ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΩΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μεταπτυχιακό Δίπλωμα Ειδίκευσης
"Επιστήμη και Τεχνολογία Υπολογιστών"

Διπλωματική Εργασία

---

# Πρωτόκολλα Πληθυσμών

---

Όθων Σ. Μιχαήλ
Μηχανικός Η/Υ και Πληροφορικής

*Επιβλέπων:*
Παύλος Σπυράκης, Καθηγητής

*Τριμελής Εξεταστική Επιτροπή*
Παύλος Σπυράκης, Καθηγητής
Χρήστος Κακλαμάνης, Καθηγητής
Σωτήρης Νικολετσέας, Επίκουρος Καθηγητής

ΠΑΤΡΑ, ΜΑΡΤΙΟΣ 2009

*Στη Βίκυ και την οικογένειά μου …*

# Πρόλογος

Στην εργασία αυτή επεκτείνουμε το μοντέλο των πρωτοκόλλων πληθυσμών που προτάθηκε από τους Angluin et al. στο [3], ούτως ώστε να μοντελοποιήσουμε πιο ισχυρά δίκτυα αποτελούμενα από πολύ μικρά τεχνουργήματα περιορισμένων πόρων (πράκτορες), τα οποία είναι πιθανόν να ακολουθούν μη-προβλέψιμη παθητική κίνηση. Οι πράκτορες αυτοί επικοινωνούν μόνον κατά ζεύγη σύμφωνα με τις επιλογές ενός εχθρικού δρομολογητή. Ένας κατευθυνόμενος (ή μη-κατευθυνόμενος) γράφος επικοινωνίας αποτυπώνει την ακόλουθη πληροφορία: κάθε ακμή $(u, v)$ του γράφου υποδηλώνει ότι επιτρέπεται κατά τον υπολογισμό να συμβούν μία ή περισσότερες αλληλεπίδρασεις του $u$ με τον $v$ στις οποίες ο $u$ είναι ο μυητής και ο $v$ ο αποκρινόμενος. Το νέο χαρακτηριστικό του μοντέλου των πρωτοκόλλων πληθυσμών με διαμεσολαβητή το οποίο προτείνουμε στην παρούσα εργασία είναι η ύπαρξη ενός παθητικού παρόχου επικοινωνίας τον οποίο καλούμε διαμεσολαβητή.

Ο διαμεσολαβητής είναι μία απλή βάση δεδομένων με δυνατότητες επικοινωνίας. Βασική δουλειά του είναι να διατηρεί τις επιτρεπόμενες αλληλεπιδράσεις σε κλάσεις επικοινωνίας, τον οποίων ο αριθμός είναι σταθερός και ανεξάρτητος του μεγέθους του πληθυσμού. Για τον λόγο αυτό υποθέτουμε ότι κάθε πράκτορας του πληθυσμού έχει έναν μοναδικό προσδιοριστή (ίσως εργοστασιακό) τον οποίο ο ίδιος δεν μπορεί να γνωρίζει. Όταν δύο πράκτορες πρόκειται να αλληλεπιδράσουν αποστέλουν τους μοναδικούς προσδιοριστές τους (ταυτότητες) στον διαμεσολαβητή ο οποίος τους κοινοποιεί την κλάση στην οποία ανήκει το μεταξύ τους κανάλι επικοινωνίας (δηλαδή, την κατάσταση του κατευθυνόμενου ή μη ζεύγους των προσδιοριστών τους) και οι πράκτορες ανανεώνουν την κατάστασή τους και την κατάσταση της μεταξύ τους ακμής βάσει μίας καθολικής συνάρτησης μετάβασης. Εάν η μεταξύ τους αλληλεπίδραση δεν επιτρέπεται ή με άλλα λόγια αν το ζεύγος αυτό δεν υπάρχει στη βάση δεδομένων του διαμεσολαβητή οι πράκτορες ενημερώνονται ότι θα πρέπει να ματαιώσουν την αλληλεπίδραση. Παρατηρούμε ότι με τον τρόπο αυτό αρχίζουμε να αποκτούμε κάποιον έλεγχο σχετικά με την ασφάλεια του δικτύου και επιπλέον μέσω του διαμεσολαβητή μπορούμε ανά πάσα στιγμή να γνωρίζουμε την τοπολογία του δικτύου.

Ισοδύναμα, είναι σα να επιτρέπουμε στις ακμές του γράφου επικοινωνίας να έχουν καταστάσεις από ένα σύνολο καταστάσεων ακμών σταθερού πληθικού αριθμού. Ο εναλλακτικός αυτός τρόπος να δούμε το νέο μοντέλο έχει πολλά πλεονεκτήματα ως προς την τυπική μοντελοποίηση και τον σχεδιασμό πρωτοκόλλων αφού μας επιτρέπει να παραβλέψουμε τις λεπτομέρειες υλοποίησης του διαμεσολαβητή. Επιπρόσθετα, επεκτείνουμε περαιτέρω το νέο μοντέλο επιτρέποντας στις ακμές να έχουν κόστη από ένα επίσης σταθερού πληθικού αριθμού σύνολο τα οποία είναι μόνο προς ανάγνωση. Εν συνεχεία επιτρέπουμε τους κανόνες μεταβάσεων των εκάστοτε πρωτοκόλλων να διαβάζουν τις καταστάσεις του ζεύγους πρακτόρων που αλληλεπιδρούν και την κατάσταση και το κόστος της ακμής μέσω της οποίας γίνεται η αλληλεπίδραση (αν, φυσικά, έχουμε ορίσει κόστη στο πρόβλημά μας) και να ανανεώνουν όλα αυτά τα στοιχεία πέραν από τα κόστη που είναι μόνο προς ανάγνωση. Παρατηρούμε, επομένως, ότι οι προδιαγραφές των πρωτοκόλλων του νέου μοντέλου συνεχίζουν, όπως και στο [3], να είναι ανεξάρτητες του μεγέθους του πληθυσμού και συνεχίζουν να μην χρησιμοποιούν μοναδικούς προσδιοριστές, δηλαδή, το νέο μοντέλο διατηρεί τα χαρακτηριστικά της κλιμάκωσης, της ομοιομορφίας και της ανωνυμίας.

