Λογική και Πολυπλοκότητα

Χρήστος Κοναξής
$\mu\Pi\lambda\forall$

1 Προτασιακή λογική

Η γλώσσα της προτασιακής λογικής που θα την συμβολίζουμε με Γ_0 περιλαμβάνει σύμβολα-προτάσεις και σύμβολα-συνδέσμων. Αναλυτικά το σύνολο των συμβόλων της αποτελείται από τα εξής στοιχεία:

- $x_0, x_1, x_2, \ldots$, που καλούνται προτασικές μεταβλητές,
- $\neg, \wedge, \vee$, που καλούνται σύνδεσμοι και
- $(,)$, που καλούνται 'παρενθέσεις'.

Ορισμός 1.1 Έκφραση της Γ_0 είναι μια τυχαία ακολουθία από σύμβολα της, όπως για παράδειγμα $x_0\neg) \rightarrow (x_{10}$.

Οι εκφράσεις της Γ_0 δεν αντιστοιχούν πάντα σε προτάσεις της φυσικής γλώσσας. Αυτές που αντιστοιχούν ορίζονται ως:

Ορισμός 1.2 Μια έκφραση της Γ_0 καλείται 'προτασιακός τύπος', αν και μόνο αν

- είναι προτασιακή μεταβλητή ή
- είναι της μορφής $(\neg\beta), (\beta \wedge \gamma), (\beta \vee \gamma), (\beta \rightarrow \gamma), (\beta \leftrightarrow \gamma),$, όπου β, γ είναι ήδη κατασκευασμένοι προτασιακοί τύποι.

Ένα προτασιακό τύπο της μορφής x_i ή $\neg x_i$, θα τον καλούμε *προσημασμένο* (*literal*). Το σύνολο των προτασιακών τύπων της Γ_0 συμβολίζεται $T(\Gamma_0)$.

Ένας προτασιακός τύπος μπορεί να είναι αληθής ή ψευδής. Η απόδοση τιμών αλήθειας σε ένα προτασιακό τύπο γίνεται μέσω μιας αποτίμησης:

Ορισμός 1.3 Αποτίμηση είναι μια συνάρτηση $\alpha : M(\Gamma_0) \rightarrow A, \Psi$, όπου τα A, Ψ καλούνται τιμές αλήθειας και αντιστοιχούν στις έννοιες 'αληθής' και 'ψευδής' αντίστοιχα.

Δεδομένης μιας αποτίμησης α, μπορούμε να αποδώσουμε τιμή αλήθειας σε κάθε προτασιακό τύπο ϕ, δηλαδή να ορίσουμε μια μοναδική συνάρτηση $\overline{\alpha} : T(\Gamma_0) \to A, \Psi$, η οποία είναι επέκταση της α σύμφωνα με τους κανόνες που αντιστοιχούν στους παρακάτω πίνακες αλήθειας:

$\overline{\alpha}(\phi)$	$\overline{\alpha}(\neg\phi)$
A	Ψ
Ψ	A

$\overline{\alpha}(\phi)$	$\overline{\alpha}(\psi)$	$\overline{\alpha}(\phi \wedge \psi)$	$\overline{\alpha}(\phi \vee \psi)$	$\overline{\alpha}(\phi \to \psi)$	$\overline{\alpha}(\phi \leftrightarrow \psi)$
A	A	A	A	A	A
A	Ψ	Ψ	A	Ψ	Ψ
Ψ	A	Ψ	A	A	Ψ
Ψ	Ψ	Ψ	Ψ	A	A

Ορισμός 1.4 Έστω $T \subseteq T(\Gamma_0), \phi$ προτασιακός τύπος και α αποτίμηση. Τότε θα λέμε ότι:

- Η αποτίμηση α ικανοποιεί τον ϕ, ανν $\overline{\alpha}(\phi) = A$ και 'η αποτίμηση α ικανοποιεί το T', ανν η α ικανοποιεί κάθε στοιχείο του.
- 'Το T είναι ικανοποιήσιμο', ανν υπάρχει μια αποτίμηση που το ικανοποιεί. Αντίστοιχα ο ϕ είναι ικανοποιήσιμος ανν υπάρχει αποτίμηση α που τον ικανοποιεί.
- Ο ϕ είναι 'ταυτολογία' ή 'έγκυρος', ανν κάθε αποτίμηση ικανοποιεί τον ϕ.
- Ο ϕ είναι 'αντίφαση', ανν ο $\neg\phi$ είναι ταυτολογία.

Ορισμός 1.5 Έστω $T \subseteq T(\Gamma_0)$, και ϕ προτασιακός τύπος. Τότε θα λέμε ότι 'το T συνεπάγεται ταυτολογικά τον ϕ', συμβολικά $T \models \phi$, ανν κάθε αποτίμηση που ικανοποιεί το T ικανοποιεί και τον ϕ. Αν δεν ισχύει $T \models \phi$ θα γράφουμε $T \not\models \phi$.

Παρατηρήσεις

1. Προφανώς $T \models \phi$ για κάθε $\phi \in T$.
2. Αν το T δεν είναι ικανοποιήσιμο, τότε $T \models \phi$ για κάθε ϕ.
3. Αν $\phi \models \psi$ και $\psi \models \phi$, τότε γράφουμε $\phi \equiv \psi$ και θα λέμε ότι οι τύποι ϕ, ψ είναι ταυτολογικά ισοδύναμοι.

Πρόταση 1.1 Έτσω ϕ, ψ, θ προτασιακοί τύποι. Τότε ισχύουν:

1. $(\phi \vee \psi) \equiv (\psi \vee \phi)$,
2. $(\phi \wedge \psi) \equiv (\psi \wedge \phi)$,
3. $\neg\neg\phi \equiv \phi$,
4. $((\phi \vee \psi) \vee \theta) \equiv (\phi \vee (\psi \vee \theta))$,
5. $((\phi \wedge \psi) \wedge \theta) \equiv (\phi \wedge (\psi \wedge \theta))$,
6. $((\phi \wedge \psi) \vee \theta) \equiv ((\phi \vee \psi) \wedge (\psi \vee \theta))$,
7. $((\phi \vee \psi) \wedge \theta) \equiv ((\phi \wedge \psi) \vee (\psi \wedge \theta))$,
8. $\neg(\phi \vee \psi) \equiv (\neg\phi \wedge \neg\psi)$,
9. $\neg(\phi \wedge \psi) \equiv (\neg\phi \vee \neg\psi)$,
10. $(\phi \vee \phi) \equiv \phi$,
11. $(\phi \wedge \phi) \equiv \phi$,
12. $(\neg\phi \vee \psi) \equiv (\phi \rightarrow \psi)$.

Ένας προτασιακός τύπος ϕ είναι σε κανονική συζευκτική μορφή ανν $\phi = \bigwedge_{i=1}^{n} C_i$, $n \geq 1$ και κάθε C_i είναι η διάζευξη μιας ή περισσότερων literals. Οι C_i λέγονται *όροι* (*clauses*). Αντίστοιχα ένας προτασιακός τύπος ϕ είναι σε κανονική διαζευκτική μορφή ανν $\phi = \bigvee_{i=1}^{n} D_i$, $n \geq 1$ και κάθε D_i είναι η σύζευξη μιας ή περισσότερων literals. Οι D_i λέγονται *implicants*.

Χρησιμοποιώντας την πρόταση 1.1, μπορούμε να αποδείξουμε την παρακάτω:

Πρόταση 1.2 Κάθε προτασιακός τύπος ϕ μπορεί να γραφεί σε κανονική διαζευκτική (DNF) ή κανονική συζευκτική μορφή (CNF).

Η απόδειξη της προηγούμενης πρότασης γίνεται με επαγωγή στην πολυπλοκότητα του προτασιακού τύπου ϕ. Από την απόδειξη έπεται ότι το μέγεθος της κανονικής μορφής ενός τύπου μπορεί να είναι εκθετικά μεγαλύτερο από αυτό του αρχικού τύπου.

