 1.4.
($\Rightarrow$) Έστω R διμελής σχέση στο Λ που ορίζεται από το δεξιό σκέλος της πρότασης, δηλαδή $M\ R\ N$ ανν υπάρχει L ώστε $M \twoheadrightarrow_\beta L$ και $N \twoheadrightarrow_\beta L$. Η σχέση R είναι προφανώς αυτοπαθής και συμμετρική. Επίσης, περιέχει τη σχέση $\rightarrow_\beta$, διότι αν $M \rightarrow_\beta N$ τότε υπάρχει $L(L \equiv N)$ ώστε $M \twoheadrightarrow_\beta L$ και $N \twoheadrightarrow_\beta L$. Η σχέση R είναι και μεταβατική, διότι έστω $M\ R\ N$ και $N\ R\ N'$. Τότε $M \twoheadrightarrow_\beta L$ και $N \twoheadrightarrow_\beta L$, για κάποιο L, και $N \twoheadrightarrow_\beta L'$ και $N' \twoheadrightarrow_\beta L'$, για κάποιο L'. Από το Church–Rosser, υπάρχει L'' ώστε $L \twoheadrightarrow_\beta L''$ και $L' \twoheadrightarrow_\beta L''$. Οπότε και τελικά (επειδή $\twoheadrightarrow_\beta$ μεταβατική) $M \twoheadrightarrow_\beta L''$ και $N' \twoheadrightarrow_\beta L''$, δηλαδή $M\ R\ N'$. Συμπεραίνουμε ότι R είναι αυτοπαθής, συμμετρική, μεταβατική και περιέχει τη β, άρα περιέχει και την $=_\beta$ ως μικρότερη τέτοια σχέση.

Πόρισμα 1.4 *N είναι η (μοναδική) β-κανονική μορφή του $M \Leftrightarrow N$ είναι κανονική μορφή και $M =_\beta N$.*

Πόρισμα 1.5 *Αν $M \twoheadrightarrow_\beta N$, $M \twoheadrightarrow_\beta L$ και N, L κανονικές μορφές, τότε $N \equiv L$.*

Πόρισμα 1.6 *Ο λ-λογισμός ως θεωρία της β-ισότητας είναι συνεπής θεωρία, δηλαδή υπάρχει ένα ζεύγος M και N λ-όρων που δεν είναι β-ισοδύναμοι [3].*

Απόδειξη: $\lambda x.\, x \neq_\beta \lambda x.\, \lambda y.\, x$

[3] Το εντελώς ανάλογο ισχύει και στη λογική. Αν ορίσουμε τη συνέπεια ως αδυναμία να αποδείξουμε στην τυπική θεωρία μία αντίφαση της μορφής $p \wedge \neg p$, τότε ο ορισμός αυτός είναι ισοδύναμος με την ιδιότητα να υπάρχει τουλάχιστον μία πρόταση που να μην αποδεικνύεται σ'αυτό το σύστημα.

1.3 Εκφρασιμότητα και Αναποκρισιμότητα

Στο λ-λογισμό μπορούμε να ορίσουμε τα στοιχεία (αριθμούς, συναρτήσεις) που αφορούν στους συνήθεις υπολογισμούς. Με αυτή την έννοια ο λ-λογισμός μπορεί να νοηθεί ως μία εναλλακτική τυποποίηση της θεωρίας αναδρομής.

Ορισμός 1.8 *Αν $F, A \in \Lambda$ για κάθε $n \in \mathbb{N}$ ορίζουμε το $F^n(M) \in \Lambda$ ως ακολούθως:*

$$\begin{array}{lcl} F^0(M) & = & M \\ F^{n+1}(M) & = & F\,(F^n(M)) \end{array}$$

Π.χ. $F^3(M) = F\,(F\,(F\,M))$. Το $F^n(M)$ μπορεί να θεωρηθεί ως n φορές διαδοχικές εφαρμογές της συνάρτησης F στο όρισμα M.

Ορισμός 1.9 (Νούμερα του Church) *Για $n \in \mathbb{N}$, τα νούμερα του Church $\boldsymbol{c}_0, \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots$ ορίζονται ως:*

$$\boldsymbol{c}_n \equiv \lambda f x.\, f^n(x)$$

Τα νούμερα του Church $\boldsymbol{c}_n$ είναι οι αναπαραστάσεις των αριθμών $n \in \mathbb{N}$ στον λ-λογισμό. Τα $\boldsymbol{c}_n$ είναι όλα σε κανονική μορφή.

Παράδειγμα 1.4 Ακολουθούν μερικά νούμερα του Church:

$$\begin{array}{lcl} \boldsymbol{c}_0 & \equiv & \lambda f.\, \lambda x.\, x \\ \boldsymbol{c}_1 & \equiv & \lambda f.\, \lambda x.\, f\,x \\ \boldsymbol{c}_2 & \equiv & \lambda f.\, \lambda x.\, f\,(f\,x) \end{array}$$

■

Μπορούμε να ορίσουμε αναπαραστάσεις των συνήθων αριθμητικών συναρτήσεων; Η ακόλουθη πρόταση μας λέει πώς ναι.

Πρόταση 1.5 *Υπάρχουν όροι $\boldsymbol{A}_+, \boldsymbol{A}_*, \boldsymbol{A}_{\exp}$ για τους οποίους ισχύει:*

1. $\boldsymbol{A}_+ \, \boldsymbol{c}_n \, \boldsymbol{c}_m =_\beta \boldsymbol{c}_{n+m}$ ($\boldsymbol{A}_+$ *αναπαριστά την πρόσθεση*)
2. $\boldsymbol{A}_* \, \boldsymbol{c}_n \, \boldsymbol{c}_m =_\beta \boldsymbol{c}_{nm}$ ($\boldsymbol{A}_*$ *αναπαριστά τον πολλαπλασιασμό*)
3. *Αν* $m > 0$ *τότε* $\boldsymbol{A}_{\exp} \, \boldsymbol{c}_n \, \boldsymbol{c}_m =_\beta \boldsymbol{c}_{(n^m)}$ ($\boldsymbol{A}_{\exp}$ *αναπαριστά την ύψωση σε δύναμη*)

Απόδειξη (Rosser): Ορίζουμε τους όρους ως εξής:

1. $\boldsymbol{A}_+ \equiv \lambda xypq.\, x\, p\, (y\, p\, q)$
2. $\boldsymbol{A}_* \equiv \lambda xyz.\, x\, (y\, z)$
3. $\boldsymbol{A}_{\exp} \equiv \lambda xy.\, y\, x$

Έχουμε λοιπόν:

1. Για το $\boldsymbol{A}_+$:

$$
\begin{aligned}
\boldsymbol{A}_+\, \boldsymbol{c}_n\, \boldsymbol{c}_m &=_\beta \lambda p.\, \lambda q.\, \boldsymbol{c}_n\, p\, (\boldsymbol{c}_m\, p\, q) \\
&=_\beta \lambda p.\, \lambda q.\, (\lambda x.\, p^n(x))\, p^m(q) \\
&=_\beta \lambda p.\, \lambda q.\, p^n\, (p^m(q)) \\
&=_\beta \lambda p.\, \lambda q.\, p^{n+m}(q) \\
&\equiv \boldsymbol{c}_{n+m}
\end{aligned}
$$

2. Για το $\boldsymbol{A}_*$:

$$
\begin{aligned}
\boldsymbol{A}_*\, \boldsymbol{c}_n\, \boldsymbol{c}_m &=_\beta \lambda z.\, \boldsymbol{c}_n\, (\lambda w.\, z^m(w)) \\
&=_\beta \lambda z.\, (\lambda f.\, \lambda x.\, (\underbrace{f\, (f\, (\cdots\, (f}_{n \text{ φορές}}\, x) \cdots))))\, (\lambda w.\, z^m(w)) \\
&=_\beta \lambda z.\, \lambda x.\, (\underbrace{(\lambda w.\, z^m(w))\, ((\lambda w.\, z^m(w))\, (\cdots\, ((\lambda w.\, z^m(w))}_{n \text{ φορές}}\, x) \cdots))) \\
&=_\beta \lambda z.\, \lambda x.\, (\underbrace{(\lambda w.\, z^m(w))\, ((\lambda w.\, z^m(w))\, (\cdots\, ((\lambda w.\, z^m(w))}_{n-1 \text{ φορές}}\, z^m(x)) \cdots))) \\
&=_\beta \lambda z.\, \lambda x.\, (\underbrace{(\lambda w.\, z^m(w))\, ((\lambda w.\, z^m(w))\, (\cdots\, ((\lambda w.\, z^m(w))}_{n-2 \text{ φορές}}\, z^{m+m}(x)) \cdots \\
&=_\beta \lambda z.\, \lambda x.\; z^{\overbrace{m + \cdots + m}^{n \text{ φορές}}}(x) \\
&=_\beta \lambda z.\, \lambda x.\; z^{nm}(x) \\
&\equiv \boldsymbol{c}_{nm}
\end{aligned}
$$

3. Για το $\boldsymbol{A}_{\mathrm{exp}}$, με $m \geq 1$:

$$
\begin{array}{rcl}
\boldsymbol{A}_{\exp}\, \boldsymbol{c}_n\, \boldsymbol{c}_m & =_\beta & \boldsymbol{c}_m\, \boldsymbol{c}_n \\
& \equiv & (\lambda z.\, \lambda f.\, z^m(f))\, (\lambda z.\, \lambda w.\, z^n(w)) \\
& =_\beta & \lambda f.\, \underbrace{(\lambda z.\, \lambda w.\, z^n(w)) \cdots (\lambda z.\, \lambda w.\, z^n(w))}_{m \text{ φορές}}\, f \\
& =_\beta & \lambda f.\, \underbrace{(\lambda z.\, \lambda w.\, z^n(w)) \cdots (\lambda z.\, \lambda w.\, z^n(w))}_{m-1 \text{ φορές}}\, \lambda w.\, f^n(w) \\
& =_\beta & \lambda f.\, \underbrace{(\lambda z.\, \lambda w.\, z^n(w)) \cdots (\lambda z.\, \lambda w.\, z^n(w))}_{m-2 \text{ φορές}}\, \lambda w.\, f^{nn}(w) \\
& =_\beta & \lambda f.\, \lambda w.\, f^{\overbrace{n \cdots n}^{m \text{ φορές}}}(w) \\
& \equiv & \boldsymbol{c}_{(n^m)}
\end{array}
$$

<u>Παρατήρηση:</u> Η ισότητα $=_\beta$ δηλώνει μάλλον την ισότητα των συναρτήσεων ως προς την ένταση. Βέβαια, αν $M =_\beta N$, τότε οι M και N δηλώνουν ως προς την έκταση την ίδια συνάρτηση, γιατί τότε $M\, Z =_\beta N\, Z$, για κάθε Z. Θεωρείστε τώρα τους όρους $A_s \equiv \lambda x.\, \lambda s.\, \lambda z.\, s\, (x\, s\, z)$ και $A'_s \equiv \lambda x.\, \lambda s.\, \lambda z.\, x\, s\, (s\, z)$. Ισχύει ότι

$$
\begin{array}{rcl}
A_s\, \boldsymbol{c}_n & =_\beta & \boldsymbol{c}_{n+1} \\
A'_s\, \boldsymbol{c}_n & =_\beta & \boldsymbol{c}_{n+1}
\end{array}
$$

Δηλαδή και οι δύο όροι αναπαριστούν στον λ-λογισμό τη συνάρτηση S του επόμενου ($S(n) = n + 1$). Αλλά

$$A_s \;\neq_\beta\; A'_s$$

Στη συνέχεια, θα δούμε ότι μπορούμε να αναπτύξουμε στον λ-λογισμό όλες τις προγραμματιστικές τεχνικές, δηλαδή να ορίσουμε τις αληθοτιμές bool, το **if**. . .**then**. . .**else**, τα ζεύγη κ.λπ.

Ορισμός 1.10
$$
\begin{array}{rcl}
\textbf{true} & \equiv & \lambda x.\, \lambda y.\, x \\
\textbf{false} & \equiv & \lambda x.\, \lambda y.\, y
\end{array}
$$

Ορισμός 1.11 *Ορίζουμε (B, P, Q όροι)*

$$\textbf{if } B \textbf{ then } P \textbf{ else } Q \quad \equiv \quad B\,P\,Q$$

Τότε βέβαια έχουμε ότι

$$\begin{aligned} \textbf{if true then } P \textbf{ else } Q &=_\beta P \\ \textbf{if false then } P \textbf{ else } Q &=_\beta Q \end{aligned}$$

Δηλαδή στον όρο «**if** B **then** P **else** Q» εάν το B υπολογιστεί να είναι **true** «επιστρέφεται» το P, αν το B υπολογιστεί να είναι **false** «επιστρέφεται» το Q.

Ορισμός 1.12 *Ορίζουμε*

$$\begin{aligned} [P, Q] &\equiv \lambda x.\, x\,P\,Q \\ \pi_1 &\equiv \lambda x.\, \lambda y.\, x \equiv \textbf{true} \ (\textit{πρώτη προβολή}) \\ \pi_2 &\equiv \lambda x.\, \lambda y.\, y \equiv \textbf{false} \ (\textit{δεύτερη προβολή}) \end{aligned}$$

Τότε έχουμε ότι

$$\begin{aligned} [P, Q]\,\pi_1 &=_\beta P \\ [P, Q]\,\pi_2 &=_\beta Q \end{aligned}$$

Όντως,

$$\begin{aligned} [P, Q]\,\pi_1 &\equiv (\lambda x.\, x\,P\,Q)\,(\lambda x.\, \lambda y.\, x) \\ &=_\beta (\lambda x.\, \lambda y.\, x)\,P\,Q \\ &=_\beta (\lambda y.\, P)\,Q \\ &=_\beta P \end{aligned}$$

Ομοίως για τη δεύτερη προβολή.

Ορισμός 1.13 *Ορίζουμε*

(i) *Αριθμητική συνάρτηση είναι μια συνάρτηση* $f : \mathbb{N}^m \to \mathbb{N}$

(ii) *Μία αριθμητική συνάρτηση* $f : \mathbb{N}^m \to \mathbb{N}$ *(*m *μεταβλητών) είναι* λ-ορίσιμη *ή* λ-αναπαραστάσιμη *εάν υπάρχει όρος* $F \in \Lambda$ *έτσι ώστε*

$$F\ \boldsymbol{c}_{n_1}\ \boldsymbol{c}_{n_2} \cdots \boldsymbol{c}_{n_1} =_\beta \boldsymbol{c}_{f(n_1,n_2,\ldots n_m)}$$

για όλα τα $n_1, n_2, \ldots n_m \in \mathbb{N}$. Λέμε τότε ότι ο F ορίζει ή αναπαριστά (στο λ-λογισμό) την συνάρτηση f

Παρατήρηση: Εάν $F\ \boldsymbol{c}_{n_1}\ \boldsymbol{c}_{n_2} \cdots \boldsymbol{c}_{n_1} =_\beta \boldsymbol{c}_{f(n_1,n_2,\ldots n_m)}$ και επειδή $\boldsymbol{c}_{f(n_1,n_2,\ldots n_m)}$ είναι σε κανονική μορφή, από το θεώρημα Church–Rosser θα έχουμε ότι $F\ \boldsymbol{c}_{n_1}\ \boldsymbol{c}_{n_2} \cdots \boldsymbol{c}_{n_1} \twoheadrightarrow_\beta \boldsymbol{c}_{f(n_1,n_2,\ldots n_m)}$.