Τα Πρωτόκολλα Πληθυσμών με Διαμεσολαβητή (Mediated Population Protocols - MPP) που προτείνουμε μπορούν να υπολογίσουν σταθερά ιδιότητες γράφων σχετικά με τον γράφο επικοινωνίας. Για να το δείξουμε αυτό παρουσιάζουμε πρωτόκολλα για το μεγιστοτικό ταίριασμα, την μεταβατική θήκη, τις ακμές ελαχίστου κόστους και το ελάχιστο μονοπάτι από τη ρίζα ως τα φύλλα ενός έξω-κατευθυνόμενου δέντρου και αποδεικνύουμε την ορθότητά τους.

Εν συνεχεία, δείχνουμε ότι το μοντέλο των πρωτοκόλλων με διαμεσολαβητή αποτελεί ένα ισχυρότερο υπολογιστικά μοντέλο από το κλασικό μοντέλο των πρωτοκόλλων πληθυσμών. Πρώτα παρατηρούμε το προφανές, ότι, δηλαδή, το κλασικό μοντέλο των πρωτοκόλλων πληθυσμών είναι ειδική περίπτωση του νέου μοντέλου, άρα το νέο μοντέλο μπορεί να κάνει σίγουρα τουλάχιστον ότι και το κλασικό. Εν συνεχεία παρουσιάζουμε ένα πρωτόκολλο με διαμεσολαβητή το οποίο υπολογίζει σταθερά το γινόμενο δύο θετικών ακεραίων στην περίπτωση που ο $G$ (γράφος επικοινωνίας) είναι πλήρης κατευθυνόμενος και συνεκτικός. Τα κατηγορήματα που περιλαμβάνουν πολλαπλασιασμό δύο ακεραίων μεταβλητών δεν είναι ημιγραμμικά και στο [6] έχει αποδειχθεί ότι τα κλασικά πρωτόκολλα πληθυσμών σε πλήρεις γράφους υπολογίζουν σταθερά μονον ημιγραμμικά κατηγορήματα, άρα με τον τρόπο αυτό δείχνουμε ότι υπάρχει τουλάχιστον ένα κατηγόρημα που ενώ δεν υπολογίζεται σταθερά απ' το βασικό μοντέλο υπολογίζεται σταθερά από το μοντέλο το οποίο προτείνουμε. Για τις ανάγκες της απόδειξης διατυπώνουμε και αποδεικνύουμε ένα γενικό Θεώρημα σχετικά με τη σύνθεση δύο πρωτοκόλλων πληθυσμών με διαμεσολαβητή, το ένα εκ των οποίων χρησιμοποιεί σταθεροποιούμενες εισόδους.

Δείχνουμε, επίσης, ότι όλα τα κατηγορήματα που υπολογίζονται σταθερά απ' το μοντέλο μας ανήκουν (μη-ομοιόμορφα) στην κλάση $NSPACE(m)$, όπου το $m$ συμβολίζει το πλήθος των ακμών του γράφου επικοινωνίας. Τέλος, ορίζουμε τα πιθανοτικά πρωτόκολλα πληθυσμών με διαμεσολαβητή, στα οποία ο δρομολογητής επιλέγει σε κάθε βήμα την επόμενη αλληλεπίδραση ισοπίθανα μεταξύ των ακμών του γράφου επικοινωνίας και δείχνουμε ότι κάθε Peano κατηγόρημα που υπολογίζεται σταθερά από ένα πιθανοτικό MPP μπορεί να επαληθευτεί σε αιτιοκρατικό πολυωνυμικό χρόνο.

Θα ήθελα να ευχαριστήσω τον κ. Ιωάννη Χατζηγιαννάκη, τα μέλη της τριμελούς επιτροπής αξιολόγησης της παρούσας εργασίας κ.κ. Χρήστο Κακλαμάνη και Σωτήρη Νικολετσέα και ιδιαίτερα τον επιβλέποντα Καθηγητή κ. Παύλο Σπυράκη για την εμπιστοσύνη που μου έδειξε, για τον πολύτιμο χρόνο που σπατάλησε στις, για εμένα, πολύτιμες συζητήσεις μας και για το γεγονός ότι με έκανε να εκτιμήσω την αξία και να δω την ομορφιά της μαθηματικής θεμελίωσης των εκάστοτε τεχνολογιών.

Όθων Σ. Μιχαήλ
Πάτρα, Μάρτιος 2009

# Περιεχόμενα

# Κεφάλαιο 1

# Εισαγωγή

*Η αρχή είναι το ήμισυ του παντός.*

## 1.1 Παραδοσιακά Κατανεμημένα Συστήματα

Στα παραδοσιακά *κατανεμημένα συστήματα* η συνήθης υπόθεση είναι ότι κάθε πράκτορας του συστήματος, δηλαδή κάθε ανεξάρτητη υπολογιστική μονάδα (πιθανώς εφοδιασμένη με κάποιους αισθητήρες), είναι τόσο υπολογιστικά ισχυρή όσο και μία αιτιοκρατική (ντετερμινιστική) μηχανή Turing. Επομένως, στα παραδοσιακά κατανεμημένα συστήματα φανταζόμαστε μία συλλογή αυτόνομων υπολογιστών (ισχυρών υπολογιστικών μονάδων) που μέσω κάποιας δικτύωσης μπορούν να επικοινωνούν μεταξύ τους (π.χ. μπορεί να ανταλλάσσουν μηνύματα μέσω καλωδίων).