Ένας προτασιακός τύπος ϕ μπορεί να κωδικοποιηθεί ως ένα string σε ένα αλφάβητο που περιέχει τα σύμβολα $x, 0, 1, \neg, \vee, \wedge$. Το μήκος του ϕ είναι το μήκος του αντίστοιχου string. Το πρόβλημα *SATISFIABILITY* ή *SAT* είναι: ο τυχαίος προατασιακός τύπος ϕ ο οποίος είναι σε κανονική συζευκτική

μορφή μορφή (CNF), είναι ικανοποιήσιμος;
Προφανώς το SAT μπορεί να λυθεί εξετάζοντας όλες τις δυνατές αποτιμήσεις για τις έστω n μεταβλητές του τύπου ϕ. Ο αλγόριθμος αυτός έχει χρόνο $\mathcal{O}(n^2 2^n)$. Το SAT είναι το πρώτο πρόβλημα το οποίο αποδείχθηκε ($Cook$) ότι ανήκει στο NP. Είναι άγμωστο ακόμα αν το SAT ανήκει στο P. Θέτοντας όμως περιορισμούς στο SAT μπορούμε να κατασκευάσουμε προβλήματα που λύνονται σε πολυωνυμικό χρόνο.

2 Horn Clauses

Ένα τέτοιο πρόβλημα είναι το $Horn\text{-}SAT$:

Ορισμός 2.1 Ο περιορισμός του SAT σε στιγμιότυπα των οποίων οι clauses περιέχουν το πολύ μια θετική literal, όπου θετική literal είναι μια μεταβλητή και αρνητική literal είναι η άρνηση μιας μεταβλητής, καλείται HORN-SAT.

Μια clause που περιέχει το πολύ μια θετική literal καλείται Horn clause. Για παράδειγμα οι επόμενες clauses είναι Horn: $(\neg x_1 \vee x_2), (\neg x_2 \vee x_3 \vee \neg x_4 \vee \neg x_5)), (x_7)$. Μια clause η οποία έχει ακριβώς μια θετική literal καλείται *implication*. Παρατηρούμε ότι κάθε implication (λόγω της πρότασης 1.1 (9),(12)), μπορεί να γραφεί ως: $((x_1 \wedge x_2 \wedge \ldots \wedge x_m) \rightarrow y)$, όπου y είναι η μοναδική θετική literal της implication. Αν έχουμε μια implication της μορφής (x_i) τότε αυτή καλείται *fact* και γράφεται ως (από τον πίνακα αλήθειας της συνεπαγωγής): $(C \rightarrow x_i)$, όπου η έκφραση C παίρνει τιμή αλήθειας A. Μια clause που περιέχει μόνο αρνητικές literals καλείται *constraint*.

Θεώρημα 2.1 Το HORN-SAT είναι στο **P**.

Απόδειξη Έστω ένας προτασιακός τύπος ϕ με μεταβλητές $x_1, x_2, \ldots, x_n$, σε κανονική συζευκτική μορφή, του οποίου όλες οι clauses είναι Horn. Θα περιγράψουμε έναν αλγόριθμο ο οποίος ελέγχει σε πολυωνυμικό χρόνο αν ο τύπος αυτός είναι ικανοποιήσιμος ή όχι. Δηλαδή ο αλγόριθμος ψάχνει (αν υπάρχει) μια αποτίμηση α τέτοια ώστε $\overline{\alpha}(\phi) = A$. Φυσικά μας ενδιαφέρουν μόνο οι τιμές αλήθειας που δίνει η α στις μεταβλητές που εμφανίζονται στον ϕ. Έτσι μπορούμε να θεωρήσουμε την αποτίμηση ως ένα σύνολο μεταβλητών T, το οποίο αποτελείται από τις μεταβλητές οι οποίες έχουν τιμή αλήθειας A. Προφανώς γνωρίζοντας το T, γνωρίζουμε και τις τιμές αλήθειας που δίνει η αποτίμηση στο σύνολο των μεταβλητών του ϕ.

Αρχικά ελέγχουμε αν οι implications του ϕ είναι ικανοποιήσιμες. Αρχικοποιούμε το σύνολο $T := \emptyset$, δηλαδή όλες οι μεταβλητές έχουν τιμή αλήθειας false. Προφανώς τότε θα ικανοποιούνται όλες οι implications που έχουν τουλάχιστον δυο literals αφού αυτές θα γράφονται ως $((x_1 \wedge x_2 \wedge \ldots \wedge x_m) \rightarrow y)$ και αφού η υπόθεση και το συμπέρασμα της συνεπαγωγής είναι ψευδή, αυτή

θα είναι αληθής. Επομένως αν δεν υπάρχει implication που να περιέχει μόνο μια literal, δηλαδή clause της μορφής (x_i), έχουμε ήδη βρει μια αποτίμηση που ικανοποιεί όλες της implications του ϕ. Στην περίπτωση που υπάρχει τέτοια implication, ο αλγόριθμος επαναλαμβάνει το επόμενο βήμα μέχρι η αποτίμηση που αντιστοιχεί στο σύνολο T να ικανοποιεί όλες τις implications: επέλεξε μια implication $((x_1 \wedge x_2 \wedge \ldots \wedge x_m) \rightarrow y)$ που δεν ικανοποιείται με το υπάρχον T. Επομένως θα πρέπει $x_1, x_2, \ldots, x_m \in T$ και $y \notin T$. Πρόσθεσε την μεταβλητή y στο T. Έτσι το T μετά την ενημέρωση θα ικανοποιεί την implication αυτή.

Ο αλγόριθμος αυτός τερματίζει αφού το σύνολο $x_1, x_2, \ldots, x_n$, των μεταβλητών του ϕ είναι πεπερασμένο και το T σε κάθε βήμα του αλγόριθμου δεν μπορεί να μικραίνει σε μέγεθος. Προφανώς το T που παίρνουμε μετά τον τερματισμό του αλγόριθμου πρέπει να ικανοποιεί όλες τις implications του ϕ, αφού μόνο τότε τερματίζει ο αλγόριθμος. Επιπλέον, το T που κατασκευάζεται με αυτό τον τρόπο είναι το ελάχιστο από όλα τα σύνολα T' που ικανοποιούν όλες τις implications του ϕ. Πράγματι έστω T' ένα σύνολο αληθοτιμών που ικανοποιεί όλες τις implications του ϕ. Θα δείξουμε ότι $T \subseteq T'$. Υποθέτουμε ότι δεν ισχύει η προηγούμενη συμπερίληψη. Τότε θεωρούμε το ελάχιστο βήμα του αλγόριθμου στο οποίο έχουμε την εισαγωγή στο T μιας μεταβλητής y, μετά την οποία ισχύει $T' \subset T$. Τότε η μεταβλητή y μέχρι πριν από το βήμα αυτό δεν ανήκε στο T επομένως η αντίστοιχη implication δεν ικανοποιούνταν από το T και αφού $T' \subset T$, η implication που εξετάσθηκε στο βήμα αυτό δεν μπορεί να ικανοποιείται από το T', άτοπο.

Τώρα μπορούμε να αποφασίσουμε για την ικανοποιησιμότητα του ϕ: ο ϕ είναι ικανοποιήσιμος ανν η αποτίμηση που αντιστοιχεί στο σύνολο T ικανοποιεί τον ϕ. Προφανώς η αποτίμηση αυτή ικανοποιεί όλες τις implications του ϕ από την κατασκευή της. Αν τώρα υπάρχει constraint του ϕ, π.χ. μια clause της μορφής $(\neg(x_1 \wedge \neg x_2 \wedge \ldots \wedge \neg x_m))$, που δεν ικανοποιείται από το T, τότε θα πρέπει $x_1, x_2, \ldots, x_m \subseteq T$. Επομένως δεν υπάρχει σύνολο T' τέτοιο που $T \subseteq T'$ και το T' να ικανοποιεί την clause αυτή. Εφόσον όλα τα σύνολα που ικανοποιούν τον ϕ είναι υπερσύνολα του T, έπεται ότι ο ϕ δεν είναι ικανοποιήσιμος.