Στη συνέχεια θα ορίσουμε την κλάση των αναδρομικών συναρτήσεων.

Ορισμός 1.14 *Η κλάση των αναδρομικών συναρτήσεων είναι η μικρότερη κλάση των αριθμητικών συναρτήσεων που περιλαμβάνει τις αρχικές συναρτήσεις:*

(i) *προβολές: $U_i^m(n_1, \ldots n_m) = n_i$, για όλα τα i με $1 \leq i \leq m$*

(ii) *επόμενος: $S^+(n) = n + 1$*

(iii) *μηδενική: $Z(n) = 0$*

και είναι κλειστή για τη σύνθεση, την πρωτογενή αναδρομή και την ελαχιστοποίηση:

(i) *σύνθεση: αν $g : \mathbb{N}^k \to \mathbb{N}$ και $h_1, \ldots h_k : \mathbb{N}^m \to \mathbb{N}$ είναι αναδρομικές, τότε είναι αναδρομική και η $f : \mathbb{N}^m \to \mathbb{N}$ που ορίζεται από το ακόλουθο σχήμα*

$$f(n_1, \ldots n_m) = g(h_1(n_1, \ldots n_m), \ldots h_k(n_1, \ldots n_m))$$

(ii) *πρωτογενής αναδρομή: αν $g : \mathbb{N}^m \to \mathbb{N}$ και $h : \mathbb{N}^{m+2} \to \mathbb{N}$ είναι αναδρομικές, τότε και η $f : \mathbb{N}^{m+1} \to \mathbb{N}$ που ορίζεται από το ακόλουθο σχήμα είναι αναδρομική*

$$\begin{aligned} f(0, n_1, \ldots n_m) &= g(n_1, \ldots n_m) \\ f(n+1, n_1, \ldots n_m) &= h(f(n, n_1, \ldots n_m), n, n_1, \ldots n_m) \end{aligned}$$

(iii) *ελαχιστοποίηση: αν* $g : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$ *είναι αναδρομική και αν για όλα τα* $n_1, \ldots n_m$ *υπάρχει* n *ώστε* $g(n, n_1, \ldots n_m) = 0$*, τότε και η* $f : \mathbb{N}^m \rightarrow \mathbb{N}$ *που ορίζεται από το παρακάτω σχήμα είναι αναδρομική*

$$f(n_1, \ldots n_m) = \mu n.g(n, n_1, \ldots n_m) = 0$$

όπου $\mu n.g(n, n_1, \ldots n_m) = 0$ *δηλώνει τον μικρότερο αριθμό* n *για τον οποίο ισχύει η* $g(n, n_1, \ldots n_m) = 0$*. Σημειώνεται ότι έχουμε προϋποθέσει την ύπαρξη ενός τέτοιου* n *για κάθε* $n_1, \ldots n_m$*, άρα και την ύπαρξη ενός τέτοιου ελάχιστου.*

Παρατήρηση: Η μικρότερη κλάση αριθμητικών συναρτήσεων που περιλαμβάνει τις αρχικές συναρτήσεις και είναι κλειστή για τη σύνθεση και την πρωτογενή αναδρομή είναι η κλάση των πρωτογενών αναδρομικών συναρτήσεων. Ενώ αυτή που περιλαμβάνει τις αρχικές συναρτήσεις και είναι κλειστή για τη σύνθεση και την ελαχιστοποίηση (χωρίς το σχήμα της πρωτογενούς αναδρομής) αποδεικνύεται ότι είναι ίση με την κλάση των αναδρομικών συναρτήσεων που ορίστηκε πιο πάνω, δηλαδή το σχήμα της αναδρομής μπορεί να οριστεί με βάση το σχήμα της ελαχιστοποίησης. Η κλάση των πρωτογενών αναδρομικών συναρτήσεων είναι γνήσια υποκλάση των αναδρομικών συναρτήσεων, π.χ. η συνάρτηση Ackermann είναι αναδρομική χωρίς να είναι πρωτογενής αναδρομική. Η κλάση των αναδρομικών συναρτήσεων γενικά πιστεύεται ότι συμπίπτει με την κλάση των *υπολογίσιμων συναρτήσεων*, δηλαδή των συναρτήσεων που μπορούν να υπολογιστούν με βάση ένα αλγόριθμο ή αλλιώς με τη χρήση οδηγιών μηχανικού υπολογισμού (*Αίτημα του Church*).

Στη συνέχεια, θα δούμε ότι όλες οι αναδρομικές συναρτήσεις είναι λ-ορίσιμες.

Λήμμα 1.1 *Οι αρχικές συναρτήσεις είναι λ-ορίσιμες.*

Απόδειξη: Ορίζουμε

$$\begin{array}{lcl} U_i^m & \equiv & \lambda x_1 \ldots \lambda x_m.\, x_i \\ S^+ & \equiv & \lambda x.\, \lambda y.\, \lambda z.\, y\,(x\,y\,z) \\ Z & \equiv & \lambda x.\, \boldsymbol{c}_0 \end{array}$$

Λήμμα 1.2 *Οι λ-ορίσιμες συναρτήσεις είναι κλειστές για τη σύνθεση.*

Απόδειξη: Έστω $g : \mathbb{N}^k \to \mathbb{N}$ είναι λ-ορίσιμη από τον όρο $G \in \Lambda$ και $h_1, \ldots h_k : \mathbb{N}^m \to \mathbb{N}$ είναι λ-ορίσιμες από τους $H_1, \ldots H_k \in \Lambda$, αντίστοιχα. Τότε η

$$f(n_1, \ldots n_m) \quad = \quad g(h_1(n_1, \ldots n_m), \ldots h_k(n_1, \ldots n_m))$$

είναι λ-ορίσιμη από τον

$$F \quad \equiv \quad \lambda x_1 \ldots \lambda x_m.\, G\,(H_1\, x_1 \cdots x_m) \cdots (H_k\, x_1 \cdots x_m)$$

Λήμμα 1.3 *Οι λ-ορίσιμες συναρτήσεις είναι κλειστές για το σχήμα της πρωτογενούς αναδρομής.*

Απόδειξη: Η απόδειξη είναι αρκετά κολπατζίδικη. Έστω $g : \mathbb{N}^m \to \mathbb{N}$ είναι λ-ορίσιμη από τον $G \in \Lambda$ και $h : \mathbb{N}^{m+2} \to \mathbb{N}$ είναι λ-ορίσιμη από τον $H \in \Lambda$. Τότε πρέπει να βρούμε $F \in \Lambda$ που να ορίζει στο λ-λογισμό τη συνάρτηση

$$\begin{array}{lcl} f(0, n_1, \ldots n_m) & = & g(n_1, \ldots n_m) \\ f(n+1, n_1, \ldots n_m) & = & h(f(n, n_1, \ldots n_m), n, n_1, \ldots n_m) \end{array}$$

Η ιδέα είναι να παραστήσουμε με διατεταγμένα ζεύγη τα ζεύγη $[n, f(n)]$, όπου $f(n)$ η τιμή της συνάρτησης στο όρισμα n. Για να το πετύχουμε αυτό θα πρέπει να αρχίσουμε από το ζεύγος $[0, g(n_1, \dots n_m)]$ και να επαναλάβουμε n φορές έναν τελεστή **next** που θα έχει την ιδιότητα

$$\mathbf{next}\,([n, x]) \quad = \quad [n+1, h(x, n, n_1, \dots n_m)]$$

Ο λ-όρος που θα έχει αυτή την ιδιότητα μπορεί να είναι ο

$$\mathbf{next} \quad \equiv \quad \lambda p.\, [S^+(p\,\pi_1), H\,(p\,\pi_2)(p\,\pi_1)x_1 \cdots x_m]$$

Η επανάληψη κατά n φορές του **next** μπορεί να επιτευχθεί χρησιμοποιώντας το νούμερο $\boldsymbol{c}_n$, διότι $\boldsymbol{c}_n\,\mathbf{next}\,N =_\beta (\mathbf{next})^n\,(N)$. Οπότε αν ξεκινήσουμε με $N \equiv [\boldsymbol{c}_0, G\,x_1 \cdots x_m]$ (που παριστάνει το $[0, g(n_1, \dots n_m)]$) τότε το $\boldsymbol{c}_n\,\mathbf{next}\,N$ θα είναι η επανάληψη του $[0, g(n_1, \dots n_m)]$ κατά n φορές, άρα το ζεύγος $[n, f(n)]$. Και σ'αυτό το ζεύγος μπορούμε να εξαγάγουμε τη δεύτερη συνιστώσα χρησιμοποιώντας το π_2. Οπότε τελικά ο όρος F θα είναι

$$F \quad \equiv \quad \lambda x.\, \lambda x_1.\, \dots \lambda x_m.\, x\,\mathbf{next}\,[\boldsymbol{c}_0, G\,x_1 \cdots x_m]\,\pi_2$$

Πριν προχωρήσουμε στο να αποδείξουμε ότι το σχήμα της ελαχιστοποίησης μπορεί να οριστεί στο λ-λογισμό, θα δούμε πρώτα πώς μπορεί να εκφραστεί γενικότερα η αναδρομή στο λ-λογισμό.

Θεώρημα 1.2 (Θεώρημα του Σταθερού Σημείου)

(i) *Για κάθε* $F \in \Lambda$ *υπάρχει ένας* $X \in \Lambda$ *ώστε*

$$F\,X =_\beta X \qquad \textit{(X είναι σταθερό σημείο του F)}$$

(ii) *Υπάρχει ένας* συνδυαστής σταθερού σημείου $\mathsf{Y} \in \Lambda$ *ώστε για όλα τα* $F \in \Lambda$

$$F\,(\mathsf{Y}\,F) =_\beta \mathsf{Y}\,F$$

[δηλαδή για κάθε F*,* $\mathsf{Y}\,F$ *είναι σταθερό σημείο του* F*]*

Απόδειξη: Έστω $\mathsf{Y} \equiv \lambda f.\,(\lambda x.\,f\,(x\,x))\,\lambda x.\,f\,(x\,x)$. Τότε

$$\begin{aligned}
\mathsf{Y}\,F &\equiv (\lambda f.\,(\lambda x.\,f\,(x\,x))\,\lambda x.\,f\,(x\,x))\,F \\
&=_\beta (\lambda x.\,F\,(x\,x))\,\lambda x.\,F\,(x\,x) \\
&=_\beta F\,((\lambda x.\,F\,(x\,x))\,\lambda x.\,F\,(x\,x)) \\
&=_\beta F\,(\mathsf{Y}\,F) \qquad [\text{διότι } \mathsf{Y}\,F \to_\beta (\lambda x.\,F\,(x\,x))\,\lambda x.\,F\,(x\,x)]
\end{aligned}$$

Πόρισμα 1.7 *Δοθέντος* λ*-όρου* $M \equiv M[f]$ *που ενδεχομένως έχει ως ελεύθερη μεταβλητή την* f*, υπάρχει* $F \in \Lambda$ *ώστε*

$$F =_\beta M[f := F]$$

Απόδειξη: Πρέπει

$$F =_\beta M[f := F] =_\beta (\lambda f.\,M)\,F$$

Οπότε αρκεί να επιλέξουμε τον F ως το σταθερό σημείο του $\lambda f.\,M$, δηλαδή

$$F \equiv Y\,(\lambda f.\,M)$$

<u>Παρατήρηση:</u> Το ως άνω πόρισμα μπορεί να διατυπωθεί ως εξής: Η εξίσωση $x =_\beta M$ μπορεί να λυθεί ως προς x, ή γενικότερα η εξίσωση $x\,y_1 \cdots y_n =_\beta M$ μπορεί να λυθεί ως προς x, δηλαδή υπάρχει F ώστε

$$\forall Y_1, \ldots Y_n, \quad F\,Y_1 \cdots Y_n =_\beta M\,[x := F][y_1 := Y_1] \cdots [y_n := Y_n]$$

Αρκεί να ορίσουμε $F \equiv \mathsf{Y}\,(\lambda x\ y_1 \ldots y_n.\,M)$.