Τα κατανεμημένα συστήματα χρησιμοποιούνται καθημερινά στο χώρο των επιχειρήσεων, της εκπαίδευσης, της δημόσιας διοίκησης αλλά ακόμα και στο σπίτι, ιδιαίτερα στις μέρες μας, όπου ο παγκόσμιος ιστός επιτρέπει την πρόσβαση σε δεδομένα ανεξαρτήτως της γεωγραφικής τους τοποθεσίας. Οι θεμελιώδεις δυσκολίες που πρέπει να αντιμετωπιστούν από ένα κατανεμημένο σύστημα σχετίζονται κυρίως με τους ακόλουθους παράγοντες:

- *Ασύγχρονη εκτέλεση διεργασιών*: το ετερογενές περιβάλλον εκτέλεσης των διεργασιών δεν επιτρέπει τον απόλυτο ή έστω και σχετικό εντοπισμό της χρονικής στιγμής εμφάνισης συγκεκριμένων καταστάσεων του συστήματος.

- *Περιορισμένη τοπική γνώση*: εφόσον κάθε υπολογιστική μονάδα είναι ενήμερη μόνο για τις πληροφορίες που μπορεί να προσπελάσει, διαθέτει μια σαφώς περιορισμένη οπτική εικόνα της συνολικής κατάστασης τους συστήματος.

- *Σφάλματα*: κάθε μια από τις υπολογιστικές μονάδες που αποτελούν το σύστημα μπορεί να αντιμετωπίσει κάποιο σφάλμα, θέτοντας ορισμένες μονάδες εκτός λειτουργίας.

Η *Θεωρία του Κατανεμημένου Υπολογισμού* έχει ως βασικό στόχο την επίτευξη ενός πλαισίου εργασίας για τα κατανεμημένα συστήματα μέσω του οποίου θα μπορέσουμε να εντοπίσουμε τα θεμελιώδη προβλήματα που εμφανίζονται στην πλειοψηφία των καταστάσεων που αντιμετωπίζουν τα κατανεμημένα συστήματα και να επιχειρήσουμε να τα ορίσουμε με σαφήνεια. Επομένως, μας δίνεται η δυνατότητα να σχεδιάσουμε και να αναλύσουμε την απόδοση αλγοριθμικών λύσεων για την επίλυση των προβλημάτων και να αποδείξουμε την ορθότητα και βέλτιστη λειτουργία τους. Με άλλα λόγια, επιχειρούμε να μοντελοποιήσουμε σε ένα αφαιρετικό θεωρητικό πλαίσιο τα συστήματα αυτά, έτσι ώστε να μπορέσουμε να καταλήξουμε σε ορισμένα καθολικά και αποδεδειγμένα συμπεράσματα σχετικά με την εγγενή πολυπλοκότητά τους και τις υπολογιστικές τους δυνατότητες, κατά τρόπο ανάλογο με αυτόν που ακολουθήθηκε (και συνεχίζει να ακολουθείται μέχρι και σήμερα) για τους συμβατικούς υπολογιστές.

## 1.2 Δίκτυα Αισθητήρων

Η σύγχρονη πρόοδος στην τεχνολογία των μικρο-ελεκτρο-μηχανικών συστημάτων (MEMS), των ασύρματων επικοινωνιών και της ψηφιακής ηλεκτρονικής έχει καταστήσει δυνατή την ανάπτυξη κόμβων αίσθησης χαμηλού κόστους (λιγότερο από 1$ Ηνωμένων Πολιτειών ανά τεμάχιο), χαμηλής κατανάλωσης ενέργειας που μπορούν να επιτελούν πολλές λειτουργίες. Οι αισθητήρες αυτοί έχουν πολύ μικρό μέγεθος (π.χ. στόχος του προγράμματος SmartDust ήταν το μέγεθος αυτό να μην ξεπερνάει τα λίγα τετραγωνικά χιλιοστά) και έχουν δυνατότητες τοπικής ασύρματης επικοινωνίας. Αυτοί οι τόσο μικροί κόμβοι αίσθησης έχουν κάνει εφικτή και πραγματοποιήσιμη τη δημιουργία *δικτύων αισθητήρων* τα οποία βασίζουν τη λειτουργικότητά τους στην συνεργασία ενός μεγάλου αριθμού τέτοιων κόμβων.

Ένας κόμβος αίσθησης αποτελείται από πέντε κύριες συνιστώσες:

- Έναν *ελεγκτή* (κεντρική μονάδα επεξεργασίας του κόμβου) για να επεξεργάζεται όλα τα σχετικά δεδομένα και να μπορεί να εκτελεί κώδικά.

- Κάποια *μνήμη* για να αποθηκεύει προγράμματα και ενδιάμεσα δεδομένα· συνήθως, διαφορετικοί τύποι μνήμης χρησιμοποιούνται για τα προγράμματα και τα δεδομένα.

- *Αισθητήρες* και *μηχανισμούς κίνησης* που αποτελούν τα μέσα αλληλεπίδρασης του κόμβου με τον έξω κόσμο: είναι συσκευές που παρατηρούν ή ελέγχουν φυσικές παραμέτρους του περιβάλλοντος.