Ο αλγόριθμος που περιγράψαμε προφανώς είναι πολυωνυμικού χρόνου.

3 Συναρτήσεις Boole και Λογικά κυκλώματα

Ορισμός 3.1 Μια n-μελής *Boolean συνάρτηση* είναι μια συνάρτηση $f : \{A, \Psi\} \mapsto \{A, \Psi\}$. Υπάρχουν 2^{2^n} τέτοιες συναρτήσεις.

Θεώρημα 3.1 Σε κάθε προτασιακό τύπο ϕ με n διαφορετικές μεταβλητές αντιστοιχεί μια συνάρτηση Boole με $k+1$ μεταβλητές και αντίστροφα αν f είναι μια συνάστηση Boole με n μεταβλητές τότε υπάρχει ένας προτασιακός τύπος ϕ_f στον οποίο εμφανίζονται οι $x_1, x_2, \ldots, x_n$, τέτοιος που για κάθε αποτίμηση α να ισχύει

$$\overline{\alpha}(\phi) = f(\alpha(x_1), \ldots, \alpha(x_n)),$$

δηλαδή ο πίνακας αλήθειας του ϕ_f περιγράφει πλήρως την f.

Για παράδειγμα οι σύνδεσμοι $\wedge, \vee, \rightarrow, \leftrightarrow$ είναι διμελείς συναρτήσεις Boole ενώ ο σύνδεσμος $\neg$ είναι μονομελής συνάρτηση Boole.

Ο προτασιακός τύπος ϕ_f του προηγούμενου θεωρήματος έχει μήκος $\mathcal{O}(n^2 2^n)$. Υπάρχουν όμως και άλλοι πιο 'οικονομικοί' τρόποι για να αναπαριστούμε Boolean συναρτήσεις, τα *λογικά κυκλώματα (Boolean circuits)*.

Ορισμός 3.2 Ένα λογικό κύκλωμα είναι ένας κατευθυνόμενος γράφος $C = (V, E)$, όπου οι κόμβοι του C, δηλαδή τα στοιχεία στο $V = \{0, 1, 2, \ldots, n\}$, καλούνται *πύλες, (gates)* και ισχύουν τα εξής:

1. ο γράφος C δεν περιέχει κύκλους,
2. οι πύλες του C έχουν indegree (αριθμό εισερχομένων ακμών) $0, 1,$ ή 2,
3. σε κάθε πύλη $i \in V$ αντιστοιχεί ένα σύμβολο (ο χαρακτήρας της πύλης) $s(i) \in \{A, \Psi, \neg, \vee, \wedge\} \cup \{x_1, x_2, \ldots\}$. Αν $s(i) \in \{A, \Psi\} \cup \{x_1, x_2, \ldots\}$, τότε ο indegree της πύλης i είναι 0, δηλαδή ο i δεν έχει εισερχόμενες ακμές. Τέτοιες πύλες καλούνται *είσοδοι (inputs)* του λογικού κυκλώματος. Αν $s(i) \in \{\wedge, \vee\}$ τότε η πύλη i έχει indegree 2. Αν $s(i) = \neg$ τότε η πύλη i έχει indegree 1. Τέλος αν $i = n$ τότε η πύλη i έχει *outdegree (αριθμό εξερχόμενων ακμών)* 0 και θα καλείται *έξοδος (output)* του κυκλώματος. Υπάρχουν λογικά κυκλώματα που έχουν περισσότερες της μιας εξόδου. Αυτά θα υπολογίζουν περισσότερες από μια συναρτήσεις Boole.

Ένα λογικό κύκλωμα αναπαριστά μια Boolean συνάρτηση επομένως μας ενδιαφέρει να υπολογίσουμε την τιμή αλήθειας ενός κυκλώματος (τιμή αλήθειας της output), δεδομένης μιας αποτίμησης α των εισόδων του. Ο τρόπος που υπολογίζουμε την τιμή αλήθειας $\alpha(i)$ μιας πύλης $i \in V$ ενός λογικού κυκλώματος, γίνεται αναδρομικά ως εξής:

- Αν $s(i) = A$, τότε $\alpha(i) = A$,
- Αν $s(i) = \Psi$, τότε $\alpha(i) = \Psi$.
- Αν $s(i) \in \{x_1, x_2, \ldots\}$, τότε $\alpha(i) = \alpha(s(j))$
- Αν $s(i) = \neg$, τότε $\alpha(i) = \neg s(j)$, όπου j είναι η μοναδική πύλη με $j < i$ και $(j, i) \in E$.
- Αν $s(i) = \vee$, τότε $\alpha(i) = \alpha(s(j) \vee s(j'))$, όπου j, j' είναι οι εισερχόμενες πύλες στην i, με $j, j' < i$ και $(j, i), (j', i) \in E$.
- Αν $s(i) = \wedge$, τότε $\alpha(i) = \alpha(s(j) \wedge s(j'))$, όπου j, j' είναι οι εισερχόμενες πύλες στην i, με $j, j' < i$ και $(j, i), (j', i) \in E$.
- Αν $i = n$, δηλαδή η πύλη i είναι η έξοδος του κυκλώματος, τότε η τιμή $\alpha(n)$ είναι η τιμή αλήθειας του κυκλώματος.

Παράδειγμα Έστω το λογικό κύκλωμα του σχήματος 3.1 (α)(σελ. 18). Το κύκλωμα αυτό αναπαριστά τον προτασιακό τύπο

$$\phi = \Big(x_1 \vee \big(x_3 \wedge \neg(x_1 \vee x_2)\big)\Big) \wedge \big((x_1 \vee x_2) \wedge \neg x_3\big)$$

ο οποίος αντιστοιχεί στην Boolean συνάρτηση που περιγράφει το κύκλωμα.

Αντίστροφα, δοθέντος του προτασιακού τύπου ϕ, (δηλαδή της συνάρτησης Boole που αντιστοιχεί στον ϕ), μπορούμε να κατασκευάσουμε το λογικό κύκλωμα που περιγράφει τον ϕ. Το κύκλωμα αυτό φαίνεται στο σχήμα 3.1 (β)(σελ. 19).

Οι διαφορές στο μέγεθος των δυο ισοδύναμων λογικών κυκλωμάτων οφείλονται στο ότι στην κατασκευή του λογικού κυκλώματος του σχήματος 3.1 (β) δεν λάβαμε υπ'όψιν τους κοινούς υποτύπους που έμφανίζονται στον ϕ. Η ύπαρξη τέτοιων υποτύπων οι οποίοι αντιστοιχούν σε πύλες του κυκλώματος με outdegree μεγαλύτερο του 1, κάνει την αναπαράσταση των Boolean συναρτήσεων από λογικά κυκλώματα 'οικονομικότερη' από την ισοδύναμη αναπαράσταση με προτασιακούς τύπους.

Δεδομένης μιας Boolean συνάρτησης f με n μεταβλητές *(ισοδύναμα ενός προτασιακού τύπου με n μεταβλητές)*, Θα θέλαμε να γνωρίζουμε ένα άνω φράγμα στο μέγεθος των λογικών κυκλωμάτων που περιγράφουν την f.

Θεώρημα 3.2 Για κάθε $n \geq 2$ υπάρχει μια n-μελής Boolean συνάρτηση f τέτοια που δεν υπάρχει λογικό κύκλωμα με $\frac{2^n}{2n}$ ή λιγότερες πύλες που την υπολογίζει.

Απόδειξη Προς άτοπο, έστω ότι για κάποιο $n \geq 2$ κάθε n-μελής Boolean συνάρτηση μπορεί να υπολογιστεί από λογικά κυκλώματα με $m = \frac{2^n}{2n}$ το πολύ πύλες.