Ως μία εφαρμογή, μπορούμε να κατασκευάσουμε όρους F και G ώστε για κάθε $X, Y \in \Lambda$ ισχύουν

$$\begin{array}{lll} F\,X & =_\beta & X\,F \\ G\,X\,Y & =_\beta & Y\,G\,(Y\,X\,G) \end{array}$$

Λήμμα 1.4 *Οι λ-ορίσιμες συναρτήσεις είναι κλειστές για την ελαχιστοποίηση.*

Απόδειξη: Έστω $g : \mathbb{N}^{m+1} \to \mathbb{N}$ είναι λ-ορίσιμη από τον $G \in \Lambda$ και έστω ότι για όλα τα $n_1, \ldots n_m$ υπάρχει n ώστε $g(n, n_1, \ldots n_m) = 0$. Θέλουμε να ορίσουμε στον λ-λογισμό την

$$f(n_1, \ldots n_m) = \mu m.\ g(m, n_1, \ldots n_m) = 0$$

Ορίζουμε μία συνάρτηση **zero** που ελέγχει αν ένα αριθμητικό όρισμα είναι 0 ή όχι

$$\mathbf{zero} \equiv \lambda n.\, n\, (\mathbf{true}\, \mathbf{false})\, \mathbf{true}$$

Τότε

$$\begin{aligned} \mathbf{zero}\, \boldsymbol{c}_0 &=_\beta \mathbf{true} \\ \mathbf{zero}\, \boldsymbol{c}_{n+1} &=_\beta \mathbf{false} \end{aligned}$$

Η ιδέα είναι η εξής: Θα ξεκινήσουμε από το $g(0, n_1, \ldots n_m)$ και θα ελέγχουμε το κάθε $g(n, n_1, \ldots n_m)$. Αν αυτό είναι 0, τότε θα επιστρέφουμε το n (δηλαδή το πρώτο n που θα ικανοποιεί την $g(n, n_1, \ldots n_m) = 0$). Αν όχι θα ελέγχουμε το $g(n+1, n_1, \ldots n_m)$. Η διαδικασία αυτή του διαδοχικού ελέγχου επιτυγχάνεται μέσω μίας συνάρτησης H, η οποία θα ικανοποιεί το ακόλουθο σχήμα

$$H\, y\, x_1 \cdots x_m =_\beta \mathbf{if}\ (\mathbf{zero}\ (G\, y\, x_1 \cdots x_m))\ \mathbf{then}\ y\ \mathbf{else}\ H\, (S^+\, y)\, x_1 \cdots x_m$$

Από το θεώρημα του σταθερού σημείου υπάρχει όρος H που ικανοποιεί την ως άνω εξίσωση. Ορίζουμε $F \equiv \lambda x_1 \cdots x_n.\, H\, \boldsymbol{c}\, x_1 \cdots x_n$, οπότε

$$
\begin{aligned}
F\,\boldsymbol{c}_{n_1}\cdots\boldsymbol{c}_{n_m} &=_\beta H\,\boldsymbol{c}_0\,\boldsymbol{c}_{n_1}\cdots\boldsymbol{c}_{n_m}\\
&=_\beta \begin{cases} \boldsymbol{c}_0, & \text{αν } G\,\boldsymbol{c}_0\,\boldsymbol{c}_{n_1}\cdots\boldsymbol{c}_{n_m} =_\beta \boldsymbol{c}_0\\ H\,\boldsymbol{c}_1\,\boldsymbol{c}_{n_1}\cdots\boldsymbol{c}_{n_m}, & \text{διαφορετικά}\end{cases}\\
&=_\beta \begin{cases} \boldsymbol{c}_1, & \text{αν } G\,\boldsymbol{c}_1\,\boldsymbol{c}_{n_1}\cdots\boldsymbol{c}_{n_m} =_\beta \boldsymbol{c}_0\\ H\,\boldsymbol{c}_2\,\boldsymbol{c}_{n_1}\cdots\boldsymbol{c}_{n_m}, & \text{διαφορετικά}\end{cases}\\
&\quad \text{κ.ο.κ}\\
&\quad [\text{κάποτε θα σταματήσει στο ελάχιστο}]
\end{aligned}
$$

Θεώρημα 1.3 *Όλες οι αναδρομικές συναρτήσεις είναι λ-ορίσιμες.*

Απόδειξη: Από τα προηγούμενα λήμματα.

Παρατήρηση: Το αντίστροφο επίσης ισχύει. Δηλαδή κάθε λ-ορίσιμη αριθμητική συνάρτηση είναι αναδρομική. Το αποτέλεσμα μπορεί να επεκταθεί και στις μερικές συναρτήσεις. Έτσι, λοιπόν, έχουμε μία πλήρη ταύτιση μεταξύ των (μερικών) αναδρομικών συναρτήσεων και των λ-ορίσιμων συναρτήσεων. Και οι δύο αυτοί φορμαλισμοί σκοπεύουν να ορίσουν με ακριβή τρόπο την έννοια της υπολογίσιμης συνάρτησης. Μία άλλη προσέγγιση, είναι ο φορμαλισμός του Turing και οι Turing-υπολογίσιμες συναρτήσεις. Η ισοδυναμία όλων αυτών των προσεγγίσεων ενισχύει την πεποίθηση ότι οι αναδρομικές συναρτήσεις ταυτίζονται με τις (είναι ο σωστός τρόπος να οριστούν οι) υπολογίσιμες συναρτήσεις.

Στη συνέχεια, θα δώσουμε κάποια αποτελέσματα αναποκρισιμότητας. Έστω η συνάρτηση $\langle \cdot\,,\cdot \rangle : \mathbb{N}^2 \rightarrow \mathbb{N}$ είναι μία 1-1 και επί αναδρομική απεικόνιση. Δηλαδή κάθε ζεύγος (n, m) φυσικών αριθμών παίρνει ένα μοναδικό κωδικό αριθμό $\langle n\,, m\rangle$.
(Άσκηση: Ορίστε μία τέτοια συνάρτηση.
Υπόδειξη: Για κάθε n διατάξτε τα ζεύγη (x, y) ώστε $x + y = n$. Δηλαδή

$$\underbrace{(0,0)}_{x+y=0}, \underbrace{(0,1),(1,0)}_{x+y=1}, \underbrace{(0,2),(1,1),(2,0)}_{x+y=2}, \text{κ.ο.κ.}$$

και ορίστε τη συνάρτηση διάταξης.) Θα δώσουμε τώρα σε κάθε όρο $L \in \Lambda$ ένα μοναδικό κωδικό $\#(L)$. Με επαγωγή στους όρους:

$$\begin{array}{rcl}
\#(u^{\overbrace{\prime\prime\cdots\prime}^{n \text{ φορές}}}) & = & \langle 0\,, n\rangle, \text{όπου } u^{\overbrace{\prime\prime\cdots\prime}^{n \text{ φορές}}} \text{ είναι η } n-\text{ οστή μεταβλητή} \\
\#(M\,N) & = & \langle 2\,, \langle \#(M)\,, \#(N)\rangle\rangle \\
\#(\lambda x.\, M) & = & \langle 3\,, \langle \#(x)\,, \#(M)\rangle\rangle
\end{array}$$

Συμβολίζουμε με $\ulcorner M \urcorner$ το $\boldsymbol{c}_{\#(M)}$ δηλαδή το $\ulcorner M \urcorner$ είναι ο όρος (νούμερο Church) που αναπαριστά στο λ-λογισμό τον κωδικό του M.

Ορισμός 1.15 *Έστω $\mathcal{A} \subseteq \Lambda$.*

1. *$\mathcal{A}$ είναι κλειστό για το $=_\beta$ αν*

$$M \in \mathcal{A}, M =_\beta N \Rightarrow N \in \mathcal{A}$$

2. *$\mathcal{A}$ είναι μη-τετριμμένο αν $\mathcal{A} \neq \emptyset$ και $\mathcal{A} \neq \Lambda$*

3. *$\mathcal{A}$ είναι αναδρομικό αν το σύνολο $\#\mathcal{A} = \{\#M | M \in \mathcal{A}\}$ είναι αναδρομικό*[4]

[4]Ένα υποσύνολο των φυσικών αριθμών A είναι αναδρομικό εάν η χαρακτηριστική του συνάρτηση f_A, που ορίζεται ως $f_A = 0$ αν $x \in A$ και $f_A = 1$ αν $x \notin A$, είναι αναδρομική. Σύμφωνα με το αίτημα του Church ένα σύνολο είναι αναδρομικό στην περίπτωση που μπορούμε να αποφασίσουμε αλγοριθμικά αν ένας αριθμός ανήκει στο σύνολο ή όχι.

Θεώρημα 1.4 *Έστω $\mathcal{A} \subseteq \Lambda$ είναι μη-τετριμμένο και κλειστό για την ισότητα $=_\beta$. Τότε $\mathcal{A}$ δεν είναι αναδρομικό.*

<u>Απόδειξη:</u> Ορίζουμε $\mathcal{B} = \{M | M \ulcorner M \urcorner \in \mathcal{A}\}$. Εάν $\mathcal{A}$ είναι αναδρομικό τότε και $\mathcal{B}$ είναι αναδρομικό (γιατί;). Οπότε είναι αναπαραστάσιμο στο λ-λογισμό δηλαδή υπάρχει $F \in \Lambda$ ώστε

$$\begin{array}{lll} M \in \mathcal{B} & \Leftrightarrow & F \ulcorner M \urcorner =_\beta \mathbf{c}_0 \\ M \notin \mathcal{B} & \Leftrightarrow & F \ulcorner M \urcorner =_\beta \mathbf{c}_1 \end{array}$$

Έστω $M_0 \in \mathcal{A}$ και $M_1 \notin \mathcal{A}$. Μπορούμε να ορίσουμε $G \in \Lambda$ ώστε

$$\begin{array}{lllllll} M \in \mathcal{B} & \Leftrightarrow & G \ulcorner M \urcorner =_\beta M_1 \notin \mathcal{A} & & & & \\ M \notin \mathcal{B} & \Leftrightarrow & F \ulcorner M \urcorner =_\beta M_0 \in \mathcal{A} & & & & \\ & & [\text{π.χ. παίρνουμε } G\,x \equiv \textbf{if zero}\,(F\,x)\ \textbf{then}\ M_1\ \textbf{else}\ M_0] & & & & \\ G \in \mathcal{B} & \Leftrightarrow & G \ulcorner G \urcorner =_\beta M_1 & \Rightarrow & G \ulcorner G \urcorner \notin \mathcal{A} & \Rightarrow & G \notin \mathcal{B} \\ G \notin \mathcal{B} & \Leftrightarrow & G \ulcorner G \urcorner =_\beta M_0 & \Rightarrow & G \ulcorner G \urcorner \in \mathcal{A} & \Rightarrow & G \in \mathcal{B} \end{array}$$

Πόρισμα 1.8 (Church) *Το σύνολο $\{M \in \Lambda | M =_\beta \mathbf{true}\}$ δεν είναι αναδρομικό.*

Πόρισμα 1.9 *Το σύνολο $\{M \in \Lambda | M$ έχει β-κανονική μορφή$\}$ δεν είναι αναδρομικό.*

Κεφάλαιο 2

Λάμδα λογισμός με απλούς τύπους

Στον καθαρό λ-λογισμό θεωρήσαμε ότι μία συνάρτηση δεν έχει προκαθορισμένο *πεδίο ορισμού* και *πεδίο τιμών*. Δεν υπάρχουν απαιτήσεις προκαθορισμένου προσδιορισμού ότι π.χ. μία συνάρτηση (όπως η $n \mapsto n^3$) δέχεται ως ορίσματα φυσικούς αριθμούς και επιστρέφει φυσικούς αριθμούς. Η επιβολή τέτοιου είδους απαιτήσεων γίνεται μέσω των τύπων. Ο κάθε όρος (πρόγραμμα) συνοδεύεται από ένα τύπο, ο οποίος μπορεί να θεωρηθεί ως ένας προσδιορισμός ή σχόλιο (specification) για το τι κάνει ένα πρόγραμμα. Ο Curry και ο Church εισήγαγαν τέτοιες εκδοχές λ-λογισμού με τύπους.

2.1 λ-λογισμός με απλούς τύπους à la Curry

Το πρώτο σύστημα που εισάγουμε είναι το σύστημα του Curry.

Ορισμός 2.1 (Τύποι) *Έστω U ένα αριθμήσιμο πλήθος συμβόλων που θα ονομάζονται* ατομικοί τύποι *ή και* μεταβλητές τύπων. *Το σύνολο των τύπων T ορίζεται επαγωγικά ως εξής:*

1. *Κάθε στοιχείο του U είναι τύπος.*

2. *Αν σ και τ τύποι τότε η έκφραση $(\sigma \to \tau)$ είναι τύπος.*

Ή χρησιμοποιώντας εναλλακτικό ορισμό

$$T ::= U \mid (T \to T)$$

Θα χρησιμοποιήσουμε τα $\alpha, \beta, \gamma \ldots$ για ατομικούς τύπους και τα $\sigma, \tau, \rho \ldots$ γενικά για τύπους. Θα παραλείπουμε τις εξωτερικές παρενθέσεις στη γραφή των τύπων.

Ορισμός 2.2 Περιβάλλον *ή* Βάση *θα είναι κάθε σύνολο της μορφής*

$$\{x_1 : \tau_1, \ldots, x_n : \tau_n\}$$

όπου $x_1, \ldots x_n \in \Lambda$ δηλαδή είναι μεταβλητές-όροι του λ-λογισμού και $\tau_1, \ldots, \tau_n$ τύποι.

Θα πρέπει $x_i \neq x_j$ για $i \neq j$, δηλαδή δεν μπορεί να έχουμε αντιστοιχήσει στην ίδια μεταβλητή δύο διαφορετικούς τύπους. Εάν $\Gamma = \{x_1 : \tau_1, \ldots, x_n : \tau_n\}$, τότε $\mathrm{dom}(F) = \{x_1, \ldots, x_n\}$. To $\mathrm{dom}(F)$ είναι το πεδίο του Γ. Κάθε περιβάλλον Γ μπορεί να θεωρηθεί ως μία απονομή ενός τύπου σε κάθε μεταβλητή του πεδίου του (αν $x : \tau \in \Gamma$ τότε ο τύπος τ απονέμεται στη μεταβλητή x). Συνήθως γράφουμε $x_1 : \tau_1, \ldots x_n : \tau_n$ αντί του $\{x_1 : \tau_1, \ldots x_n : \tau_n\}$ και $\Gamma, x : \tau$ αντί του $\Gamma \cup \{x : \tau\}$. Στην τελευταία περίπτωση, προϋπόθεση για να γράψουμε αυτό είναι ότι $x : \tau \notin \Gamma$, δηλαδή η μεταβλητή x δεν έχει απονομή στο Γ.

Κανόνες Τυποποίησης: Ορίζουμε τη σχέση $\Gamma \vdash M : \sigma$, όπου Γ περιβάλλον, M λ-όρος και σ τύπος, ορίζοντας επαγωγικά τα αξιώματα και τους κανόνες απαγωγής.

Αξίωμα: $\Gamma, x : \tau \vdash x : \tau$

Κανόνες: $\dfrac{\Gamma, x{:}\sigma \vdash M{:}\tau}{\Gamma \vdash \lambda x.\, M{:}\sigma \to \tau} \qquad \dfrac{\Gamma \vdash M{:}\sigma \to \tau \qquad \Gamma \vdash N{:}\sigma}{\Gamma \vdash M\, N{:}\tau}$

Παρατήρηση: 1. Το $\Gamma \vdash M : \sigma$ θα ισχύει αν έχει προκύψει από τα αξιώματα με διαδοχικές εφαρμογές των κανόνων απαγωγής.
2. Στον πρώτο κανόνα η μεταβλητή x μπορεί να θεωρηθεί ως ιδιομεταβλητή. Αν υποθέσουμε ότι έχουμε αποδείξει το $\Gamma \vdash \lambda x.\, M : \sigma \to \tau$ θα θεωρούμε ότι η x δεν εμφανίζεται στο Γ (αλλιώς παίρνουμε ένα α-ισοδύναμο του $\lambda x.\, M$) ώστε να μπορούμε να σχηματίζουμε το $\Gamma, x : \sigma \vdash M : \tau$ (π.χ. ως επαγωγική υπόθεση) το οποίο απαιτεί $x : \sigma \notin \Gamma$. Όταν γράφουμε $\vdash M : \sigma$ εννοούμε ότι ο όρος M τυποποιείται με κενό περιβάλλον ($\Gamma = \emptyset$).
3. Το σύστημα τυποποίησης που περιγράφτηκε είναι ο λ-λογισμός με απλούς τύπους à la Curry. Μέσω του μηχανισμού αυτού τυποποίησης αποδίδεται ένας τύπος σ σε έναν (αλλά όχι και σε κάθε) λ-όρο M.