- Κάποιο μηχανισμό *επικοινωνίας*: η δικτύωση των κόμβων απαιτεί την ενσωμάτωση σε αυτούς κάποιας συσκευής που να έχει τη δυνατότητα αποστολής και λήψης πληροφορίας μέσω ενός ασύρματου καναλιού.

- *Παροχή ισχύος*: Συνήθως, οι κόμβοι δεν έχουν κάποια σταθερή παροχή ισχύος (σε ορισμένες εφαρμογές μπορεί να είναι δυνατή η ύπαρξη ηλιακών κυψελών ή άλλων μηχανισμών περιορισμένης άντλησης ενέργειας από το περιβάλλον) και ως εκ τούτου είναι απαραίτητη η ύπαρξη κάποιου τύπου ενσωματωμένης μπαταρίας για την παροχή ενέργειας στον κόμβο.

Η γενική ιδέα είναι ότι ένας μεγάλος αριθμός κόμβων αίσθησης τοποθετείται σε κάποιο περιβάλλον (π.χ. δάσος, ποτάμι, κτίριο κ.ο.κ.) για να παρατηρεί ορισμένες παραμέτρους του περιβάλλοντος. Οι κόμβοι χρησιμοποιούν τους αισθητήρες και τους μηχανισμούς κίνησης τους οποίους διαθέτουν για να αλληλεπιδρούν με το περιβάλλον και επικοινωνούν μεταξύ τους και με κάποιο σταθμό βάσης ο οποίος συλλέγει τα δεδομένα των παρατηρήσεων και των υπολογισμών του συστήματος (δικτύου). Για παράδειγμα, μπορούμε να φανταστούμε την ρίψη μεγάλου πλήθους αισθητήρων, από αέρος, σε ένα δάσος με σκοπό την δημιουργία ενός δικτύου που θα αναλάβει να σημαίνει συναγερμό εάν ανιχνευτεί πυρκαγιά στο δάσος.

Επομένως, ένα δίκτυο αισθητήρων μπορούμε να πούμε ότι αποτελείται από ένα μεγάλο αριθμό κόμβων αίσθησης οι οποίοι παρατάσσονται είτε εντός του φαινομένου (π.χ. εντός ενός εργοστασίου με διαρροή ραδιενέργειας) είτε πολύ κοντά σε αυτό. Η ακριβής θέση των κόμβων δεν οφείλει απαραίτητα να είναι προσχεδιασμένη. Αυτό επιτρέπει την τυχαία διασπορά σε μη-προσβάσιμες περιοχές ή περιοχές που έχουν πληγεί από κάποια καταστροφή. Από την άλλη μεριά, αυτό σημαίνει επίσης ότι τα πρωτόκολλα και οι αλγόριθμοι που σχεδιάζονται για δίκτυα αισθητήρων θα πρέπει να διαθέτουν ικανότητες αυτοοργάνωσης. Ένα άλλο μοναδικό χαρακτηριστικό των δικτύων αισθητήρων είναι η συνεργατική τους λειτουργία. Καθώς οι κόμβοι είναι εφοδιασμένοι με επεξεργαστικές μονάδες, αντί να αποστέλλουν όλα τα δεδομένα στο σταθμό βάσης για επεξεργασία, αναλαμβάνουν με κατανεμημένο τρόπο να εκτελούν απλούς υπολογισμούς (συνεργατικά) και αποστέλλουν μόνο τα απαραίτητα και τα μερικώς επεξεργασμένα δεδομένα στη βάση.

Τα δίκτυα αισθητήρων βρίσκουν πληθώρα εφαρμογών. Κάποιες από αυτές είναι η υγεία, η διευκόλυνση της καθημερινής ζωής των ανθρώπων (π.χ. έξυπνα κτίρια), η εξοικονόμηση ενέργειας, οι στρατιωτικές επιχειρήσεις και

η ασφάλεια. Ως ένα παράδειγμα αξίζει να αναφέρουμε την ιδέα των έξυπνων κτιρίων. Είναι γεγονός ότι τα σύγχρονα κτίρια σπαταλούν τεράστιες ποσότητες ενέργειας λόγω μη-αποδοτικής κατασκευής ως προς την υγρασία, τον εξαερισμό και τον κλιματισμό. Ένα δίκτυο αισθητήρων μπορεί να χρησιμοποιηθεί για να ελέγχει όλες αυτές τις παραμέτρους και να τις ρυθμίζει ανάλογα με τις ανάγκες. Υπολογίζεται ότι με τη χρήση τέτοιων συστημάτων θα εξοικονομηθούν μόνο στις ΗΠΑ δύο τετράκις εκατομμύρια θερμικές μονάδες. Στην ουσία, τα δίκτυα αισθητήρων είναι σε θέση να παρέχουν στον τελικό χρήστη επιπρόσθετη ευφυία και καλύτερη κατανόηση του εκάστοτε περιβάλλοντος. Το όραμα είναι ότι στο μέλλον τα ασύρματα δίκτυα αισθητήρων θα αποτελούν ένα αναπόσπαστο κομμάτι της καθημερινής ζωής των ανθρώπων, ίσως σε μεγαλύτερο βαθμό απ' ότι οι σημερινοί συμβατικοί υπολογιστές.