Υπάρχουν 2^{2^n} n-μελείς Boolean συναρτήσεις. Μπορούμε να υπολογίσουμε ένα άνω φράγμα του αριθμού των λογικών κυκλωμάτων με m το πολύ πύλες: κάθε λογικό κύκλωμα καθορίζεται από δυο παραμέτρους για κάθε πύλη του: τον χαρακτήρα $s(i)$ της πύλης i και τις πύλες από τις οποίες ξεκινούν οι ακμές που εισέρχονται στην i. Αφού $s(i) \in \{A, \Psi, \neg, \vee, \wedge\} \cup \{x_1, x_2, \ldots\}$ και υπάρχουν m πύλες το πολύ, για κάθε πύλη έχουμε το πολύ $(n+5)m^2$ επιλογές, επομένως το πολύ $\left((n+5)m^2\right)^m$ επιλογές συνολικά.

Αν λογαριθμήσουμε (με βάση το 2), τις ποσότητες $\left((n+5)m^2\right)^m$ και 2^{2^n}, παίρνουμε: $\Phi = 2^n(1 - \frac{\log \frac{4n^2}{n+5}}{2n})$ και $B = 2^n$ αντίστοιχα. Έφόσον $n \geq 2$, ισχύει $\Phi < B$. Έτσι αφού έχουμε υποθέσει ότι κάθε n-μελής Boolean συνάρτηση μπορεί να υπολογιστεί από λογικά κυκλώματα με m το πολύ πύλες, θα πρέπει να υπάρχουν τουλάχιστον δυο διαφορετικές n-μελείς Boolean συναρτήσεις f, f' οι οποίες υπολογίζονται από το ίδιο λογικό κύκλωμα, το οποίο είναι άτοπο.

Ανάλογο είναι και το επόμενο θεώρημα.

Θεώρημα 3.3 Για κάθε πολυώνυμο p υπάρχουν n και n-μελής συνάρτηση Boole f , τέτοια που για κάθε προτασιακό τύπο ϕ, αν ο ϕ αντιστοιχεί στην f, τότε $||\phi|| > p(n)$. Δηλαδή υπάρχουν n-μελείς συναρτήσεις Boole που οι τύποι που τις περιγράφουν δεν έχουν πολυωνυμικό μέγεθος ως προς n.

Απόδειξη Θεωρούμε όλους τους προτασιακούς τύπους ϕ τέτοιους που $||\phi|| \leq p(n)$. Υπάρχουν $2^{p(n)}$ τέτοιοι τύποι. Όμως υπάρχουν 2^{2^n} n-μελείς Boolean συναρτήσεις. Επομένως υπάρχουν n-μελείς Boolean συναρτήσεις που δεν μπορούν να αναπαρασταθούν από προτασιακούς τύπους πολυωνυμικού μεγέθους.

4 Κατηγορηματικός Λογισμός

Η γλώσσα του προτασιακού λογισμού έχει περιορισμένες δυνατότητες έκφρασης. Για να μπορέσουμε να εκφράσουμε λεπτομερέστερες μαθηματικές προτάσεις χρησιμοποιούμε τις λεγόμενες πρωτοβάθμιες γλώσσες (συμβ. Γ_1).

Το λεξιλόγιο μιας πρωτοβάθμιας γλώσσας αποτελείται από τα παρακάτω σύμβολα:

1. $x_0, x_1, x_2, \ldots$, που καλούνται 'μεταβλητές'
2. $\neg, \rightarrow$, που καλούνται 'σύνδεσμοι'
3. $(,)$, που καλούνται 'παρενθέσεις'
4. $\approx$, που καλείται 'ισότητα'
5. $\forall$, που καλείται 'καθολικός ποσοδείκτης'
6. για κάθε $n \in \mathbb{N} - \{0\}$, ένα σύνολο (ίσως κενό) $\{P_{n_i} \mid i \in I_n\}$, τα στοιχεία του οποίου καλούνται 'n-μελή κατηγορηματικά σύμβολα'
7. για κάθε $n \in \mathbb{N} - \{0\}$, ένα σύνολο (ίσως κενό) $\{f_{n_j} \mid j \in J_n\}$, τα στοιχεία του οποίου καλούνται 'n-θέσια συναρτησιακά σύμβολα'
8. ένα σύνολο (ίσως κενό) $\{c_k \mid k \in K\}$, τα στοιχεία του οποίου καλούνται 'ατομικές σταθερές'.

Το σύνολο των συμβόλων της Γ_1 το συμβολίζουμε με $\Sigma(\Gamma_1)$ και το σύνολο των μεταβλητών της με $M(\Gamma_1)$. Τα σύμβολα των κατηγοριών (1)-(5) καλούνται 'λογικά σύμβολα' γιατί η ερμηνεία τους είναι πάντα η ίδια και στηρίζεται στην διαισθητική λογική ενώ τα σύμβολα των (6)-(8) καλούνται 'μη λογικά σύμβολα' γιατί μπορούν να ερμηνευθούν με διάφορους τρόπους. Θα γράφουμε $\exists x\phi$ αντί για $\neg\forall x\neg\phi$.

Παραδείγματα α) Η γλώσσα $\Gamma_1^{\theta\alpha}$ της θεωρίας αριθμών έχει εκτός από τα λογικά σύμβολα, ένα μονοθέσιο συναρτησιακό σύμβολο $'$, δύο διθέσια συναρτησιακά σύμβολα $\oplus, \odot$ και μια σταθερά $\mathbf{0}$.
β) Η γλώσσα $\Gamma_1^{\theta\gamma}$ της θεωρίας γραφημάτων έχει εκτός από τα λογικά σύμβολα, μόνο ένα διμελές κατηγορηματικό σύμβολο G.

Ορισμός 4.1 Μια έκφραση α της Γ_1 είναι 'όρος', αν και μόνο αν

1. ο α είναι μεταβλητή ή σταθερά
2. ο α είναι της μορφής $f(t_1, t_2, \ldots, t_n)$, όπου $t_1, t_2, \ldots, t_n$ είναι ήδη κατασκευασμένοι όροι.

Το σύνολο των όρων συμβολίζεται με $O(\Gamma_1)$.

Ορισμός 4.2 Μια έκφραση α της Γ_1 είναι 'τύπος', αν και μόνο αν η α είναι της μορφής:

1. $t_1 \approx t_2$ ή
2. $P(t_1, t_2, \ldots, t_n)$, όπου P είναι n-μελές κατηγορηματικό σύμβολο και $t_1, t_2, \ldots, t_n$ όροι, ή
3. $(\neg\beta), (\beta \rightarrow \gamma), \forall x\beta$, όπου β, γ είναι ήδη κατασκευασμένοι τύποι.

Ένας τύπος της μορφής (1) ή (2) καλείται ατομικός. Το σύνολο των ατομικών τύπων συμβολίζεται με $AT(\Gamma_1)$ και το σύνολο των τύπων με $T(\Gamma_1)$.

Ένας τύπος στον οποίο δεν εμφανίζονται ελεύθερες μεταβλητές (δηλαδή μεταβλητές που δεν δεσμεύονται από κάποιον ποσοδείκτη) θα λέγεται πρόταση.

Θεώρημα 4.1 (Αρχή της επαγωγής) α) Αν $A \subseteq O(\Gamma_1)$ τέτοιο που

1. όλες οι μεταβλητές και οι σταθερές να ανήκουν στο A και
2. $f(t_1, t_2, \ldots, t_n) \in A$, για κάθε n-θέσιο συναρτησιακό σύμβολο f και κάθε όρους $t_1, t_2, \ldots, t_n \in A$,

τότε $A = O(\Gamma_1)$.