Παραδείγματα

1. $\vdash \lambda x.\, x : \sigma \to \sigma$ διότι υπάρχει η απαγωγή $\dfrac{x : \sigma \vdash x : \sigma}{\vdash \lambda x.\, x : \sigma \to \sigma}$

2. $\vdash \lambda x\ y.\, x : \sigma \to (\tau \to \sigma)$ διότι $\dfrac{\dfrac{x : \sigma, y : \tau \vdash x : \sigma}{x : \sigma \vdash \lambda y.\, x : \tau \to \sigma}}{\vdash \lambda x\ y.\, x : \sigma \to (\tau \to \sigma)}$

Ορισμός 2.3 *Έστω M λ-όρος. Εάν υπάρχουν Γ και σ ώστε $\Gamma \vdash M : \sigma$ τότε M λέγεται* τυποποιήσιμος.

Παρατήρηση: Ένας όρος ο οποίος μπορεί να τυποποιηθεί με τύπο $\sigma \to \tau$ μπορεί να νοηθεί ότι αναπαριστά μία (κατασκευαστική) συνάρτηση, η οποία δέχεται ορίσματα (όρους) τύπου σ και επιστρέφει τιμές τύπου τ. Αυτό αντανακλάται στους κανόνες απαγωγής όπου όταν απονέμεται ο τύπος $\sigma \to \tau$ δημιουργείται μία αφαίρεση $\lambda x. M$ (το x «έχει» τύπο σ και το M τύπο τ) και όταν απονέμεται ο τύπος τ στην εφαρμογή $M\,N$ προϋποτίθεται ότι η «συνάρτηση» M που «έχει» τύπο $\sigma \to \tau$ εφαρμόζεται στην N που «έχει» τύπο σ.

Λήμμα 2.1 *Έστω $\Gamma \vdash M : \sigma$. Τότε:*

1. $\Gamma \subseteq \Gamma' \Rightarrow \Gamma' \vdash M : \sigma$
2. $\boldsymbol{FV}(M) \subseteq \mathrm{dom}(\Gamma)$
3. *Αν $\Gamma' \subseteq \Gamma$ και $\mathrm{dom}(\Gamma') = \boldsymbol{FV}(M)$ τότε $\Gamma' \vdash M : \sigma$. (Δηλαδή σε μία τυποποίηση ενός όρου μπορούμε να αρκεστούμε σε απονομές τύπων μόνο για τις ελεύθερες μεταβλητές αυτού του όρου).*

Απόδειξη: Με προφανή επαγωγή στην τυποποίηση του $\Gamma \vdash M : \sigma$ (Άσκηση).
Π.χ. έστω ότι θέλουμε να αποδείξουμε το 1, στην περίπτωση που $\Gamma \vdash \lambda x. M : \sigma \to \tau$. Τότε μπορούμε να θεωρήσουμε ότι το x δεν εμφανίζεται στο $\mathrm{dom}(\Gamma')$. Επειδή $\Gamma, x : \sigma \vdash M : \tau$ από Ε.Υ. (Επαγωγική Υπόθεση) έχουμε $\Gamma', x : \sigma \vdash M : \tau$ (διότι $\Gamma, x : \sigma \subseteq \Gamma', x : \sigma$). Οπότε $\Gamma' \vdash \lambda x. M : \sigma \to \tau$.

Οι τύποι που αποδίδονται σε κάποιο όρο εξαρτώνται από τη μορφή του όρου, σύμφωνα με το παρακάτω λήμμα.

Λήμμα 2.2 (Δημιουργίας) *Ισχύουν τα παρακάτω:*

1. $\Gamma \vdash x : \sigma \Rightarrow x : \sigma \in \Gamma$
2. $\Gamma \vdash M\,N : \sigma \Rightarrow$ *Υπάρχει τύπος τ ώστε* $\Gamma \vdash M : \tau \to \sigma$ *και* $\Gamma \vdash N : \tau$.

3. $\Gamma \vdash \lambda x.\, M : \sigma \Rightarrow$ *Υπάρχουν τύποι* τ *και* ρ *ώστε* $\Gamma, x : \tau \vdash M : \rho$ *και* $\sigma = \tau \to \rho$.

Απόδειξη: Εύκολη επαγωγή στο μήκος της τυποποίησης του όρου.

Ορισμός 2.4 *Ένας τύπος δημιουργείται με αφετηρία τις μεταβλητές τύπων (ατομικοί τύποι). Αν* σ *τύπος τότε με* $\sigma[\alpha := \tau]$ *συμβολίζουμε τον τύπο που προκύπτει από το* σ *αφού αντικαταστήσουμε κάθε εμφάνιση του* α *στον* σ *με τον τύπο* τ. *Αν* $\Gamma = \{x_1 : \sigma_1, \ldots, x_n : \sigma_n\}$ *τότε* $\Gamma[\alpha := \tau] = \{x_1 : \sigma_1[\alpha := \tau], \ldots, x_n : \sigma_n[\alpha := \tau]\}$.

Πρόταση 2.1 (Το λήμμα της αντικατάστασης) *Ισχύουν τα παρακάτω:*

1. *Αν* $\Gamma \vdash M : \sigma$, *τότε* $\Gamma[\alpha := \tau] \vdash M : \sigma[\alpha := \tau]$.

2. *Αν* $\Gamma, x : \tau \vdash M : \sigma$ *και* $\Gamma \vdash N : \tau$, *τότε* $\Gamma \vdash M[x := N] : \sigma$

Απόδειξη του 2: Με επαγωγή στο $\Gamma, x : \tau \vdash M : \sigma$. Αν είναι αξίωμα, τότε $M \equiv x$ και $\tau = \sigma$ ή $M \equiv y \in \mathrm{dom}(\Gamma)$ $(y \neq x)$. Στην πρώτη περίπτωση, $M[x := N] \equiv N$ οπότε $\Gamma \vdash N : \sigma$ $(= \tau)$ εξ' υποθέσεως, ενώ στη δεύτερη $M[x := N] \equiv y$ άρα, επειδή $\Gamma, x : \tau \vdash y : \sigma$, θα πρέπει και $\Gamma \vdash y : \sigma$.
Αν έχει προκύψει από κανόνα απαγωγής.

Περίπτωση: $$\frac{\Gamma, x : \tau, y : \sigma_1 \vdash P : \sigma_2}{\Gamma, x : \tau \vdash \lambda y.\, P : \sigma_1 \to \sigma_2}$$

όπου $M \equiv \lambda y.\, P$ και $\sigma = \sigma_1 \to \sigma_2$ και y καινούργια μεταβλητή.
Από Ε.Υ. $\Gamma, y : \sigma_1 \vdash P[x := N] : \sigma_2$ (επειδή $\Gamma, y : \sigma_1 \vdash N : \tau$), άρα $\Gamma \vdash \lambda y.\, P[x := N] : \sigma_1 \to \sigma_2$ οπότε το ζητούμενο επειδή $(\lambda y.\, P)[x := N] \equiv \lambda y.\, P[x := N]$. Η άλλη περίπτωση παρομοίως.

Το λήμμα της αντικατάστασης έχει ως σημαντικό αποτέλεσμα την ακόλουθη πρόταση.

Πρόταση 2.2 (Subject reduction) *Εάν* $\Gamma \vdash M : \sigma$ *και* $M \twoheadrightarrow_\beta N$ *τότε* $\Gamma \vdash N : \sigma$*.*

Απόδειξη: Αρκεί να αποδείξουμε την πρόταση στην περίπτωση του $M \rightarrow_\beta N$. Μπορούμε να εργαστούμε με επαγωγή στον τρόπο με τον οποίο δημιουργείται η σχέση $M \rightarrow_\beta N$. Η αρχική περίπτωση είναι όταν $M \equiv (\lambda x.\, P)Q$ και $N \equiv P[x := Q]$. Από $\Gamma \vdash (\lambda x.\, P)\, Q : \sigma$ παίρνουμε ότι $\Gamma \vdash (\lambda x.\, P) : \rho \rightarrow \sigma$ και $\Gamma \vdash Q : \rho$, για κάποιο ρ (Λήμμα δημιουργίας). Επίσης από λήμμα δημιουργίας $\Gamma, x : \rho \vdash P : \tau$. Οπότε από λήμμα αντικατάστασης $\Gamma \vdash P[x := Q] : \sigma$.
Οι υπόλοιπες περιπτώσεις με παρόμοιο (και πιο εύκολο) τρόπο.
Παρατήρηση: Η ιδιότητα $\Gamma \vdash N : \sigma \,\wedge\, M \twoheadrightarrow_\beta N \Rightarrow \Gamma \vdash M : \sigma$ (Subject Expansion) δεν ισχύει για το σύστημα τυποποίησης à la Curry.

Πρόταση 2.3 (Church–Rosser για τους τυποποιήσιμους όρους) *Έστω* $\Gamma \vdash N : \sigma$ *και έστω* $M \twoheadrightarrow_\beta M'$ *και* $M \twoheadrightarrow_\beta M''$*. Τότε υπάρχει όρος* L *ώστε* $M' \twoheadrightarrow_\beta L$ *και* $M'' \twoheadrightarrow_\beta L$ *και* $\Gamma \vdash L : \sigma$*.*

Απόδειξη: Από το θεώρημα Church–Rosser για το λ-λογισμό και την ιδιότητα Subject Reduction.

2.2 λ-λογισμός με απλούς τύπους à la Church

Στο σύστημα τυποποίησης του Curry υπάρχει ήδη ο όρος του λ-λογισμού και «εκ των υστέρων» τυποποιείται. Γι' αυτό και είναι γνωστό ως *σύστημα απονομής τύπων*. Στο σύστημα του Church ο όρος δημιουργείται ταυτόχρονα με την τυποποίησή του. Σε κάθε στάδιο της κατασκευής του «φέρει» τον τύπο του και μόνον όροι με τους σωστούς τύπους μπορούν να συνθέσουν ένα καινούριο όρο.

Ορισμός 2.5 (Τύπος) *Οι τύποι είναι ίδιοι με το σύστημα του Curry.*

Θα παρουσιάσουμε δύο τρόπους δημιουργίας λ-όρων με τύπους. Ο πρώτος είναι ο αρχικός τρόπος σχηματισμού που χρησιμοποίησε ο Church (αρχικό σύστημα Church) και ο δεύτερος μία προσαρμογή του πρώτου στον τρόπο τυποποίησης à la Curry. (Θα αναφέρεται απλά ως σύστημα (à la) Church).

2.2.1 Αρχικό σύστημα Church

Μεταβλητές όρων: Για κάθε τύπο σ υπάρχει ένα αριθμήσιμο πλήθος μεταβλητών τύπου σ. Οι μεταβλητές τύπου σ θα γράφονται ως x^σ (θα νοούνται δηλαδή ως ζεύγη (x, σ)), όπου x είναι ένα σύμβολο μεταβλητής. Υποθέτουμε ότι αν $\sigma \neq \tau$ τότε στις x^σ και y^τ έχουμε $x \not\equiv y$, δηλαδή χρησιμοποιούμε διαφορετικά σύμβολα μεταβλητών για τους διαφορετικούς τύπους. Αν λοιπόν V_σ είναι το σύνολο των συμβόλων μεταβλητών για κάθε τύπο σ [δηλαδή (i). $x \in V_\sigma \Rightarrow x^\sigma$ είναι μεταβλητή τύπου σ και (ii). $\sigma \neq \tau \Rightarrow V_\sigma \cap V_\tau = \emptyset$], τότε $V = \cup_{\sigma \in T} V_\sigma$ είναι το σύνολο όλων των συμβόλων μεταβλητών.

Ορισμός 2.6 (Όροι) *Το σύνολο των όρων ορίζεται επαγωγικά ως εξής:*

1. *Κάθε μεταβλητή x^σ είναι όρος τύπου σ.*

2. *Αν M είναι όρος τύπου $\sigma \to \tau$ και N όρος τύπου σ τότε $(M\,N)$ είναι όρος τύπου τ.*

3. *Αν M είναι όρος τύπου τ και x^σ μεταβλητή τύπου σ τότε $(\lambda x^\sigma . M)$ είναι όρος τύπου $\sigma \to \tau$.*

Συμβολισμοί: Αν M είναι ένας όρος τύπου σ θα γράφουμε πολλές φορές $M \in \sigma$ ή και M^σ. Πολλές φορές θα παραλείπουμε τον τύπο στις μεταβλητές, δηλαδή μπορούμε να γράψουμε $\lambda x. M$. Θα παραλείπουμε τις εξωτερικές παρενθέσεις. Οι όροι του παραπάνω ορισμού θα λέγονται και όροι Church.

Παρατήρηση: Όσον αφορά την α-ισοδυναμία θα ισχύουν τα ίδια με την περίπτωση του λ-λογισμού. Όταν αλλάζουμε το όνομα μιας δεσμευμένης μεταβλητής x^σ αλλάζουμε μόνο το σύμβολο x σε y και διατηρούμε τον ίδιο τύπο σ. Δηλαδή το $\lambda x^\sigma. M$ μετατρέπεται σε $\lambda y^\sigma. M[x^\sigma := y^\sigma]$, όπου y είναι σύμβολο μεταβλητής για τον τύπο σ ($y \in V_\sigma$). Η αντικατάσταση ορίζεται επίσης με τον ίδιο τρόπο αλλά με την προϋπόθεση ότι μία (ελεύθερη) μεταβλητή τύπου σ αντικαθίσταται μόνο από όρο τύπου σ. Δηλαδή ορίζεται μόνο το $M[x^\sigma := N]$ όπου $N \in \sigma$, ως εξής:

1. $x^\sigma[x^\sigma := N] \equiv N$
2. $y^\tau[x^\sigma := N] \equiv y^\tau$, αν $x^\sigma \not\equiv y^\tau$
3. $(P\,Q)[x^\sigma := N] \equiv (P[x^\sigma := N])\,(Q[x^\sigma := N])$
4. $(\lambda x^\sigma. P)[x^\sigma := N] \equiv \lambda x^\sigma. P$
5. $(\lambda y^\tau. P)[x^\sigma := N] \equiv \lambda y^\tau. P[x^\sigma := N]$, αν $x^\sigma \not\equiv y^\tau$

Ένα redex έχει τη μορφή $(\lambda x^\sigma. M)\,N$, όπου βέβαια ο $\lambda x^\sigma. M$ έχει τύπο $\sigma \to \tau$ ($M \in \tau$) και $N \in \sigma$ (αναγκαστικά για να μπορέσει να σχηματιστεί ο όρος). Το contractum θα είναι το $M[x^\sigma := N]$. Είναι προφανές ότι ο όρος που προκύπτει από μία τέτοια αντικατάσταση έχει τον ίδιο τύπο με τον M.