Η πραγματοποίηση τέτοιων εφαρμογών απαιτεί τη χρήση ασύρματων τεχνικών ad hoc δικτύωσης. Παρότι πληθώρα πρωτοκόλλων και αλγορίθμων έχει προταθεί για τα παραδοσιακά ασύρματα ad hoc δίκτυα, αυτά δεν ικανοποιούν τα μοναδικά χαρακτηριστικά και τις απαιτήσεις των εφαρμογών των δικτύων αισθητήρων. Οι βασικές διαφορές των δύο τεχνολογιών είναι οι εξής:

- Το πλήθος των κόμβων σε ένα δίκτυο αισθητήρων είναι αρκετές τάξεις μεγέθους μεγαλύτερο.
- Οι κόμβοι αίσθησης παρατάσσονται σε πυκνή διάταξη.
- Οι κόμβοι αίσθησης είναι επιρεπείς σε σφάλματα και βλάβες.
- Η τοπολογία ενός δικτύου αισθητήρων μεταβάλλεται πολύ συχνά.
- Οι κόμβοι αίσθησης έχουν πολύ περιορισμένη ενέργεια, μνήμη και υπολογιστικές δυνατότητες.
- Οι κόμβοι αίσθησης μπορεί να μην έχουν μοναδικούς προσδιοριστές (IDs) λόγω του μεγάλου τους πλήθους (θα απαιτούνταν μεγάλες αποθηκευτικές δυνατότητες).

## 1.3 Πρωτόκολλα Πληθυσμών

Όπως είδαμε, οι κατανεμημένοι αλγόριθμοι για τα παραδοσιακά κατανεμημένα συστήματα υποθέτουν ότι οι επιμέρους πράκτορες που αποτελούν το σύστημα είναι υπολογιστικά ισχυροί, ικανοί να αποθηκεύουν μη-τετριμμένη ποσότητα δεδομένων και να εκτελούν σύνθετους υπολογισμούς. Σε συστήματα όμως που αποτελούνται από τεράστιο πλήθος φτηνών και μικρών πρακτόρων οι πόροι που είναι διαθέσιμοι σε κάθε πράκτορα μπορεί να είναι

ισχυρά περιορισμένοι. Τέτοιοι περιορισμοί δεν είναι απαγορευτικοί εάν ο κατασκευαστής του συστήματος μπορεί να ελέγχει τον τρόπο με τον οποίο διεξάγονται οι αλληλεπιδράσεις μεταξύ των πρακτόρων. Στην περίπτωση αυτή τα συστήματα μπορούν ακόμα και να προσομοιώσουν μηχανές Turing γραμμικού χώρου. Εάν όμως οι αλληλεπιδράσεις αυτές δεν υπόκεινται σε έλεγχο, π.χ. εάν διεξάγονται με τυχαίο τρόπο λόγω της τυχαίας κίνησης στην οποία αναγκάζει το περιβάλλον τους πράκτορες, τότε σε αυτή την περίπτωση δεν είναι προφανές ποια είναι τα υπολογιστικά όρια.

Τα δίκτυα αισθητήρων, που συζητήσαμε στην προηγούμενη ενότητα, είναι ένα κλασικό παράδειγμα αυτού του φαινομένου. Κάθε κόμβος αίσθησης έχει μεγάλους περιορισμούς σχετικά με την παρεχόμενη ισχύ, την αποθηκευτική και υπολογιστική ικανότητα και τις δυνατότητες επικοινωνίας λόγω της ανάγκης να κρατηθούν το κόστος και το μέγεθος κάθε κόμβου σε πολύ μικρά επίπεδα. Η έρευνα στο πεδίο των δικτύων αισθητήρων έχει αρχίσει να επικεντρώνεται στην χρήση δυνατοτήτων κατανεμημένου υπολογισμού με στόχο τη μείωση του κόστους επικοινωνίας. Παρότι συνήθως υποθέτουμε ότι οι κόμβοι αίσθησης είναι στατικοί ή σχεδόν στατικοί, γεγονός που επιτρέπει την εφαρμογή στρατηγικών που βασίζονται σε σταθερή δρομολόγηση, η υπόθεση αυτή δεν είναι καθολική στην βιβλιογραφία των δικτύων αισθητήρων.

Το βασικό ερώτημα που τίθεται είναι τί υπολογισμούς μπορεί να φέρει σε πέρας ένα συνεργατικό δίκτυο παθητικά κινούμενων πεπερασμένων αυτομάτων με δυνατότητα αίσθησης του περιβάλλοντός τους. Με άλλα λόγια, θεωρούμε ότι κάθε κόμβος αίσθησης είναι ένα πεπερασμένο αυτόματο που μπορεί να αισθάνεται το περιβάλλον του. Το ότι ο κόμβος είναι μία τόσο ασήμαντη υπολογιστική συσκευή αντικατοπτρίζει την απλότητα και το χαμηλό κόστος που πρέπει να διέπει τους κόμβους αίσθησης στα δίκτυα αισθητήρων. Αυτού του είδους οι πράκτορες υποθέτουμε ότι βρίσκονται σε διαρκή, μη-προβλέψιμη κίνηση (π.χ. κάθε μέλισσα μίας κυψέλης εφοδιασμένη με έναν τέτοιο πράκτορα) και επικοινωνούν κατά ζεύγη όταν δύο τέτοιοι πράκτορες έρχονται σε επαφή ή σε πολύ κοντινή απόσταση. Φυσικά, κάθε τέτοιο πεπερασμένο αυτόματο θεωρούμε ότι μπορεί να αποθηκεύει μόνο δεδομένα σταθερού μεγέθους, ανεξάρτητα δηλαδή απ' το μέγεθος του πληθυσμού. Έτσι, οι προδιαγραφές των πρωτοκόλλων πρέπει να είναι σταθερές και ανεξάρτητες του μεγέθους του πληθυσμού και επιπλέον τα πρωτόκολλα πρέπει να είναι ανώνυμα αφού η σταθερή μνήμη των πρακτόρων δεν επιτρέπει την χρήση μοναδικών προσδιοριστών.