β) Αν $A \subseteq T(\Gamma_1)$ τέτοιο που

1. $AT(\Gamma_1) \subseteq A$ και
2. $(\neg\psi) \in A, (\psi \rightarrow \chi) \in A, \forall x\psi \in A$, για κάθε $\chi, \psi \in A$ και κάθε μεταβλητή x,

τότε $A = T(\Gamma_1)$.

Για να αποδώσουμε τιμές αλήθειας σε τύπους μιας πρωτοβάθμιας γλώσσας χρειαζόμαστε κάτι περισσότερο πολύπλοκο από μια αποτίμηση του προτασιακού λογισμού και αυτό γιατί πρέπει να ερμηνεύσουμε τα μη λογικά σύμβολα της γλώσσας αλλά και γιατί οι μεταβλητές της μπορούν να παίρνουν τιμές μέσα σε οποιοδήποτε σύνολο ακόμα και άπειρο.

Ορισμός 4.3 Μια 'δομή' $\mathcal{A}$ για μια πρωτοβάθμια γλώσσα Γ_1 αποτελείται από τα εξής:

1. ένα μη κενό σύνολο $|\mathcal{A}|$, το 'σύμπαν' της $\mathcal{A}$,

2. για κάθε $n \in \mathbb{N} - \{0\}$, ένα σύνολο (ίσως κενό) $\{P_{n_i}^{\mathcal{A}} \mid i \in I_n\}$ από n-μελείς σχέσεις στο $|\mathcal{A}|$ που αποτελούν τις ερμηνείες των n-μελών κατηγορηματικών συμβόλων,

3. για κάθε $n \in \mathbb{N} - \{0\}$, ένα σύνολο (ίσως κενό) $\left\{f_{n_j}^{\mathcal{A}} \mid j \in J_n\right\}$, από συναρτήσεις με πεδίο ορισμού το $|\mathcal{A}|^n$ και πεδίο τιμών ένα υποσύνολο του $|\mathcal{A}|$ που αποτελούν τις ερμηνείες των n-θέσεων συναρτησιακών συμβόλων, και

4. ένα σύνολο (ίσως κενό) $\{c_k^{\mathcal{A}} \mid k \in K\}$, από στοιχεία του $|\mathcal{A}|$ που αποτελούν τις ερμηνείες των συμβόλων σταθερών.

Παράδειγμα Η δομή $\mathcal{N}$ για την γλώσσα $\Gamma_1^{\theta\alpha}$ ορίζεται: $|\mathcal{N}| = \mathbb{N}$, στις συναρτήσεις $',\oplus,\odot$ αντιστοιχούν οι συνήθεις συναρτήσεις του επόμενου, της πρόσθεσης και του πολλαπλασιασμού στους φυσικούς και το $\mathbf{0}$ αντιστοιχεί στο $0 \in \mathbb{N}$.

Ορισμός 4.4 Έστω $\mathcal{A}$ δομή για την Γ_1. Αποτίμηση στην $\mathcal{A}$ είναι μια συνάρτηση $\upsilon : M(\Gamma_1) \to |\mathcal{A}|$. Για κάθε τέτοια συνάρτηση υ υπάρχει μοναδική επέκταση της $\overline{\upsilon} : O(\Gamma_1) \to |\mathcal{A}|$ τέτοια που: $\overline{\upsilon}(x) = \upsilon(x), \overline{\upsilon}(c) = c$ και $\overline{\upsilon}(f(t_1, t_2, \ldots, t_n) = f^{\mathcal{A}}(\overline{\upsilon}(t_1, \ldots, \overline{\upsilon}(t_n))$, για κάθε μεταβλητή x, σταθερά c, συναρτησιακό σύμβολο f και όρους $t_1, t_2, \ldots, t_n$.

Τώρα μπορούμε να ορίσουμε τι σημαίνει να αληθεύει ένας τύπος ϕ για μια δομή $\mathcal{A}$ και μια αποτίμηση υ στην $\mathcal{A}$.

Ορισμός 4.5 Έστω $\mathcal{A}$ δομή για την Γ_1, ϕ τύπος, T σύνολο τύπων και υ αποτίμηση στην $\mathcal{A}$. Τότε

1. ο ϕ αληθεύει για την υ στην $\mathcal{A}$, συμβολικά $\mathcal{A} \models \phi[\upsilon]$, ανν
   - $\overline{\upsilon}(t_1) = \overline{\upsilon}(t_2)$, αν ο ϕ είναι της μορφής $t_1 \approx t_2$,
   - $< \overline{\upsilon}(t_1), \ldots, \overline{\upsilon}(t_n) > \in P^{\mathcal{A}}$, αν ο ϕ είναι της μορφής $P(t_1, t_2, \ldots, t_n)$,
   - δεν ισχύει: $\mathcal{A} \models \psi[\upsilon]$, αν ο ϕ είναι της μορφής $\neg\psi$,
   - αν $\mathcal{A} \models \psi[\upsilon]$, τότε $\mathcal{A} \models \chi[\upsilon]$, αν ο ϕ είναι της μορφής $\psi \to \chi$,
   - για κάθε $\alpha \in |\mathcal{A}| : \ \mathcal{A} \models \psi[\upsilon(x|\alpha)]$, αν ο ϕ είναι της μορφής $\forall x\psi$. Με $\upsilon(x|\alpha)$ συμβολίζουμε την αποτίμηση που συμφωνεί με την υ σε όλες τις μεταβλητές και δίνει στην μεταβλητή x την τιμή $\alpha \in |\mathcal{A}|$.

2. το T αληθεύει για την υ στην $\mathcal{A}$ ή η υ ικανοποιεί το T στην $\mathcal{A}$, ανν κάθε στοιχείο του T αληθεύει για την υ στην $\mathcal{A}$. Αν υπάρχει δομή $\mathcal{A}$ και αποτίμηση υ στην $\mathcal{A}$, έτσι που το T να αληθεύει για τις υ,$\mathcal{A}$, θα λέμε ότι το T είναι ικανοποιήσιμο.

Μια πρόταση ϕ αληθεύει για όλες τις αποτιμήσεις υ σε μια δομή $\mathcal{A}$ ή για καμία τους. Μια δομή $\mathcal{A}$ για την οποία ισχύει $\mathcal{A} \models \phi$ θα λέγεται μοντέλο της πρότασης ϕ.

Μοντέλα της θεωρίας Γραφημάτων

Μια δομή $\mathcal{A}$ μπορεί να είναι ή όχι μοντέλο μιας πρότασης ϕ. Μια πρόταση ϕ μπορεί να θεωρηθεί ότι αποτελεί περιγραφή όλων των μοντέλων της. Αυτή η αντιστοιχία γίνεται καλύτερα φανερή αν χρησιμοποιήσουμε προτάσεις της γλώσσας $\Gamma_1^{\theta\gamma}$ της θεωρίας γραφημάτων. Κάθε μοντέλο μιας τέτοιας πρότασης είναι ένας γράφος. Θα περιοριστούμε στα επόμενα μόνο σε πεπερασμένους γράφους, δηλαδή γράφους με πεπερασμένο αριθμό κορυφών.

Έστω η πρόταση

$$\phi = \Big(\forall x \exists y G(x,y) \wedge \forall x \forall y \forall z \big(G(x,y) \wedge G(x,z) \rightarrow y \approx z\big)\Big)$$

και γράφος Γ. Αν ερμηνεύσουμε την σχέση $G(x,y)$ ως 'υπάρχει ακμή από το x στο y στον Γ', τότε είναι προφανές ότι η ϕ αληθεύει σε κάθε γράφο ο οποίος αναπαριστά μια συνάρτηση (οι κορυφές του έχουν outdegree ένα). Διαφορετικά, η ϕ εκφράζει την ιδότητα 'η σχέση G είναι συνάρτηση'.

Ανάλογα η πρόταση $\phi = \forall x \big(\forall y (G(x,y) \rightarrow G(y,x))\big)$ εκφράζει την ιδιότητα 'η G είναι συμμετρική'. Κάθε μοντέλο της ϕ είναι ένας συμμετρικός γράφος.