Ένας όρος του αρχικού συστήματος Church είναι σαν ένας όρος του καθαρού λ-λογισμού με τη διαφορά ότι σε όλες τις μεταβλητές, ελεύθερες και δεσμευμένες, υπάρχει μία απονομή-αναγραφή τύπων. Αν «σβήσουμε» αυτές τις απονομές ο όρος αυτός μετατρέπεται σε όρο του λ-λογισμού χωρίς τύπους.

Ορισμός 2.7 *Έστω M όρος του αρχικού συστήματος Church. Ορίζουμε επαγωγικά το $|M|$, το* σβήσιμο των τύπων του *M, ως εξής:*

1. $|x^\sigma| = x$

2. $|M\,N| = |M|\,|N|$

3. $|\lambda x^\sigma.\, M| = \lambda x.\, |M|$

Παρατήρηση: Έστω $V = \cup_{\sigma \in T} V_\sigma$. Μπορούμε να θεωρήσουμε ότι το σύνολο V είναι το σύνολο των μεταβλητών στο σχηματισμό των όρων του καθαρού λ-λογισμού. Δηλαδή, ουσιαστικά, έχουμε διαμερίσει τις μεταβλητές του καθαρού λ-λογισμού σε ένα αριθμήσιμο σύνολο (ένα για κάθε τύπο σ) από αριθμήσιμα σύνολα (τα σύμβολα μεταβλητών για τον τύπο σ). Με αυτήν την παραδοχή ο λ-λογισμός παραμένει ως έχει (ίδιοι όροι). Επιπλέον, μπορούμε να τροποποιήσουμε ελαφρώς την έννοια της α-ισοδυναμίας και να δεχόμαστε ότι οι α-ισοδύναμοι όροι παράγονται μόνο με αντικατάσταση των δεσμευμένων μεταβλητών, που αντιστοιχούν σε σύμβολα μεταβλητών του ίδιου τύπου, π.χ. $\lambda x.\, x$ είναι α-ισοδύναμος με το $\lambda y.\, y$ μόνο εάν $x, y \in V_\sigma$ για κάποιο τύπο σ. Αυτή η παραδοχή έχει την έννοια ότι, αν για κάποιο όρο M του λ-λογισμού χρειαστεί να θεωρήσουμε έναν α-ισοδύναμό του M', τότε ο M' δημιουργείται από τον M εφαρμόζοντας την περιοριστική α-ισοδυναμία, δηλαδή αντικαθιστώντας δεσμευμένες μεταβλητές μόνο με σύμβολα μεταβλητών που αντιστοιχούν στον ίδιο τύπο. Όλες οι ιδιότητες του λ-λογισμού παραμένουν σε ισχύ με βάση αυτήν την παρατήρηση.

Το αποτέλεσμα της διαμέρισης $V = \cup_{\sigma \in T} V_\sigma$ είναι ότι ο όρος $|M|$ «θυμάται» την απονομή τύπων στις μεταβλητές του. Υπάρχει πάντα μία συνάρτηση $\mathcal{T} : V \to T$ που ορίζεται ως

$$\mathcal{T}(x) = \text{ο μοναδικός } \sigma \text{ ώστε } x \in V_\sigma$$

Ορισμός 2.8 *Αν M όρος, ορίζουμε τον τυποποιημένο $\mathcal{C}(M)$ ως εξής:*

$$\begin{aligned}\mathcal{C}(x) &= x^{\mathcal{T}(x)}\\ \mathcal{C}(M\,N) &= \mathcal{C}(M)\,\mathcal{C}(N)\\ \mathcal{C}(\lambda x.\,M) &= \lambda x^{\mathcal{T}(x)}.\,\mathcal{C}(M)\end{aligned}$$

Ο $\mathcal{C}(M)$ προκύπτει αν σε κάθε μεταβλητή x του M (ελεύθερη ή δεσμευμένη) προσθέσουμε τον αντίστοιχο τύπο σ (αν $x \in V_\sigma$). Για τυχόντα M ο $\mathcal{C}(M)$ δεν είναι όρος Church. Εύκολα βλέπουμε ότι, αν M και N είναι α-ισοδύναμοι με την περιοριστική έννοια που αναφέρθηκε πιο πάνω, τότε $\mathcal{C}(M)$ και $\mathcal{C}(N)$ είναι α-ισοδύναμοι ως όροι Church.

Πρόταση 2.4 *Αν M είναι όρος Church, τότε $\mathcal{C}(|M|) = M$.*

Απόδειξη: Επαγωγή στον M.

Πρόταση 2.5 *Αν M και N και L είναι όροι Church, τότε*

1. $|M[x^\sigma := N]| = |M|[x := |N|]$
2. $M \to_\beta N$ *συνεπάγεται* $|M| \to_\beta |N|$
3. *αν* $|M| \to_\beta L$ *τότε* $M \to_\beta \mathcal{C}(L)$ *και* $\mathcal{C}(L)$ *είναι όρος Church*
4. *αν* $|M| \twoheadrightarrow_\beta L$ *τότε* $M \twoheadrightarrow_\beta \mathcal{C}(L)$

Απόδειξη: (1). Επαγωγή στον M.

$$\begin{array}{lll} M \equiv x^\sigma & \to & |M[x^\sigma := N]| = |N| = x[x := |N|] = |M|[x := |N|] \\ M \equiv y^\tau (x^\sigma \not\equiv y^\tau) & \to & |M[x^\sigma := N]| = |y^\tau| = y = y[x := |N|] \\ M \equiv \lambda x^\sigma.\, M_1 & \to & |M[x^\sigma := N]| = |\lambda x^\sigma.\, M_1| = |M| = \lambda x.\, |M_1| = \lambda x.\, |M_1|[x := |N|] \\ M \equiv \lambda y^\tau.\, M_1 & \to & |M[x^\sigma := N]| = |\lambda y^\tau.\, M_1[x^\sigma := N]| = \lambda y.\, |M_1[x^\sigma := N]| = \\ & & \lambda y.\, (|M_1|[x := |N|]) = \lambda y.\, |M_1|[x := |N|] = |M|[x := |N|] \end{array}$$

(3). Η κυριότερη περίπτωση είναι όταν $|M| \equiv |(\lambda x^\sigma . P)\, Q|$.
Τότε $|M| = (\lambda x. |P|)\, |Q| \to_\beta |P|[x := |Q|] \equiv |P[x^\sigma := Q]|$ άρα $|M| \to_\beta |P[x^\sigma := Q]|$ οπότε $M \to_\beta P[x^\sigma := Q] = \mathcal{C}(L)$, όπου $L \equiv |P|[x := |Q|]$.

Πρόταση 2.6 *Η ιδιότητα Church–Rosser ικανοποιείται από τους όρους Church.*

Απόδειξη: Αν $M \twoheadrightarrow_\beta M_1$ και $M \twoheadrightarrow_\beta M_2$, τότε $|M| \twoheadrightarrow_\beta |M_1|$ και $|M| \twoheadrightarrow_\beta |M_1|$. Από Church–Rosser για λ-λογισμό, υπάρχει λ-όρος L ώστε $|M_1| \twoheadrightarrow_\beta L$ και $|M_2| \twoheadrightarrow_\beta L$ και κατά συνέπεια από παραπάνω πρόταση $M_1 \twoheadrightarrow_\beta \mathcal{C}(L)$ και $M_2 \twoheadrightarrow_\beta \mathcal{C}(L)$.

Πρόταση 2.7 *Ισχύουν οι παρακάτω προτάσεις:*

1. *Αν M είναι όρος Church τύπου σ και οι ελεύθερες μεταβλητές του $|M|$ είναι μεταξύ των $x_1, \ldots x_k$ και αν $\Gamma = \{x_1 : \mathcal{T}(x_1), \ldots x_k : \mathcal{T}(x_k)\}$, τότε $\Gamma \vdash |M| : \sigma$.*

2. *Αν M είναι λ-όρος και $\Gamma \vdash M : \sigma$ (όπου υποθέτουμε ότι αν $x : \tau \in \Gamma$ τότε $\mathcal{T}(x) = \tau$) τότε $\mathcal{C}(M)$ είναι όρος Church τύπου σ.*

[Η πρόταση αυτή παρουσιάζει την σχέση μεταξύ των όρων Church και την τυποποίηση τω λ-όρων στο σύστημα Curry.]

2.2.2 Σύστημα Church

Μπορούμε να διαφοροποιήσουμε το αρχικό σύστημα Church και να το παρουσιάσουμε με τον τρόπο με τον οποίο τυποποιούνται οι λ-όροι στο σύστημα Curry. Θα χρειαστούμε την έννοια του προόρου.

Ορισμός 2.9 *Έστω T το σύνολο των τύπων. Ορίζουμε ως προόρους τις εκφράσεις Λ_T που σχηματίζονται από τον ακόλουθο ορισμό:*

$$\Lambda_T ::= V \mid (\lambda x : T. \Lambda_T) \mid (\Lambda_T\, \Lambda_T)$$

Ορισμός 2.10 *Η σχέση τυποποίησης $\vdash^*$ ορίζεται από:*

$$\Gamma, x : \sigma \vdash^* x : \sigma$$

$$\frac{\Gamma, x : \sigma \vdash^* M : \tau}{\Gamma \vdash^* \lambda x : \sigma . M : \sigma \to \tau} \qquad \frac{\Gamma \vdash^* M : \sigma \to \tau \qquad \Gamma \vdash^* N : \sigma}{\Gamma \vdash^* M\, N : \tau}$$

Η σχέση $\Gamma \vdash^* M : \sigma$ τυποποιεί τον προόρο M με τύπο σ στο περιβάλλον Γ.

Η α-ισοδυναμία, η αντικατάσταση και η αναγωγή ορίζονται με προφανή τρόπο στους προόρους.

Εάν M είναι προόρος, τότε μπορούμε να ρυθμίσουμε τα σύμβολα μεταβλητών ώστε, αν $\lambda x : \sigma. \ldots$ εμφανίζεται στο M, τότε $\mathcal{T}(x) = \sigma$. Με αυτήν την προϋπόθεση μπορούμε, εάν έχουμε επίσης φροντίσει για το ακόλουθο:

$$x : \tau \in \Gamma \to \mathcal{T}(x) = \tau$$

να μετατρέψουμε κάθε $\Gamma \vdash^* M : \sigma$ σε έναν όρο Church $M^{\mathcal{C}}$ ως εξής:

> Κάθε εμφάνιση $\lambda x : \sigma$ στον M αντικαθίσταται με λx^σ.
> Κάθε άλλη εμφάνιση μεταβλητής x αντικαθίσταται από $x^{\mathcal{T}(x)}$.

Πρόταση 2.8 *Αν $\Gamma \vdash^* M : \sigma$ (κάτω από τις προϋποθέσεις μεταβλητών που αναπτύχθηκαν πιο πανω), τότε $M^{\mathcal{C}}$ είναι όρος Church.*

Το αντίστροφο ισχύει επίσης.

Πρόταση 2.9 *Αν M είναι όρος Church τύπου ρ και M^π είναι ο προόρος που αποκτάται από τον M αντικαθιστώντας κάθε εμφάνιση του λx^σ στον M με $\lambda x : \sigma$ και κάθε άλλη εμφάνιση μεταβλητής x^τ στον M με x και αν $x_1^{\sigma_1}, \ldots x_k^{\sigma_k}$ περιέχουν τις ελεύθερες μεταβλητές* *του M, θα έχουμε ότι:*

$$x_1 : \sigma_1, \ldots x_k : \sigma_k \vdash^* M : \rho$$

Για την τυποποίηση $\vdash^*$ ισχύουν τα παρακάτω:

Λήμμα 2.3 *Αν $\Gamma \vdash^* M : \sigma$, τότε:*

1. $\Gamma \subseteq \Gamma' \Rightarrow \Gamma' \vdash^* M : \sigma$
2. $\boldsymbol{FV}(M) \subseteq \mathrm{dom}(\Gamma)$
3. $\Gamma' \vdash^* M : \sigma$, *όπου* $\mathrm{dom}(\Gamma') = \boldsymbol{FV}(M)$ *και* $\Gamma' \subseteq \Gamma$

Λήμμα 2.4 (Δημιουργίας) *Ισχύουν τα ακόλουθα:*

1. $\Gamma \vdash^* x : \sigma \Rightarrow x : \sigma \in \Gamma$
2. $\Gamma \vdash^* M\,N : \sigma \Rightarrow \exists \tau$ *ώστε* $\Gamma \vdash^* M : \tau \to \sigma$ *και* $\Gamma \vdash^* N : \tau$
3. $\Gamma \vdash^* \lambda x : \tau.\, M : \sigma \Rightarrow \exists \rho$ *ώστε* $\sigma = \tau \to \rho$ *και* $\Gamma, x : \tau \vdash^* M : \rho$

Πρόταση 2.10 (Αντικατάσταση) *Ισχύουν τα ακόλουθα:*

1. $\Gamma \vdash^* M : \sigma \Rightarrow \Gamma[\alpha := \tau] \vdash^* M : \sigma[\alpha := \tau]$
2. $\Gamma, x : \tau \vdash^* M : \sigma$ *και* $\Gamma \vdash^* N : \tau \Rightarrow \Gamma \vdash^* M[x := N] : \sigma$

Πρόταση 2.11 (Subject reduction) *Αν $\Gamma \vdash^* M$ και $M \to_\beta N$ τότε $\Gamma \vdash^* N$.*

Πρόταση 2.12 (Church–Rosser) *Αν $\Gamma \vdash^* M : \sigma$ και $M \twoheadrightarrow_\beta M_1$ και $M \twoheadrightarrow_\beta M_2$, τότε υπάρχει L ώστε $M_1 \twoheadrightarrow_\beta L$ και $M_2 \twoheadrightarrow_\beta L$ και $\Gamma \vdash^* L : \sigma$.*

Πρόταση 2.13 (Μοναδικότητα τυποποίησης) *Ισχύουν τα ακόλουθα:*

1. $\Gamma \vdash^* M : \sigma$ *και* $\Gamma \vdash^* M : \tau \Rightarrow \sigma = \tau$

2. $\Gamma \vdash^* M : \sigma$ *και* $\Gamma \vdash^* N : \tau$ *και* $M \equiv_\beta N \Rightarrow \sigma = \tau$

Απόδειξη: (i). Επειδή όταν $\Gamma \vdash^* M : \sigma$ ο υπολογισμός του $M^{\mathcal{C}}$ γίνεται μόνο με βάση τα Γ και M, ο όρος $M^{\mathcal{C}}$ θα είναι κοινός και για τις δύο περιπτώσεις άρα θα έχει κοινό τύπο $\sigma = \tau$.
(ii). Από θεώρημα Church–Rosser.