Επιπλέον, τί υπολογισμούς μπορεί να φέρει σε πέρας ένα τέτοιο σύστημα με την επιπλέον δυνατότητα αποθήκευσης πληροφορίας στα κανάλια επικοινωνίας; Αυτό μπορεί να σημαίνει είτε ότι οι πράκτορες μπορούν να αποθηκεύουν στα κανάλια επικοινωνίας κάποια από κοινού πληροφορία ανά ζεύγη την οποία διαβάζουν και ανανεώνουν σε κάθε αλληλεπίδρασή τους, είτε ότι

υπάρχει κάποιος παθητικός πάροχος επικοινωνίας, π.χ. κάποιος σταθμός βάσης, ο οποίος κρατάει τις επιτρεπόμενες αλληλεπιδράσεις σε κλάσεις επικοινωνίας των οποίων τα περιεχόμενα ανανεώνει ανάλογα με τα αποτελέσματα των αλληλεπιδράσεων.

Στην παρούσα εργασία θα ασχοληθούμε με αυτού του τύπου τα συστήματα ακολουθώντας την θεμελιώδη προσέγγιση, προσπαθώντας, δηλαδή, να ορίσουμε αφαιρετικά και ρεαλιστικά μοντέλα έτσι ώστε να δώσουμε αυστηρές μαθηματικές απαντήσεις στα παραπάνω ερωτήματα.

# Κεφάλαιο 2

# Το Μοντέλο των Πρωτοκόλλων Πληθυσμών

*Πολλά μπορούν να συμβούν όταν κάθε ψάρι εφοδιάζεται με ένα πεπερασμένο αυτόματο που μπορεί να επικοινωνεί.*

## 2.1 Νέας μορφής υπολογιστικά συστήματα

Ο ιδιοκτήτης ενός ιχθυοτροφείου βρίσκεται σε απόγνωση. Αρκετά συχνά, τα ψάρια του προσβάλλονται από έναν ιό $J$ ο οποίος μεταδίδεται σε μεγάλο μέρος του πληθυσμού. Τα μολυσμένα ψάρια δεν μπορούν να διοχετευτούν στην αγορά. Υπάρχει φάρμακο κατά του $J$, το οποίο, όμως, είναι πολύ ακριβό, με αποτέλεσμα η χορήγησή του να συμφέρει μόνο εάν έχει μολυνθεί τουλάχιστον το $5\%$ του πληθυσμού. Επιπλέον, τα ψάρια παρουσιάζουν αμφιλεγόμενα συμπτώματα και μόνον ένας ειδικός (φθηνός) αισθητήρας ανίχνευσης που εμφυτεύεται στο ψάρι μπορεί να διαπιστώσει με βεβαιότητα τη μόλυνση απ' τον $J$. Τί λύση μπορεί να προτείνει η σύγχρονη τεχνολογία σε τέτοιου είδους καθημερινά, και όχι μόνο, προβλήματα;

Ας υποθέσουμε ότι κάθε ψάρι εφοδιάζεται με έναν πολύ φθηνό και μικρό *πράκτορα*. Κάθε πράκτορας αποτελείται από έναν αισθητήρα ανίχνευσης του $J$, έναν επεξεργαστή, μία μνήμη σταθερού μεγέθους $k = \mathcal{O}(1)$ (με σταθερό αριθμό κελιών), έναν χαμηλής-ισχύος μηχανισμό τοπικής ασύρματης επικοινωνίας που του επιτρέπει να επικοινωνεί με τους άλλους πράκτορες (όταν η μεταξύ τους απόσταση είναι επαρκώς μικρή) και μία μπαταρία.

Για να διευκολύνουμε τη συζήτηση, ας υποθέσουμε αρχικά ότι ο ιδιοκτήτης του ιχθυοτροφείου ενδιαφέρεται για το εάν τουλάχιστον $100$ ψάρια έχουν μολυνθεί. Υπάρχει ένα πολύ απλό *πρωτόκολλο* που λύνει το πρόβλημα αυτό και που μπορεί να τρέξει στο σύστημα που υποθέσαμε. Η ιδέα είναι ότι ό-

ταν οι πράκτορες λάβουν ένα καθολικό σήμα εκκίνησης, οι αισθητήρες τους πραγματοποιούν τον έλεγχο ύπαρξης του ιού $J$. Αν ένας αισθητήρας ανιχνεύσει τον ιό γράφει το σύμβολο 1 στη μνήμη του πράκτορά του, αλλιώς γράφει το σύμβολο 0. Μόλις πραγματοποιηθεί η εγγραφή του συμβόλου εισόδου στη μνήμη, ο πράκτορας το διαβάζει και, αν είναι 1, το μετατρέπει στην κατάσταση $q_1$, αλλιώς στην κατάσταση $q_0$. Ο πράκτορας πλέον είναι στην *κατάσταση υπολογισμού*. Όταν δύο πράκτορες που είναι στην κατάσταση υπολογισμού με καταστάσεις $q_i$ και $q_j$ συναντηθούν (λόγω του ότι τα ψάρια-φορείς τους πλησίασαν το ένα το άλλο), τότε αν $i + j < 100$ ο ένας πράκτορας περνάει στην κατάσταση $q_{i+j}$ και ο άλλος στην $q_0$. Αντίθετα, αν $i + j \geq 100$ τότε και οι δύο πράκτορες περνούν στην κατάσταση $q_{100}$. Διαισθητικά, οι πράκτορες τείνουν να συγκεντρώσουν το άθροισμα των μετρήσεών τους σε ένα μόνο πράκτορα, αν όμως κάποια στιγμή αλληλεπιδράσουν δύο πράκτορες που το άθροισμα των δεικτών των καταστάσεών τους είναι τουλάχιστον $100$, τότε και οι δύο περνούν στην κατάσταση συναγερμού $q_{100}$ η οποία διαδίδεται εν συνεχεία σε κάθε πράκτορα που την συναντάει. Είναι εύκολο να διαπιστώσει κανείς ότι, αν οι συναντήσεις των ψαριών διεξάγονται με *δίκαιο τρόπο*, η $q_{100}$ θα εμφανιστεί και θα κατακλύσει το δίκτυο εάν και μόνον εάν τουλάχιστον $100$ αισθητήρες ανίχνευσαν αρχικά τον ιό $J$, με άλλα λόγια εάν και μόνον εάν τουλάχιστον $100$ ψάρια του πληθυσμού έχουν μολυνθεί. Η τιμή εξόδου ενός πράκτορα είναι 1 αν ο πράκτορας είναι στην κατάσταση $q_{100}$ και 0 αν ο πράκτορας είναι σε οποιαδήποτε άλλη κατάσταση. Έτσι, ο ιδιοκτήτης του ιχθυοτροφείου μετά από κάποιο επαρκές χρονικό διάστημα μπορεί να λάβει την ορθή απάντηση από οποιονδήποτε πράκτορα του πληθυσμού.