Κάθε πρόταση της $\Gamma_1^{\theta\gamma}$ περιγράφει και μια ιδιότητα γράφων. Αντίστροφα, κάθε ιδιότητα γράφων αντιστοιχεί σε ένα υπολογιστικό πρόβλημα: δεδομένου ενός γράφου Γ, έχει ο Γ την ιδιότητα;

Έτσι έχουμε τον ακόλουθο ορισμό.

Ορισμός 4.6 Έστω μια δομή Γ (δηλαδή ένας γράφος) για μια πρόταση ϕ της $\Gamma_1^{\theta\gamma}$. Ορίζουμε ως ϕ-GRAPHS το πρόβλημα αν $\Gamma \models \phi$. Για παράδειγμα αν $\phi = \forall x \big(\forall y (G(x,y) \rightarrow G(y,x))\big)$, τότε το ϕ-GRAPHS είναι το πρόβλημα απόφασης αν ένας γράφος Γ είναι συμμετρικός.

Θεώρημα 4.2 Για κάθε πρόταση ϕ της $\Gamma_1^{\theta\gamma}$, το πρόβλημα ϕ-GRAPHS είναι στο **P**.

Απόδειξη Θα δείξουμε, με επαγωγή στην πολυπλοκότητα του ϕ, κάτι ισχυρότερο, ότι το θεώρημα ισχύει για κάθε τύπο ϕ. Επομένως θα ισχύει το ζητούμενο και για κάθε πρόταση ϕ.

- Έστω ϕ ατομικός τύπος της μορφής $x \approx y$ ή $G(x,y)$ ή $G(x,x)$. Τότε προφανώς ο έλεγχος της αλήθειας των παραπάνω τύπων για μια δομή Γ και μια αποτίμηση υ στην Γ, μπορεί να γίνει σε πολυωνυμικό χρόνο.

- Έστω ϕ της μορφής $\neg\psi$, όπου για τον ψ υπάρχει πολυωνυμικός αλγόριθμος που λύνει το πρόβλημα ψ-GRAPHS. Τότε ο ίδιος αλγόριθμος

τροποποιημένος ώστε οι απαντήσεις 'ναι' ή 'όχι' να είναι ανεστραμμένες, λύνει το πρόβλημα ϕ-GRAPHS.

- Έστω ϕ της μορφής $\psi \rightarrow \chi$ και υπάρχουν πολυωνυμικοί αλγόριθμοι για τα προβλήματα ψ-GRAPHS και χ-GRAPHS. Τότε ο αλγόριθμος που απαντά 'ναι' όταν ο αλγόριθμος του χ-GRAPHS απαντά 'ναι' ή ο αλγόριθμος του ψ-GRAPHS απαντά 'όχι', και απαντά 'όχι' διαφορετικά, λύνει το πρόβλημα ϕ-GRAPHS και είναι προφανώς πολυωνυμικός.

- Έστω ϕ της μορφής $\forall x\psi$, όπου για τον ψ υπάρχει πολυωνυμικός αλγόριθμος που λύνει το πρόβλημα ψ-GRAPHS. Δηλαδή για κάθε γράφο Γ και κάθε αποτίμηση υ, υπάρχει πολυωνυμικός αλγόριθμος που αποφασίζει αν $\Gamma \models \psi[\upsilon]$. Θέλουμε να κατασκευάσουμε αλγόριθμο που να αποφασίζει αν $\Gamma \models \forall x\psi[\upsilon]$, δηλαδή αν για κάθε κορυφή k του Γ ισχύει $\Gamma \models \psi[\upsilon(x|k)]$.

  Ο αλγόριθμος είναι ο εξής: για κάθε κορυφή $k \in \Gamma$ χρησιμοποιούμε τον αλγόριθμο που αποφασίζει το ψ-GRAPHS για την αποτίμηση $\upsilon(x|k)$. Αν όλοι οι αλγόριθμοι απαντήσουν 'ναι', τότε απαντά 'ναι', διαφορετικά απαντά 'όχι'. Προφανώς ο αλγόριθμος αυτός έχει χρόνο το γινόμενο των χρόνων των αλγορίθμων για τα προβλήματα ψ-GRAPHS,$\upsilon(x|k)$. Εφόσον το σύνολο των κορυφών κ του Γ είναι πεπερασμένο, ο αλγόριθμος είναι πολυωνυμικός.

Πόρισμα 4.1 Για κάθε πρόταση ϕ της $\Gamma_1^{\theta\gamma}$, το πρόβλημα ϕ-GRAPHS λύνεται σε χώρο $\mathcal{O}(\log n)$.

Στη συνέχεια θα αποδείξουμε ότι το REACHABILITY (δεδομένου ενός κατευθυνόμενου γράφου Γ και δυο κορυφών του x, y, υπάρχει μονοπάτι από την x στην y;) δεν μπορεί να εκφραστεί σαν ένα πρόβλημα ϕ-GRAPHS για κανένα τύπο ϕ της $\Gamma_1^{\theta\gamma}$. Το συμπέρασμα αυτό μας δείχνει και τα όρια της εκφραστικότητας των πρωτοβάθμιων γλωσσών. Με το REACHABILITY έχουμε ένα παράδειγμα προβλήματος για το οποίο υπάρχει πολυωνυμικός αλγόριθμος αλλά δεν εκφράζεται σε καμία πρωτοβάθμια γλώσσα.

Θα χρειαστούμε μερικά ακόμα αποτελέσματα από την κατηγορηματική λογική.

Θεώρημα 4.3 (Lowenheim-Skolem) Αν μια πρόταση ϕ έχει πεπερασμένα μοντέλα οσοδήποτε μεγάλης πληθικότητας, τότε έχει ένα άπειρο μοντέλο.

Θεώρημα 4.4 Δεν υπάρχει τύπος ϕ της πρωτοβάθμιας λογικής, με δυο ελεύθερες μεταβλητές x, y, ώστε το πρόβλημα ϕ-GRAPHS να είναι το REACHABILITY.

Απόδειξη Προς άτοπο, έστω ότι υπάρχει τύπος ϕ με τις ιδιότητες του θεωρήματος. Θεωρούμε την πρόταση $\psi_0 = \forall x \forall y \phi$. Η πρόταση αυτή εκφράζει την ιδιότητα ότι ένας γράφος Γ είναι *ισχυρά συνδεδεμένος (strongly conected)*, δηλαδή υπάρχει μονοπάτι ανάμεσα σε οποιεσδήποτε δυο κορυφές του. Θεωρούμε επίσης τις προτάσεις $\psi_1 = \forall x \exists y G(x,y) \wedge \forall x \forall y \forall z \big(G(x,y) \wedge G(x,z) \rightarrow y \approx z\big)$ και $\psi_2 = \forall x \exists y G(y,x) \wedge \forall x \forall y \forall z \big(G(y,x) \wedge G(z,x) \rightarrow y \approx z\big)$. Η πρόταση ψ_1 εκφράζει την ιδιότητα κάθε κορυφή ενός γράφου να έχει outdegree ένα και η πρόταση ψ_2 εκφράζει την ιδιότητα κάθε κορυφή ενός γράφου έχει indegree ένα. Αν πάρουμε την σύζευξη αυτών των τριών προτάσεων, δηλαδή την πρόταση $\psi = \psi_0 \wedge \psi_2 \wedge \psi_2$, αυτή θα εκφράζει την ιδιότητα ένας γράφος να είναι κύκλος.