Η σχέση των τυποποίησεων $\vdash^*$ και $\vdash$ θα είναι ανάλογη με αυτή μεταξύ των όρων Church M και των $\Gamma \vdash M : \sigma$.

Πρόταση 2.14 *Έστω* $M, N \in \Lambda_T$.

1. *Αν* $M \to_\beta N$, *τότε* $|M| \to_\beta |N|$.

2. $\Gamma \vdash^* M : \sigma \Rightarrow \Gamma \vdash |M| : \sigma$

Πρόταση 2.15 (Ύψωση) *Για όλα τα* $M, N \in \Lambda$ *(λ-όρους):*

1. $|M'| \to_\beta N \Rightarrow$ *υπάρχει* $N' \in \Lambda_T$ *με* $|N'| = N$ *ώστε* $M' \to_\beta N'$

2. *Αν* $\Gamma \vdash M : \sigma$, *τότε υπάρχει* $M' \in \Lambda_T$ *με* $|M'| = M$ *ώστε* $\Gamma \vdash^* M' : \sigma$.

2.3 Επεκτάσεις του λ-λογισμού με απλούς τύπους

Το σύστημα του λ-λογισμού με απλούς τύπους που μελετήσαμε, και το οποίο μας έδωσε τη δυνατότητα να αναπτύξουμε τη γενική μορφή των συστημάτων με τύπους, είναι αρκετά «φτωχό». Δεν μπορούμε λόγου χάριν να ορίσουμε το ζεύγος $\langle P, Q\rangle$ όταν μας δίνονται δύο όροι P και Q. Μια λοιπόν προφανής επέκταση θα είναι να προσθέσουμε στο μηχανισμό δημιουργίας των τύπων τη δυνατότητα δημιουργίας του γινομένου τύπων $\sigma \times \tau$, όταν σ και τ είναι τύποι. Αυτό θα μας επιτρέψει να ορίσουμε το ζεύγος $\langle P, Q\rangle$. Αργότερα θα μελετήσουμε επεκτάσεις που θα μας επιτρέπουν να αυξήσουμε αξιοσημείωτα την εκφραστική δυνατότητα του συστήματος.

Οι επεκτάσεις που θα μελετήσουμε θα είναι στο αρχικό σύστημα Church.

Επέκταση του αρχικού συστήματος Church με γινόμενο τύπων

Τύποι: Στον ορισμό των τύπων προσθέτουμε την ακόλουθη πρόταση.

- Αν σ και τ είναι τύποι τότε $\sigma \times \tau$ είναι τύπος.

Σημείωση: Ο τύπος $\sigma \times \tau$ είναι το (καρτεσιανό) γινόμενο των τύπων σ και τ.

Οροι: Στον ορισμό των όρων προσθέτουμε τα ακόλουθα.

- Αν M είναι όρος τύπου σ και N όρος τύπου τ τότε $\langle M, N\rangle$ είναι όρος τύπου $\sigma \times \tau$. (Δημιουργία ζεύγους)

- Αν M είναι όρος τύπου $\sigma \times \tau$ τότε $\pi^1 M$ είναι όρος τύπου σ και $\pi^2 M$ είναι όρος τύπου τ.

Σημείωση: Ο όρος $\pi^1 M$ είναι η «πρώτη προβολή» του M και ο $\pi^2 M$ η «δεύτερη προβολή».

Υπολογιστική σημασία

Οι καινούργιοι ορισμοί εισάγουν νέες μορφές από redex και contractum. Στα ήδη υπάρχοντα προστίθενται τα εξής:

$$\pi^1\langle M, N\rangle \to_\beta M$$

$$\pi^2\langle M, N\rangle \to_\beta N$$

Οι δύο προαναφερθείσες σχέσεις που έχουν τη μορφή $P \to_\beta Q$ σημαίνουν ότι P είναι ένα redex και Q είναι το contractum του.

Με προφανή τρόπο, ακριβώς όπως στην περίπτωση των απλών τύπων (και του καθαρού λ-λογισμού) μπορούμε να επεκτείνουμε τη σχέση $\to_\beta$ σε $\twoheadrightarrow_\beta$ καθώς και να ορίσουμε τη σχέση $=_\beta$. Παραμένουν οι ιδιότητες Church-Rosser καθώς και η ιδιότητα της ισχυρής κανονικοποίησης.

Κεφάλαιο 3

Λογική και ο ισομορφισμός Curry-Howard

Στη Λογική κατασκευάζουμε αποδείξεις. Ξεκινώντας από υποθέσεις, με διαδοχικά (λογικά) βήματα οδηγούμαστε στο συμπέρασμα. Αν οι υποθέσεις ταυτίζονται με τα αξιώματα μιας θεωρίας τότε το συμπέρασμα θα είναι ένα θεώρημα αυτής της θεωρίας. Αν το συμπέρασμα αποδειχθεί χωρίς να βασιζόμαστε σε καμμία υπόθεση τότε η πρόταση-συμπέρασμα είναι λογικά ορθή δηλαδή έχει μια γενική λογική αναγκαιότητα (ταυτολογία ή λογικά έγκυρη πρόταση). Οι μελέτες μεγάλων μαθηματικών λογικών, όπως οι Frege, Russell, Hilbert, Gentzen και πολλοί άλλοι, επέτρεψαν την τυποποίηση της έννοιας της απόδειξης. Οι εργασίες του Gentzen και ειδικά ο τρόπος που παρουσίασε τις αποδείξεις στο σύστημα της φυσικής απαγωγής επέτρεψαν να διαπιστωθεί μια συγκλονιστική ισομορφία μεταξύ των αποδείξεων και των όρων του λ-λογισμού (προγραμμάτων). Αυτή η αντιστοιχία αποτελεί το κλειδί της δομικής σύνδεσης της λογικής (εν γένει των μαθηματικών) και της πληροφορικής.

Στη συνέχεια θα παρουσιάσουμε το σύστημα της φυσικής απαγωγής στην απλή περίπτωση ενός μέρους του προτασιακού λογισμού.

Ορισμός 3.1 (Προτασιακές φόρμουλες) *Ξεκινάμε με ένα αριθμήσιμο σύνολο προτασιακών μεταβλητών*

π.χ. $A, B, C, \ldots, A_1, B_1, C_1, \ldots$ *θα είναι προτασιακές μςταβλητές*

και ορίζουμε

1. *Κάθε προτασιακή μεταβλητή είναι προτασιακή φόρμουλα.*

2. *Αν* ϕ *και* ψ *είναι προτασιακές φόρμουλες τότε* $(\phi \to \psi)$ *και* $(\phi \wedge \psi)$ *είναι προτασιακές φόρμουλες.*

Σημείωση: Προτασιακή φόρμουλα είναι κάθε έκφραση (συμβολοσειρά) που κατασκευάζεται με διαδοχικές εφαρμογές των κανόνων 1) και 2).

Η φόρμουλα $(\phi \to \psi)$ είναι η συνεπαγωγή με υπόθεση τη ϕ και συμπέρασμα την ψ και η φόρμουλα $(\phi \wedge \psi)$ είναι η σύζευξη των ϕ και ψ. Για λόγους απλότητας θα παραλείπουμε πολλές φορές τις παρενθέσεις.

Παράδειγμα:

1. Η προτασιακή μεταβλητή A είναι προτασιακή φόρμουλα.

2. Η έκφραση $(((A \to A) \to C) \wedge B)$ είναι προτασιακή φόρμουλα (ελέγξτε αν έχει κατασκευαστεί σωστά σύμφωνα με τις προδιαγραφές του ορισμού).

3.1 Σύστημα αποδείξεων φυσικής απαγωγής

Οι αποδείξεις στο σύστημα φυσικής απαγωγής θα είναι δέντρα όπου στους κόμβους των δέντρων θα υπάρχουν προτασιακές φόρμουλες, στη ρίζα των δέντρων θα υπάρχει η προτασιακή φόρμουλα που αποδεικνύεται και στα φύλλα των δέντρων θα υπάρχουν (αν παραμένουν ζωντανές) οι υποθέσεις στις οποίες βασίζεται η αποδεικνυόμενη φόρμουλα. Οι υποθέσεις στα φύλλα του δέντρου θα είναι ομαδοποιημένες σε πακέτα υποθέσεων (όπου κάθε πακέτο θα αποτελείται από εμφανίσεις της ίδιας φόρμουλας σε διαφορετικά φύλλα). Επίσης θα υπάρχουν και πακέτα υποθέσεων που έχουν εκφορτιστεί (κατά την πορεία της απόδειξης) και τα οποία δεν θα μετράνε ως (ζωντανές) αποδείξεις.

Τα παραπάνω γίνονται πιο ακριβή και πιο κατανοητά με τους ακόλουθους ορισμούς.

Ορισμός 3.2 *Θα ονομάζουμε* δέντρο με φόρμουλες *κάθε δέντρο, με μονή ή διπλή διακλάδωση, στους κόμβους του οποίου υπάρχουν προτασιακές φόρμουλες π.χ.*

$$\frac{\dfrac{A \qquad B}{A \wedge B}}{A \rightarrow (A \wedge B)}$$ *είναι δέντρο με φόρμουλες.*

Τα δέντρα που εξετάζουμε διακλαδώνονται προς τα πάνω π.χ. όταν γράφουμε $\dfrac{\phi \qquad \psi}{\chi}$ έχουμε διπλή διακλάδωση, ενώ όταν γράφουμε $\dfrac{\phi}{\chi}$ έχουμε μονή διακλάδωση.

Ορισμός 3.3 *Ένα* δέντρο με φόρμουλες και με πακέτα υποθέσεων *είναι ένα δέντρο με φόρμουλες όπου στα φύλλα του δέντρου σε κάθε φόρμουλα έχει αντιστοιχηθεί ένας φυσικός αριθμός. Ο περιορισμός είναι ότι σε διαφορετικές φόρμουλες πρέπει να αντιστοιχούν διαφορετικοί αριθμοί ενώ σε διαφορετικές εμφανίσεις της ίδιας φόρμουλας (ίδια φόρμουλα σε διαφορετικά φύλλα) μπορεί να αντιστοιχηθεί ο ίδιος αριθμός. Το πολυσύνολο όλων των εμφανίσεων στα φύλλα του δέντρου μιας φόρμουλας ϕ στην οποία έχει αντιστοιχηθεί ο αριθμός i λέγεται* πακέτο υποθέσεων i. *Τα πακέτα υποθέσεων χωρίζο-*

νται σε δύο ξεχωριστές κατηγορίες. Τα ζωντανά πακέτα υποθέσεων και τα εκφορτισμένα πακέτα υποθέσεων. Όταν θέλουμε να παρουσιάσουμε ότι μια συγκεκριμένη εμφάνιση μιας φόρμουλας ϕ σε ένα φύλλο ανήκει στο ζωντανό πακέτο i γράφουμε ϕ^i ενώ όταν ανήκει στο εκφορτισμένο πακέτο i γράφουμε $\overline{\phi}^{\,i}$. Επίσης, στα δέντρα με φόρμουλες και πακέτα υποθέσεων, επιτρέπουμε να υπάρχουν φυσικοί αριθμοί και στις διακλαδώσεις $\dfrac{\phi \quad \psi}{\chi}$ και $\dfrac{\phi}{\chi}$ δηλαδή επιτρέπουμε το δέντρο να έχει στους κόμβους τη μορφή

$\dfrac{\phi \quad \psi}{\chi}\,i$ *ή* $\dfrac{\phi}{\chi}\,i$.

Παράδειγμα:

$$\cfrac{\cfrac{\cfrac{\overline{A}^{\,1} \quad \overline{A}^{\,1}}{A \wedge A}}{A \to (A \wedge A)}\,1 \qquad A^2}{(A \to (A \wedge B)) \wedge A}$$

είναι δέντρο με φόρμουλες και πακέτα υποθέσεων. Ας επισημάνουμε ότι το πολυσύνολο με μοναδική εμφάνιση την A^2 στην αναπαράσταση του δέντρου είναι το ανοικτό πακέτο υποθέσεων 2 ενώ το πολυσύνολο με τις δύο εμφανίσεις $\overline{A}^{\,1}$ στην αναπαράσταση του δέντρου είναι το εκφορτισμένο πακέτο υποθέσεων 1.

Θα συμβολίζουμε τα ανοικτά πακέτα υποθέσεων i με μέλη μια φόρμουλα ϕ με $[\phi]_i$. Δηλαδή $[\phi]_i$ θα συγκεντρώνει όλες τις φόρμουλες ϕ στα φύλλα του δέντρου στις οποίες έχει αντιστοιχηθεί ο αριθμός i (και οι οποίες συγκροτούν ανοικτό πακέτο). Αντίστοιχα τα εκφορτισμένα πακέτα τα συμβολίζουμε με $\overline{[\phi]}_i$. Σημειώστε ότι $[\phi]_i$ είναι διαφορετικό από το $[\phi]_j$ αν $i \neq j$. Το ίδιο συμβαίνει και για τα εκφορτισμένα πακέτα. Ενα πακέτο υποθέσεων είναι πάντα προσδιορισμένο είτε ως ανοικτό είτε ως εκφορτισμένο πακέτο υποθέσεων. Αν αποφασίσουμε για ένα ανοικτό πακέτο υποθέσεων $[\phi]_i$ να αλλάξουμε τον προσδιορισμό του σε εκφορτισμένο τότε το συμβολίζουμε (το μετατρέπουμε σε) $\overline{[\phi]}_i$.

Στη συνέχεια θα ορίσουμε την «Π είναι απόδειξη της φόρμουλας ϕ από τα πακέτα υποθέσεων $[\phi_1]_{j_1}, \ldots, [\phi_k]_{j_k}$». Η απόδειξη Π θα είναι ένα δέντρο με φόρμουλες και πακέτα υποθέσεων στο οποίο τα ανοικτά πακέτα υποθέσεων θα είναι τα $[\phi_1]_{j_1}, \ldots, [\phi_k]_{j_k}$ και για τα εκφορτισμένα θα υπάρχει μια καταγραφή του «σε πιο σημείο» της απόδειξης έχει γίνει η εκφόρτισή τους. Η απόδειξη-δέντρο κατασκευάζεται με βάση τον ακόλουθο επαγωγικό ορισμό.

Ορισμός 3.4 *1. Για κάθε φόρμουλα ϕ και κάθε $i \in \mathbb{N}$ το δέντρο*

$$\phi$$

με μοναδικό κόμβο την ϕ είναι απόδειξη της ϕ από το πακέτο υποθέσεων $[\phi]_i$. Σ' αυτήν την περίπτωση το (ζωντανό) πακέτο υποθέσεων $[\phi]_i$ (πακέτο i) αποτελείται αποκλειστικά από τη ϕ και η απόδειξη μπορεί να παρασταθεί επίσης με ϕ^i.