Για να καταλάβει κανείς τί εννοούμε όταν λέμε ότι οι συναντήσεις πρέπει να διεξάγονται κατά δίκαιο τρόπο, αρκεί να σκεφτεί τί θα γινόταν αν δεν συνέβαινε αυτό. Για παράδειγμα, έστω ότι ένα ψάρι είναι πολύ άγριο με αποτέλεσμα τα υπόλοιπα να μην το πλησιάζουν ποτέ, ενώ το ίδιο περνάει συνεχώς την ώρα του ακίνητο σε μία άκρη του ιχθυοτροφείου. Το ψάρι αυτό είναι μολυσμένο από τον $J$ (έχει μολυνθεί μέσω του νερού) όπως και 99 άλλα ψάρια. Όμως, επειδή δεν επικοινωνεί με τον υπόλοιπο πληθυσμό, η μέτρηση του πράκτορά του δεν γίνεται να αθροιστεί με τις υπόλοιπες μετρήσεις και, έτσι, το σύστημα θα καταλήξει εσφαλμένα στο συμπέρασμα ότι μόνον 99 ψάρια έχουν μολυνθεί. Το παράδειγμα καταδεικνύει ότι για την διεξαγωγή οποιασδήποτε μορφής ορθού υπολογισμού σε τέτοια συστήματα, είμαστε αναγκασμένοι να υποθέσουμε ότι οι αλληλεπιδράσεις διεξάγονται κατά δίκαιο τρόπο και να ορίσουμε τί εννοούμε με αυτό. Τον αυστηρό ορισμό θα τον επιχειρήσουμε αργότερα, όταν θα δώσουμε τον τυπικό ορισμό του υπολογιστικού μοντέλου.

Παρατηρούμε ότι οι ίδιοι οι πράκτορες δεν ελέγχουν την κίνηση στην οποία υπόκεινται. Αντ' αυτού, είναι αναγκασμένοι να ακολουθούν την τροχιά

που διαγράφει ο φορέας τους (το ψάρι) και λέμε ότι είναι *παθητικά κινούμενοι*. Η παθητική αυτή κίνηση μπορεί να μοντελοποιηθεί μέσω της υπόθεσης ενός *εχθρικού δρομολογητή*. Υποθέτουμε ότι ο δρομολογητής είναι δίκαιος. Το "εχθρικός" χαρακτηρίζει το γεγονός ότι οι πράκτορες δεν έχουν κανέναν έλεγχο πάνω στην κίνηση που τους επιβάλλει ο δρομολογητής. Ο δρομολογητής επιλέγει το ένα μετά το άλλο τα ζεύγη των πρακτόρων που θα αλληλεπιδράσουν καθορίζοντας κάθε φορά ποιος πράκτορας είναι ο *μυητής* και ποιος ο *αποκρινόμενος*. Για παράδειγμα, όταν αλληλεπιδρά το ζεύγος πρακτόρων $(u, v)$, ο $u$ είναι ο μυητής και ο $v$ ο αποκρινόμενος ενώ στο ζεύγος $(v, u)$ οι ρόλοι είναι αντίστροφοι.

Χρησιμοποιούμε έναν κατευθυνόμενο *γράφο επικοινωνίας* $G = (V, E)$ χωρίς πολλαπλές ακμές και βρόχους, για να αναπαραστήσουμε τις επιτρεπόμενες αλληλεπιδράσεις. Το $V$ αναπαριστά έναν πληθυσμό $|V| = n$ πρακτόρων, ενώ κάθε $e = (u, v) \in E$ υποδηλώνει ότι κατά τη διάρκεια του υπολογισμού μπορεί να συμβεί μία αλληλεπίδραση στην οποία ο $u$ είναι ο μυητής και ο $v$ ο αποκρινόμενος. Το πλήθος των ακμών θα συμβολίζεται με το γράμμα $m$. Αρχικά, θα υποθέσουμε ότι ο γράφος επικοινωνίας είναι πλήρης και αργότερα θα χαλαρώσουμε αυτή την υπόθεση, οπότε και θα μιλήσουμε για *γράφους περιορισμένων αλληλεπιδράσεων*.