Προφανώς μπορούμε να κατασκευάσουμε κύκλους με οσοδήποτε μεγάλο, αλλά πεπερασμένο αριθμό κορυφών, επομένως η πρόταση ψ έχει πεπερασμένα μοντέλα οσοδήποτε μεγάλης πληθικότητας. Από το Θεώρημα 4.3 έπεται ότι η ψ πρέπει να έχει ένα άπειρο μοντέλο Γ_∞. Αυτό όμως είναι άτοπο γιατί είναι εύκολο να δούμε ότι δεν υπάρχουν κύκλοι με άπειρο αριθμό κορυφών: αν σταθεροποιήσουμε μια κορυφή του Γ_∞ και την ονομάσουμε 0, αυτή θα έχει outdegree ένα οπότε θα υπάρχει μοναδική ακμή που την συνδέει με την κορυφή 1, η οποία επίσης έχει outdegree ένα οπότε θα υπάρχει μοναδική ακμή που την συνδέει με την κορυφή 2 κ.τ.λ. Με αυτό τον τρόπο μπορούμε να περάσουμε από όλες τις κορυφές του Γ_∞ οι οποίες συνδέονται με την κορυφή 0. Αφού ο Γ_∞ είναι ισυρά συνδεδεμένος, όλες οι κορυφές του συνδέονται με την 0. Όμως η 0 έχει indegree ένα, επομένως πρέπει να υπάρχει κάποια κορυφή k η οποία συνδέεται με την 0 με μια ακμή $(k,0)$. Έτσι ο κύκλος Γ_∞ είναι τελικά πεπερασμένος.

Το προηγούμενο θεώρημα μας οδηγεί στο ερώτημα πως μπορούμε να επεκτείνουμε μια πρωτοβάθμια γλώσσα ώστε να μπορεί κάποιος τύπος της νέας γλώσσας να εκφράσει το REACHABILITY; Διαισθητικά το πρόβλημα με το REACHABILITY είναι ότι απαιτεί έναν υπαρξιακό ποσοδείκτη και μια μεταβλητή που να εκφράζει την πρόταση 'υπάρχει μονοπάτι από την κορυφή x στην κορυφή y'. Απαιτεί δηλαδή την ύπαρξη ενός συνόλου κορυφών με μια συγκεκριμένη ιδιότητα. Εφόσον δεν γνωρίζουμε εκ των προτέρων ένα άνω όριο στον αριθμό των κορυφών που αποτελούν το μονοπάτι, δεν μπορούμε να χρησιμοποιήσουμε μια έκφραση με πεπερασμένο το πλήθος υπαρξιακούς ποσοδείκτες π.χ. $\exists x_1 \exists x_2 \ldots \exists x_k$. Όμως οι μεταβλητές μιας πρωτοβάθμιας γλώσσας μπορούν να παίρνουν ως τιμές στοιχεία του συνόλου των κορυφών ενός γράφου (δομής) και όχι υποσύνολα κορυφών. Αυτό το πρόβλημα λύνεται αν επιτρέψουμε ακριβώς αυτό το φαινόμενο.

Ορισμός 4.7 Μια έκφραση της *δευτεροβάθμιας υπαρξιακής λογικής (existential second-order logic)* στο λεξιλόγιο $\Sigma(\Gamma_1)$, είναι της μορφής $\exists P \phi$, όπου ϕ είναι ένας τύπος μιας πρωτοβάθμιας γλώσσας στο λεξιλόγιο $\Sigma(\Gamma_1) \cup P$, δηλαδή που περιέχει και το νεο κατηγορηματικό σύμβολο $P \notin \{P_{n_i} \mid i \in I_n\}$.

Διαισθητικά ο τύπος $\exists P\phi$ σημαίνει ότι υπάρχει μια σχέση P τέτοια που ο τύπος ϕ να ισχύει.

Αν $\mathcal{A}$ είναι μια δομή, τότε ορίζουμε $\mathcal{A} \models \exists P\phi$ ανν υπάρχει σχέση $P^{\mathcal{A}} \subseteq |\mathcal{A}|^{arity(P)}$ τέτοια που αν στον ϕ ερμηνεύσουμε το σύμβολο P με την $P^{\mathcal{A}}$ να ισχύει $\mathcal{A} \models \phi$.

Παραδείγματα 1) Έστω ο τύπος ϕ της δευτεροβάθμιας υπαρξιακής λογικής με $\phi = \exists P \forall x \big((P(x) \vee P(x')) \wedge \neg (P(x) \wedge P(x')) \big)$. Ο τύπος απαιτεί την ύπαρξη ενός συνόλου P τέτοιου που για κάθε x ή $x \in P$ ή $x' = x + 1 \in P$ αλλά όχι και τα δυο. Ο ϕ ικανοποιείται προφανώς από την προτιθέμενη δομή $\mathcal{N}$ για την γλώσσα $\Gamma_1^{\theta\alpha}$ αν πάρουμε ως $P^{\mathcal{N}}$ το σύνολο των άρτιων αριθμών.

2) Ο τύπος $\phi(x,y) = \exists P \Big(\forall u \forall v \forall w \big(P(u,u) \wedge \big(P(u,v) \rightarrow G(u,v) \big) \wedge \big(P(u,v) \wedge P(v,w) \rightarrow P(u,w) \big) \wedge \neg P(x,y) \big) \Big)$ εκφράζει το πρόβλημα UNREACHABILITY.

Δηλώνει ότι υπάρχει ένας γράφος P ο οποίος περιέχει τον G ως υπογράφο, είναι αυτοπαθής και μεταβατικός και επιπλέον στον P δεν υπάρχει ακμή από το x στο y. Όμως κάθε γράφος P που ικανοποιεί αυτές τις τρεις ιδιότητες πρέπει να περιέχει μια ακμή μεταξύ δυο κορυφών του G που συνδέονται με κάποιο μονοπάτι, δηλαδή πρέπει να περιέχει την μεταβατική κλειστότητα του G. Όμως η ιδιότητα $\neg P(x,y)$ συνεπάγεται ότι δεν υπάρχει μονοπάτι από την κορυφή x στην κορυφή y, επομένως το πρόβλημα $\phi(x,y)$-GRAPHS είναι το συμπλήρωμα του REACHABILITY.

Για να εκφράσουμε το REACHABILITY δεν αρκεί να πάρουμε την άρνηση του τύπου $\phi(x,y)$ αφού η δευτεροβάθμια υπαρξιακή λογική δεν είναι απαραίτητα κλειστή ως προς την άρνηση[1]. Έστω γράφος $G = (V, E)$. Για να υπάρχει μονοπάτι από μια κορυφή x σε μια κορυφή y θα πρέπει να ισχύουν τα εξής:

1. να υπάρχει μια γραμμική διάταξη κάποιων κορυφών του γράφου,
2. κάθε δυο διαδοχικές κορυφές στην διάταξη αυτή θα πρέπει να συνδέονται με μια ακμή στον γράφο, και
3. η πρώτη κορυφή να είναι η x και η τελευταία η y.

Έστω P η διμελής σχέση στο σύνολο των κορυφών του γράφου, η οποία ορίζει την διάταξη που ζητάμε. Θα κατασκευάσουμε σταδιακά τον τύπο $\phi_1(x,y) = \exists P \chi$ που θα εκφράζει το REACHABILITY. Ο τύπος x αποτελείται από τους:

[1] Το ερώτημα αν για κάποιον τύπο $\exists P\phi$, υπάρχει τύπος της δευτεροβάθμιας υπαρξιακής λογικής που είναι λογικά ισοδύναμος με τον τύπο $\neg(\exists P\phi)$, είναι ισοδύναμο με το ερώτημα αν **P=co-NP**, του οποίου η απάντηση είναι άγνωστη μέχρι τώρα!

1. $\chi_1 = \forall u \forall v \forall w \big(P(u,v) \wedge P(v,w) \rightarrow P(u,w)\big) \wedge \forall u \forall v \big(P(u,v) \rightarrow \neg P(v,u)\big) \wedge \forall u \neg P(u,u)$,

2. $\chi_2 = \forall u \forall v \Big(\big(P(u,v) \wedge \forall w(\neg P(u,w) \vee \neg P(w,v))\big) \rightarrow G(u,v)\Big)$,

3. $\chi_3 = (\forall u \neg P(u,x)) \wedge (\forall v \neg P(y,v)) \wedge P(x,y)$.