2. Αν Π_1 είναι απόδειξη της ϕ και Π_2 απόδειξη της ψ (και στις δύο περιπτώσεις αντίστοιχα από κάποια πακέτα υποθέσεων έτσι ώστε να μην είναι δυνατόν για πακέτο υποθέσεων $[\phi]_i$ της Π_1 και $[\psi]_i$ της Π_2 να έχουμε $\phi \neq \psi$) τότε το δέντρο

$$\frac{\Pi_1 \qquad \Pi_2}{\phi \wedge \psi}$$

είναι απόδειξη της $\phi \wedge \psi$ από πακέτα υποθέσεων που καθορίζονται από τους αριθμούς που έχουν αποδοθεί στα φύλλα του ενιαίου δέντρου $\dfrac{\Pi_1 \qquad \Pi_2}{\phi \wedge \psi}$ και οι οποίοι έχουν κληρονομηθεί από τα δέντρα Π_1 και Π_2 (δηλαδή κάθε πακέτο υποθέσεων

$[\phi]_i$ *του* $\dfrac{\Pi_1 \qquad \Pi_2}{\phi \wedge \psi}$ *είναι πακέτο υποθέσεων είτε του* Π_1 *είτε του* Π_2*, εκτός από την περίπτωση που έχουμε για κάποιο* i *να υπάρχει πακέτο* $[\phi]_i$ *της* Π_1 *και* $[\phi]_i$ *της* Π_2 *και στην οποία περίπτωση ενοποιούμε το πακέτο* $[\phi]_i$*, δηλαδή σ' αυτό το πακέτο θα περιλαμβάνονται όλες οι εμφανίσεις της* ϕ^i *και στα δύο δέντρα* Π_1 *και* Π_2*.*

[Σχηματικά το σχηματισμό της νέας απόδειξης θα τον εμφανίζουμε ως

$\dfrac{\begin{array}{c}\vdots\\ \phi\end{array} \quad \begin{array}{c}\vdots\\ \psi\end{array}}{\phi \wedge \psi}$ *όπου* $\begin{array}{c}\vdots\\ \phi\end{array}$ *είναι η απόδειξη* Π_1 *και* $\begin{array}{c}\vdots\\ \psi\end{array}$ *η απόδειξη* Π_2*.]*

3. *Αν* Π *είναι απόδειξη της* $\phi \wedge \psi$ *από κάποια πακέτα υποθέσεων τότε* $\dfrac{\Pi}{\phi}$ *είναι απόδειξη της* ϕ *και* $\dfrac{\Pi}{\psi}$ *είναι απόδειξη της* ψ*, και οι δύο με τα ίδια πακέτα υποθέσεων.*

   [Παριστάνουμε αυτές τις αποδείξεις αντίστοιχα με $\dfrac{\begin{array}{c}\vdots\\ \phi \wedge \psi\end{array}}{\phi}$

   και $\dfrac{\begin{array}{c}\vdots\\ \phi \wedge \psi\end{array}}{\psi}$ *.]*

4. *Αν* Π *είναι απόδειξη της* ψ *από πακέτα υποθέσεων στα οποία περιλαμβάνεται το πακέτο* $[\phi]_i$ *τότε* $\dfrac{\Pi}{\phi \to \psi}\, i$ *είναι απόδειξη της* $\phi \to \psi$ *από τα ίδια πακέτα υποθέσεων εκτός του ότι το πακέτο* $[\phi]_i$ *έχει μεταταχθεί στα εκφορτισμένα, δηλαδή το* $[\phi]_i$ *έχει πάψει να είναι ανοικτό πακέτο (άρα είναι εκφορτισμένο).*

   [Σχηματικά μπορούμε να περιγράψουμε τα πιο πάνω λέγοντας ότι αν $\begin{array}{c}[\phi]_i\\ \vdots\\ \psi\end{array}$ *είναι απόδειξη της* ψ *τότε* $\dfrac{\begin{array}{c}\overline{[\phi]}_i\\ \vdots\\ \psi\end{array}}{\phi \to \psi}\, i$ *είναι απόδειξη*

της $\phi \to \psi$.*]*

5. *Αν* Π *είναι απόδειξη της* ψ *από κάποια πακέτα υποθέσεων και* ϕ *μια φόρμουλα τότε το δέντρο* $\dfrac{\Pi}{\phi \to \psi}$ *είναι απόδειξη της* $\phi \to \psi$ *από τα ίδια πακέτα υποθέσεων.*

   [Ο μηχανισμός αυτός αντιστοιχεί κατά μία έννοια στην εκφόρτιση ενός «φαινομενικού» πακέτου υποθέσεων $[\phi]_i$, *όπου το* i *δεν υπάρχει στα πακέτα υποθέσεων της απόδειξης* Π.*]*

6. *Με τη συμβολική αναπαράσταση και τις ίδιες προδιαγραφές του ορισμού που χρησιμοποιήσαμε για τη σύζευξη το δέντρο* $\dfrac{\begin{matrix}\vdots \\ \phi \to \psi\end{matrix} \qquad \begin{matrix}\vdots \\ \phi\end{matrix}}{\psi}$ *είναι απόδειξη της* ψ *στην περίπτωση που* $\begin{matrix}\vdots \\ \phi \to \psi\end{matrix}$ *είναι απόδειξη της* $\phi \to \psi$ *και* $\begin{matrix}\vdots \\ \phi\end{matrix}$ *είναι απόδειξη της* ϕ.

Παρατηρήσεις-Συμβολισμοί:

Η δημιουργία της απόδειξης Π της φόρμουλας ϕ δημιουργεί ένα δέντρο στο οποίο κρατούνται σημειώσεις για τις υποθέσεις (ζωντανές ή εκφορτισμένες) και της ακριβούς θέσης που εκφιρτίζεται ένα πακέτο υποθέσεων.

Αν με $\begin{matrix}\Pi \\ \psi\end{matrix}$ συμβολίσουμε την απόδειξη Π της φόρμουλας ψ και με $\begin{matrix}[\phi]_i \\ \Pi \\ \psi\end{matrix}$ την απόδειξη Π της ψ όπου μεταξύ των πακέτων υποθέσεων υπάρχει το $[\phi]_i$, ομοίως δε με $\begin{matrix}\overline{[\phi]}_i \\ \Pi \\ \psi\end{matrix}$ την απόδειξη της ψ όπου το πακέτο $[\phi]_i$ έχει «καταστεί» εκφορτισμένο (έχει εκφορτιστεί) τότε μπορούμε να διατυπώσουμε συνοπτικά τον ορισμό των αποδείξεων:

π.χ. η $\begin{matrix}[\psi]_i \\ \psi \\ \psi\end{matrix}$ είναι απόδειξη, η $\dfrac{\begin{matrix}\Pi_1 \\ \phi\end{matrix} \qquad \begin{matrix}\Pi_2 \\ \psi\end{matrix}}{\phi \wedge \psi}$ είναι απόδειξη (αφού έχουμε ενοποιήσει τα πακέτα υποθέσεων των $\begin{array}{c}\Pi_1\\ \phi\end{array}$ και $\begin{array}{c}\Pi_2\\ \psi\end{array}$) η $\dfrac{\begin{array}{c}\overline{[\phi]}_i\\ \Pi\\ \psi\end{array}}{\phi \to \psi}\,\mathrm{i}$ είναι απόδειξη κ.ο.κ.

Παράδειγμα 3.1 1. $\dfrac{\overline{\ \mathrm{A}\ }^{\,1}}{A \to A}\,1$. Δηλαδή το A είναι απόδειξη από την υπόθεση A (δηλ. το πακέτο $[A]_1$). Άρα μπορούμε να εκφορτίσουμε το πακέτο A^1 και να πάρουμε το $A \to A$ χωρίς υποθέσεις.

2. $\dfrac{\dfrac{\overline{\ \mathrm{A}\ }^{\,1}}{B \to A}}{A \to (B \to A)}\,1$. (Η εισαγωγή του B αντιστοιχεί στην περίπτωση 5 του ορισμού. Δηλαδή το $B \to A$ εισάγεται στην πορεία της απόδειξης χωρίς το B να περιέχεται στα ανοικτά πακέτα υποθέσεων).

3. $\dfrac{\dfrac{\dfrac{\overline{\ \mathrm{A}\ }^{\,2} \quad \overline{\ \mathrm{B}\ }^{\,1}}{A \wedge B}}{(B \to (A \wedge B))}\,1}{A \to (B \to (A \wedge B))}\,2$ είναι απόδειξη του $A \to (B \to (A \wedge B))$ χωρίς υποθέσεις.

Σημειώστε ότι όλες οι υποαποδείξεις

A^2, B^1, $\dfrac{A^2 \qquad B^1}{A \wedge B}$, $\dfrac{\dfrac{A^2 \quad \overline{\ B\ }^{\,1}}{A \wedge B}}{B \to (A \wedge B)}\,1$, είναι αποδείξεις των αντίστοιχων φορμουλών από τα αντίστοιχα πακέτα υποθέσεων.

■

Ως ένα άλλο παράδειγμα απόδειξης θεωρήστε το ακόλουθο δέντρο

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \to (B \to C)}^{\,1} \quad \overline{A}^{\,2}}{B \to C} \quad \dfrac{\overline{A \to B}^{\,3} \quad \overline{A}^{\,2}}{B}}{C}}{A \to C}\,2}{(A \to B) \to (A \to C)}\,3}{(A \to (B \to C)) \to ((A \to B) \to (A \to C))}\,1$$

ΚΑΝΟΝΕΣ ΣΧΗΜΑΤΙΣΜΟΥ ΤΩΝ ΑΠΟΔΕΙΞΕΩΝ

Οι κανόνες μπορούν να χωριστούν σε δύο κατηγορίες. Τους κανόνες *εισαγωγής* και του κανόνες *απαλοιφής*.

- Κανόνες εισαγωγής:

  Οι κανόνες $\dfrac{\begin{array}{c}\vdots\\ \phi\end{array} \qquad \begin{array}{c}\vdots\\ \psi\end{array}}{\phi \wedge \psi}$ και $\dfrac{\begin{array}{c}\overline{[\phi]}_i\\ \vdots\\ \psi\end{array}}{\phi \to \psi}\,\mathrm{i}$.

- Κανόνες απαλοιφής:

  Οι κανόνες $\dfrac{\begin{array}{c}\vdots\\ \phi \wedge \psi\end{array}}{\phi}$, $\dfrac{\begin{array}{c}\vdots\\ \phi \wedge \psi\end{array}}{\psi}$ και $\dfrac{\begin{array}{c}\vdots\\ \phi \to \psi\end{array} \qquad \begin{array}{c}\vdots\\ \phi\end{array}}{\psi}$.

Οι κανόνες εισαγωγής εισάγουν τον σύνδεσμο στην φόρμουλα του συμπεράσματός τους ενώ οι κανόνες απαλοιφής τον απομακρύνουν.

3.1.1 Redex και Contractum στις αποδείξεις φυσικής απαγωγής

Η παρουσίαση των αποδείξεων με το σύστημα της φυσικής απαγωγής εισάγει μια έννοια redex και την αντίστοιχη του contractum.

Ορισμός 3.5 *Κάθε απόδειξη της μορφής στο αριστερό μέρος είναι redex και η αντίστοιχη μορφή στο δεξιό μέρος είναι το contractum αυτού του redex.*

Redex	Contractum
$\dfrac{\dfrac{\begin{matrix}\overline{[\phi]}_i\\ \Pi\\ \psi\end{matrix}}{\phi\rightarrow\psi}\,i \qquad \begin{matrix}\Pi_2\\ \phi\end{matrix}}{\psi}$	$\begin{matrix}\Pi_2\\ [\phi]_i\\ \Pi\\ \psi\end{matrix}$
$\dfrac{\dfrac{\begin{matrix}\Pi_1\\ \phi\end{matrix} \qquad \begin{matrix}\Pi_2\\ \psi\end{matrix}}{\phi\wedge\psi}}{\phi}$	$\begin{matrix}\Pi_1\\ \phi\end{matrix}$
$\dfrac{\dfrac{\begin{matrix}\Pi_1\\ \phi\end{matrix} \qquad \begin{matrix}\Pi_2\\ \psi\end{matrix}}{\phi\wedge\psi}}{\psi}$	$\begin{matrix}\Pi_2\\ \psi\end{matrix}$

Σημείωση: Για να σχηματιστεί η απόδειξη $\begin{matrix}\Pi_2\\ [\phi]_i\\ \Pi\\ \psi\end{matrix}$ *κάθε φύλλο* ϕ *στην απόδειξη* $\begin{matrix}[\phi]_i\\ \Pi\\ \psi\end{matrix}$ *που ανήκει στο πακέτο υποθέσεων i έχει αντικατασταθεί με την απόδειξη* $\begin{matrix}\Pi_2\\ \phi\end{matrix}$. *Είναι εύκολο να δούμε ότι αυτό που προκύπτει είναι απόδειξη.*

Παρατήρηση: Το redex δημιουργείται όταν έχουμε την εφαρμογή ενός κανόνα εισαγωγής και αμέσως μετά την εφαρμογή ενός κανόνα απαλοιφής (και στις δύο περιπτώσεις για τον ίδιο σύνδεσμο). Κατά μία έννοια μια τέτοια ακολουθία είναι μια άσκοπη εναλλαγή αποδείξεων (detour) η οποία δημιουργεί απόδειξη κατά ένα έμμεσο τρόπο. Η αποκατάσταση έρχεται όταν η απόδειξη αυτή (το redex) αντικατασταθεί με την ευθεία απόδειξη (που είναι το contractum).

Ορισμός 3.6 *Μια απόδειξη που δεν περιέχει redex λέγεται κανονική απόδειξη.*

Θεώρημα 3.1 *Αν υπάρχει απόδειξη μιας φόρμουλας τότε υπάρχει και κανονική απόδειξη της ίδιας φόρμουλας. Μάλιστα, όπως θα* *δούμε και από τον ισομορφισμό του Curry-Howard, ισχύει το ισχυρότερο αποτέλεσμα ότι κάθε απόδειξη μιας φόρμουλας ϕ μετατρέπεται σε κανονική απόδειξη της ϕ με οποιαδήποτε διαδοχική αντικατάσταση ενός redex με το αντίστοιχο contractum (ισχυρή κανονικοποίηση).*

3.1.2 Ισομορφισμός Curry-Howard

Πρόκειται για μια αντιστοιχία μεταξύ των αποδείξεων και των λ-όρων με τύπους η οποία σέβεται την αναγωγή, δηλαδή την μετάβαση από redex σε contractum. Το γενικό σχήμα είναι ότι κάθε απόδειξη μιας φόρμουλας ϕ αντιστοιχεί σε ένα όρο τύπου ϕ (υπάρχει ταύτιση φορμουλών και τύπων). Και αν θεωρήσουμε ότι οι όροι τύπου σ είναι προγράμματα τύπου σ ο ισομορφισμός μπορεί σχηματικά να διατυπωθεί

$$\text{ΑΠΟΔΕΙΞΕΙΣ} \longleftarrow \text{———} \longrightarrow \text{ΠΡΟΓΡΑΜΜΑΤΑ}$$

$$\text{ΦΟΡΜΟΥΛΕΣ} \longleftarrow\text{—————} \longrightarrow \text{ΤΥΠΟΙ}$$

Δηλαδή κάθε απόδειξη μιας φόρμουλας μπορεί να νοηθεί ως ένα πρόγραμμα ενός τύπου. Η φόρμουλα περιγράφει το τι αποδεικνύει η απόδειξη ενώ ο τύπος περιγράφει το τι κάνει το πρόγραμμα (το specification του προγράμματος).

Στη συνέχεια δίνεται η περιγραφή του ισομορφισμού.

Ορισμός 3.7 *Αν ταυτίσουμε τους ατομικούς τύπους και τις προτασιακές μεταβλητές και στην συνέχεια κάθε φόρμουλα $(\phi \to \psi)$ την ταυτίσουμε με τον τύπο $(\phi \to \psi)$ και κάθε φόρμουλα $(\phi \wedge \psi)$ με τον τύπο $(\phi \times \psi)$ μπορούμε να θεωρήσουμε ότι οι φόρμουλες και οι τύποι ταυτίζονται.*

Για παράδειγμα η προτασιακή φόρμουλα $(A \to B) \wedge (C \to A)$ είναι ο τύπος $(A \to B) \times (C \to A)$ όπου A, B, C είναι προτασιακές μεταβλητές (ή ατομικοί τύποι).

Θα χρησιμοποιούμε τα γράμματα A, B, C για τις προτασιακές μεταβλητές (το ίδιο για τους ατομικούς τύπους) και τα ϕ, ψ,... για τις προτασιακές φόρμουλες (ή το ίδιο για τους τύπους του συστήματος Church).

Ορισμός 3.8 *Σε κάθε απόδειξη* Π *της φόρμουλας* ϕ *από τα πακέτα υποθέσεων* $[\phi_1]_{i_1}, \ldots, [\phi_k]_{i_k}$ *θα αντιστοιχήσουμε με μοναδικό τρόπο έναν όρο* N *τύπου* ϕ *(δηλ.* N^ϕ*) με ελεύθερες μεταβλητές* $x_{i_1}^{\phi_1}, \ldots, x_{i_k}^{\phi_k}$ *του αρχικού συστήματος Church με γινόμενο τύπων, ως εξής:*

(ο ορισμός θα δίνει και την αντίστροφη αντιστοιχία δηλαδή για κάθε όρο N *μια απόδειξη του συστήματος Church. Για να έχουμε την ακριβή αντιστοιχία θα υποθέσουμε ότι αν* x_i^σ *και* x_j^τ *είναι μεταβλητές του συστήματος με τύπους και αν* $\sigma \neq \tau$ *τότε και οι δείκτες* i *και* j *θα είναι διαφορετικοί, δηλαδή* $i \neq j$*. Εδώ π.χ. το* i *είναι ο δείκτης σε μια αρίθμηση των συμβόλων μεταβλητών του αρχικού συστήματος Church.*

1. *Σε κάθε απόδειξη* ϕ^i *(από το πακέτο υποθέσεων* $[\phi]_i$*) αντιστοιχούμε τη μεταβλητή* x_i^ϕ *(και αντιστρόφως).*

2. *Αν* $\overset{\Pi_1}{\phi}$ *και* $\overset{\Pi_2}{\psi}$ *αντιστοιχούν στα* N^ϕ *και* M^ψ *τότε η απόδειξη* $\dfrac{\overset{\Pi_1}{\phi} \quad \overset{\Pi_2}{\psi}}{\phi \wedge \psi}$ *αντιστοιχεί στον όρο* $\langle N^\phi, M^\psi \rangle$ *(τύπου* $\phi \wedge \psi$*).*

3. *Αν η* $\overset{\Pi}{\phi \wedge \psi}$ *αντιστοιχεί στον* $N^{\phi \wedge \psi}$ *τότε η απόδειξη* $\dfrac{\overset{\Pi}{\phi \wedge \psi}}{\phi}$ *αντιστοιχεί στον* $\pi^1 M$ *και η* $\dfrac{\overset{\Pi}{\phi \wedge \psi}}{\psi}$ *αντιστοιχεί στον* $\pi^2 M$*.*

4. *Αν* $\begin{matrix}[\phi]_i\\ \Pi\\ \psi\end{matrix}$ *αντιστοιχεί στον όρο* M^ψ *τότε η απόδειξη* $\dfrac{\begin{matrix}\overline{[\phi]}_i\\ \Pi\\ \psi\end{matrix}}{\phi \to \psi}\,i$ *αντιστοιχεί στον όρο* $\lambda x_i^\phi M^\psi$.

5. *Αν* $\begin{matrix}\Pi\\ \psi\end{matrix}$ *αντιστοιχεί στον όρο* M^ψ *τότε* $\dfrac{\begin{matrix}\Pi\\ \psi\end{matrix}}{\phi \to \psi}$ *αντιστοιχεί στον όρο* $\lambda x^\phi M^\psi$ *τύπου* $(\phi \to \psi)$, *(όπου* x *μπορεί να είναι το πρώτο νέο σύμβολο μεταβλητής). Εδώ στην απόδειξη δεν εκφορτίζουμε κανένα πακέτο υποθέσεων και αντίστοιχα στον όρο χρησιμοποιούμε τη μεταβλητή* x^ϕ *που δεν εμφανίζεται ελεύθερη στον* M^ψ.

Η αντιστοιχία που ορίσαμε είναι ισομορφισμός διότι σέβεται την «πράξη» της αναγωγής, δηλαδή αν μία απόδειξη Q προκύψει από την P με την αναγωγή ενός redex τότε ο αντίστοιχος της Q όρος N προκύπτει από τον αντίστοιχο της P όρο M με την αναγωγή του αντίστοιχου redex. Θα παρουσιάσουμε την ισοδυναμία σε μία χαρακτηριστική περίπτωση.

Έστω ότι η απόδειξη $\begin{matrix}\Pi_2\\ \phi\end{matrix}$ αντιστοιχεί στον όρο N^ϕ και η απόδειξη $\begin{matrix}[\phi]_i\\ \Pi_2\\ \psi\end{matrix}$ στον όρο M^ψ (που έχει ελεύθερη μεταβλητή x_i^ϕ). Τότε σύμφωνα με την αντιστοιχία Curry-Howard η απόδειξη $\dfrac{\begin{matrix}\overline{[\phi]}_i\\ \Pi_1\\ \psi\end{matrix}}{\phi \to \psi}\,\mathrm{i}$ αντιστοιχεί στον όρο $\lambda x_i^\phi M^\psi$ και η απόδειξη $\dfrac{\dfrac{\begin{matrix}\overline{[\phi]}_i\\ \Pi_1\\ \psi\end{matrix}}{\phi \to \psi}\,\mathrm{i} \qquad \begin{matrix}\Pi_2\\ \phi\end{matrix}}{\psi}$ (που είναι redex) αντιστοιχεί στον όρο $(\lambda x_i^\phi M^\psi)N^\phi$ (που κι' αυτός είναι – το αντίστοιχο – redex). Είναι εύκολο να δούμε ότι το contractum της $\dfrac{\dfrac{\begin{array}{c}\overline{[\phi]}_i\\ \Pi_1\\ \psi\end{array}}{\phi \to \psi}\,\mathrm{i} \qquad \begin{array}{c}\Pi_2\\ \phi\end{array}}{\psi}$ που είναι η απόδειξη $\begin{array}{c}\Pi_2\\ [\phi]_1\\ \Pi_1\\ \psi\end{array}$ αντιστοιχεί στον όρο $M^\psi[x_i^\phi := N]$ που είναι το contractum του $(\lambda x_i^\phi M^\psi)N^\phi$.

3.2 Το σύστημα T του Gödel

Στο κεφάλαιο αυτό θα ορίσουμε μια επέκταση του συστήματος με τύπους που θα διευρύνει εντυπωσιακά την εκφραστική του δυνατότητα, δηλαδή την δυνατότητα αναπαράστασης συναρτήσεων.

Ορισμός 3.9 (Τύποι) *Διατηρούμε τους ίδιους τύπους με το αρχικό σύστημα Church με απλούς τύπους και γινόμενο τύπων εκτός του ότι προσθέτουμε δύο ατομικούς τύπους τον* **Nat** *και τον* **Bool** *ως σταθερές.*

Ορισμός 3.10 (Όροι) *Εκτός από τους συνήθεις όρους του αρχικού συστήματος Church με απλούς τύπους και γινόμενο τύπων έχουμε τα ακόλουθα*

1. - **O** *είναι όρος (σταθερά) τύπου* **Nat**.
   - *Αν t είναι όρος τύπου* **Nat** *τότε St είναι όρος τύπου* **Nat**.
2. *Αν u, v, t είναι όροι με τύπους αντίστοιχα σ, $\sigma \to (\mathbf{Nat} \to \sigma$ και* **Nat** *τότε $R\,u\,v\,t$ είναι όρος τύπου σ.*
3. **T** *και* **F** *είναι (σταθεροί) όροι τύπου* **Bool**.
4. *Αν u, v, t είναι όροι με τύπους αντίστοιχα σ, σ και* **Bool** *τότε $D\,u\,v\,t$ είναι όρος τύπου σ.*

Η διαισθητική σημασία που αποδίδεται σ' αυτά που έχουμε εισαγάγει είναι η εξής:

1. Τα **O** και S είναι αντίστοιχα το μηδέν και η συνάρτηση του επόμενου.
2. R είναι ο τελεστής αναδρομής: $R\,u\,v\,\mathbf{O} = u$, $R\,u\,v\,(n+1) = v(R\,u\,v\,n)n$.

3. Τα $\mathbf{T}$ και $\mathbf{F}$ είναι οι τιμές αληθείας.

4. Το D είναι ο τελεστής «**if**...**then**...**else**» δηλαδή ο ορισμός με περιπτώσεις: $D\,u\,v\,\mathbf{T} = u$ και $D\,u\,v\,\mathbf{F} = v$.

Ορισμός 3.11 (Αναγωγή) *Στα redex που έχουμε ήδη στη διάθεσή μας προσθέτουμε τα ακόλουθα:*

$R\,u\,v\,\mathbf{O} \to_\beta u$

$R\,u\,v\,(St) \to_\beta v(R\,u\,v\,t)t$

$D\,u\,v\,\mathbf{T} \to_\beta u$

$D\,u\,v\,\mathbf{F} \to_\beta v$

Δηλαδή αυτά που είναι αριστερά είναι τα redex και αυτά που είναι δεξιά είναι τα contractum τους. Με βάση αυτά μπορούμε να ορίσουμε όπως συνήθως την έννοια της αναγωγής $\twoheadrightarrow_\beta$.

Θεώρημα 3.2 (Ισχυρή κανονικοποίηση) *Για τους όρους του συστήματος T ισχύει το θεώρημα της ισχυρής κανονικοποίησης, δηλαδή κάθε αναγωγή τερματίζει πάντα στην μοναδική κανονική μορφή.*

3.2.1 Εκφραστική δύναμη: παραδείγματα

Μπορούμε να ορίσουμε τους λογικούς συνδέσμους:

neg για την άρνηση, **disj** για τη διάζευξη και **conj** για τη σύζευξη. Οι ορισμοί είναι

$$\mathbf{neg}(u) = D\,\mathbf{F}\,\mathbf{T}\,u \qquad \mathbf{disj}(u,v) = D\,\mathbf{T}\,v\,u \qquad \mathbf{disj}(u,v) = D\,v\,\mathbf{F}\,u$$

Για παράδειγμα, $\mathbf{disj}(\mathbf{T},x) \twoheadrightarrow_\beta \mathbf{T}$ και $\mathbf{disj}(\mathbf{F},x) \twoheadrightarrow_\beta x$. Είναι εύκολο να δούμε ότι και με τους υπόλοιπους συνδέσμους ικανοποιούνται οι επιθυμητές ιδιότητες.

Για να αναπαραστήσουμε συναρτήσεις πρέπει πρώτα να αναπαραστήσουμε τους φυσικούς αριθμούς. Η φυσική επιλογή είναι ο όρος

$\overline{n} = S^n(\mathbf{O})$ να αναπαριστά τον φυσικό αριθμό $n \in \mathbb{N}$. ($S^n(\mathbf{O})$ είναι ο όρος $\underbrace{S(S(\cdots(S}_{n \text{ φορές}}(\mathbf{O})\cdots))$.

Οι αναδρομικές συναρτήσεις δίνονται με ορισμούς του τύπου

$$x + o = x \qquad x + Sy = S(x + y)$$

Αυτοί οι ορισμοί μπορούν να μεταφερθούν στο σύστημα T χρησιμοποιώντας τον τελεστή R. Θα δώσουμε το παράδειγμα για την πρόσθεση. Ορίζουμε

$$t[x, y] = R\,x(\lambda z^{\mathbf{Nat}}.\lambda z'^{\mathbf{Nat}}.Sz)\,y$$

Τότε έχουμε

$t[x, \mathbf{O}] \twoheadrightarrow_\beta x$ και

$t[x, Sy] \twoheadrightarrow_\beta (\lambda z^{\mathbf{Nat}}.\lambda z'^{\mathbf{Nat}}.Sz)(t[x, y])y \twoheadrightarrow_\beta St[x, y]$

πράγμα που σημαίνει ότι μπορούμε να θεωρήσουμε τον όρο $t[x, y]$ ως ορισμό της πρόσθεσης $x + y$.

Άσκηση: Ορίστε τον πολ/σμό και την εκθετική συνάρτηση.

Το σύστημα T έχει πολύ μεγάλη εκφραστική δυνατότητα. Μπορούμε να ορίσουμε όλες τις πρωτογενείς αναδρομικές συναρτήσεις και πολλές περισσότερες. Το σύστημα T συνδέεται με το αξιωματικό σύστημα της αριθμητικής του Peano με τον ακόλουθο τρόπο. Αν υποθέσουμε την αρχή της κανονικοποίησης για τους όρους του συστήματος T τότε μπορούμε να αποδείξουμε τη συνέπεια της αριθμητικής του Peano μεταφράζοντάς το κατάλληλα στο σύστημα T (μετάφραση Gödel). Ένα πόρισμα αυτού του αποτελέσματος είναι το ακόλουθο

Θεώρημα 3.3 *Οι συναρτήσεις που μπορούν να αναπαρασταθούν στο σύστημα T είναι ακριβώς αυτές των οποίων ο τερματισμός μπορεί να αποδειχθεί στην αριθμητική του Peano.*