Οι τύποι χ_1, χ_2, χ_3 περιγράφουν τις τρεις ιδιότητες που περιγράψαμε παραπάνω. Τελικά παίρνουμε ως

$$\phi_1(x,y) = \exists P \big(x = y \vee (\chi_1 \wedge \chi_2 \wedge \chi_3)\big).$$

Στην προσπάθεια μας να εκφράσουμε το REACHABILITY, επεκτείναμε την πρωτοβάθμια λογική. Το αποτέλεσμα όμως, όπως φαίνεται στο επόμενο παράδειγμα, είναι να δημιουργήσουμε μια γλώσσα αρκετά ισχυρή ώστε να μπορούμε να εκφράσουμε σε αυτή και προβλήματα για τα οποία δεν υπάρχει (μέχρι τώρα) πολυωνυμικός αλγόριθμος.

Παράδειγμα Έστω τύπος $\psi = \exists P \chi$ όπου ο τύπος χ εκφράζει τις ακόλουθες ιδιότητες:

- η P είναι γραμμική διάταξη των κορυφών ενός γράφου G, δηλαδή είναι ισόμορφη με την $<$ στο G,
- όλες οι διακεκριμμένες κορυφές του G είναι συγκρίσιμες από την P, δηλαδή

$$\forall x \forall y \big(P(x,y) \vee P(y,x) \vee x \approx y\big)$$

- η P είναι μεταβατική αλλά όχι αυτοπαθής, δηλαδή

$$\forall x \forall y \forall z \big(\neg P(x,x) \wedge \big(P(x,y) \wedge P(y,z) \rightarrow P(x,z)\big)\big),$$

- κάθε δυο συνεχόμενες κορυφές στον P πρέπει να είναι γειτονικές στο G, δηλαδή

$$\forall x \forall y \Big(\big(P(x,y) \wedge \forall z \big(\neg P(x,z) \vee \neg P(z,y)\big)\big) \rightarrow G(x,y)\Big).$$

Τότε ο τύπος $\psi = \exists P \chi$ εκφράζει το πρόβλημα HAMILTON PATH.

Θεώρημα 4.6 Για κάθε έκφραση $\exists P \phi$ της δευτεροβάθμιας υπαρξιακής λογικής, το πρόβλημα $\exists P \phi$-GRAPHS είναι στο **NP**.

Απόδειξη Έστω ένας γράφος $G = (V, E)$ με $|V| = n$. Μια αναιτιοκρατική μηχανή Turing μπορεί να μαντέψει μια σχέση $P^G \subseteq V^{arity(P)}$ τέτοια που αν στον ϕ ερμηνεύσουμε το σύμβολο P με την P^G να ισχύει $G \models \phi$, αν υπάρχει τέτοια σχέση. Στην συνέχεια αφού ο τύπος ϕ είναι στην πρωτοβάθμια λογική, η μηχανή μπορεί να χρησιμοποιήσει τον αλγόριθμο του θεωρήματος 4.2 ώστε να ελέγξει σε πολυωνυμικό χρόνο αν $G \models \phi$. Ο συνολικός χρόνος είναι πολυωνυμικός γιατί υπάρχουν το πολύ $n^{arity(P)}$ στοιχεία του P^G για να μαντέψει η μηχανή.

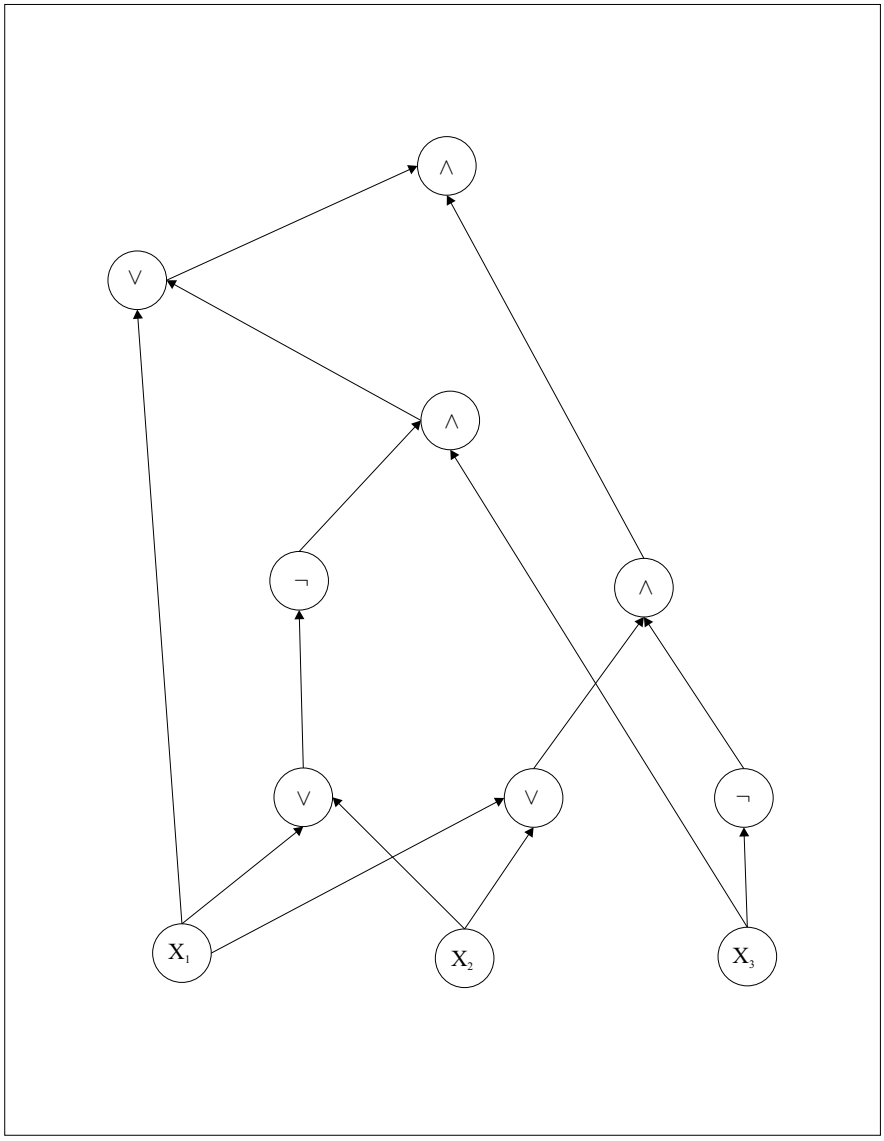
Θα εξετάσουμε μια ειδική μορφή προβλημάτων της μορφής $\exists P\phi$-GRAPHS, ανάλογα με το HORN SAT, τα οποία είναι στο **P**.

Ορισμός 4.8 Ένας τύπος της δευτεροβάθμιας υπαρξιακής λογικής είναι Horn τύπος αν είναι σε κανονική ποσοδεικτική μορφή με μόνο καθολικούς πρωτοβάθμιους ποσοδείκτες και το σώμα του είναι σύζευξη από clauses οι οποίες περιέχουν το πολύ μια θετική εμφάνιση του δευτεροβάθμιου συμβόλου P.

Για παράδειγμα ο τύπος $\phi(x, y)$ που εκφράζει το πρόβλημα UNREACHABILITY είναι ένας Horn τύπος ενώ ο τύπος ψ που εκφράζει το πρόβλημα HAMILTON PATH όχι.

Θεώρημα 4.7 Για κάθε Horn τύπο $\exists P\phi$ της δευτεροβάθμιας υπαρξιακής λογικής, το πρόβλημα $\exists P\phi$-GRAPHS είναι στο **P**.

Σχήμα 3.1 (α)



Σχήμα 3.1 (β)