**Ορισμός 1.** *Η όλων-των-ζευγών οικογένεια κατευθυνόμενων γράφων επικοινωνίας συμβολίζεται ως $\mathcal{G}_{all}^{d}$ και περιλαμβάνει για κάθε $n$ τον πλήρη γράφο με $n$ κόμβους.*

Έχοντας ορίσει τον γράφο επικοινωνίας μπορούμε να υποθέσουμε ότι ο δρομολογητής επιλέγει ακμές και σε κάθε τέτοια επιλογή οι πράκτορες που αλληλεπιδρούν είναι τα άκρα της ακμής με ρόλους που καθορίζονται από την φορά της. Παρατηρούμε ότι σε κάθε $G \in \mathcal{G}_{all}^{d}$ ο δρομολογητής μπορεί να επιλέξει για αλληλεπίδραση οποιοδήποτε στοιχείο του $V \times V$.

Ας επιχειρήσουμε μία σύντομη ανακεφαλαίωση πριν δώσουμε τον τυπικό ορισμό του μοντέλου των πρωτοκόλλων πληθυσμών. Υποθέτουμε ότι ένας πληθυσμός ισχυρά περιορισμένων υπολογιστικών συσκευών (πρακτόρων) βρίσκεται σε διαρκή κίνηση σύμφωνα με τις επιθυμίες ενός δρομολογητή. Κάθε πράκτορας διαθέτει μία σταθερή περιορισμένη μνήμη και ως εκ τούτου μπορεί να μοντελοποιηθεί ως ένα πεπερασμένο αυτόματο. Οι πράκτορες τρέχουν ένα καθολικό πρόγραμμα (πρωτόκολλο) του οποίου η περιγραφή πρέπει να είναι σταθερή και ανεξάρτητη του μεγέθους του πληθυσμού, έτσι ώστε να χωράει στη μνήμη κάθε πράκτορα. Μόλις οι πράκτορες λάβουν ένα καθολικό σήμα εκκίνησης, αισθάνονται το περιβάλλον τους και αποκτούν μια τιμή εισόδου την οποία μετατρέπουν σε κάποια αρχική κατάσταση. Όταν ο δρομολογητής επιλέξει κάποιο ζεύγος πρακτόρων $(u, v)$ για να αλληλεπιδράσουν, με τον $u$ στην κατάσταση $a$ και τον $v$ στην $b$, τότε το πρόγραμμά

τους παίρνει ως είσοδο το διατεταγμένο ζεύγος των καταστάσεών τους $(a, b)$ και παράγει ένα νέο διατεταγμένο ζεύγος $(a', b')$. Τώρα η κατάσταση $a$ του μυητή $u$ αντικαθίσταται από την $a'$ ενώ η κατάσταση $b$ του αποκρινόμενου $v$ αντικαθίσταται από την $b'$.

## 2.2 Τυπικός ορισμός του μοντέλου

Ένα *πρωτόκολλο πληθυσμού* $\mathcal{A}$ αποτελείται από πεπερασμένα *αλφάβητα εισόδου και εξόδου* $X$ και $Y$, ένα πεπερασμένο σύνολο *καταστάσεων* $Q$, μία *συνάρτηση εισόδου* $I : X \to Q$ που αντιστοιχίζει εισόδους σε καταστάσεις, μία *συνάρτηση εξόδου* $O : Q \to Y$ που αντιστοιχίζει καταστάσεις σε εξόδους και μία *συνάρτηση μετάβασης* $\delta : Q \times Q \to Q \times Q$ επί του συνόλου που αποτελείται από όλα τα διατεταγμένα ζεύγη καταστάσεων (όπου χρειάζεται, μπορούμε να υποθέτουμε την, πιο γενική, *σχέση μετάβασης* $\delta$ επί του $Q^2$). Αν $\delta(a, b) = (a', b')$, τότε καλούμε το $(a, b) \to (a', b')$ *μετάβαση* ή *κανόνα* και ορίζουμε $\delta_1(a, b) = a'$ και $\delta_2(a, b) = b'$. Καλούμε την $\delta_1$ *απόκτημα του μυητή* και την $\delta_2$ *απόκτημα του αποκρινόμενου*.

Για να γίνει πιο κατανοητός ο ορισμός, ας δούμε μία τυπική έκδοση του πρωτοκόλλου που υπολογίζει αν τουλάχιστον $100$ ψάρια έχουν μολυνθεί. Το σύνολο των καταστάσεων αποτελείται από $101$ καταστάσεις και είναι το $Q = \{q_0, q_1, \ldots, q_{100}\}$. Τα αλφάβητα εισόδου και εξόδου είναι τα $X = Y = \{0, 1\}$ (εδώ τυχαίνει να είναι ίδια). Η συνάρτηση εισόδου $I$ αντιστοιχίζει το σύμβολο $0$ στην $q_0$ και το $1$ στην $q_1$. Η συνάρτηση εξόδου $O$ αντιστοιχίζει κάθε $q \in Q - q_{100}$ στο σύμβολο $0$ και την $q_{100}$ στο $1$. Η συνάρτηση μετάβασης $\delta$ ορίζεται ως εξής: $\delta(q_i, q_j) = (q_{i+j}, q_0)$ αν $i + j < 100$ και $\delta(q_i, q_j) = (q_{100}, q_{100})$ αλλιώς (δηλαδή, αν $q_{i+j} \geq 100$).

Σύμφωνα με των αυθεντικό ορισμό των Angluin et al. (βλέπε [3]), ένα πρωτόκολλο πληθυσμού τρέχει σε έναν πληθυσμό οποιουδήποτε πεπερασμένου μεγέθους $n$. Ένας *πληθυσμός* $\mathcal{P}$ αποτελείται από ένα σύνολο $V$ με $n$ *πράκτορες*, όπου $n \geq 2$, και μία μη-ανακλαστική δυαδική σχέση $E$ επί του συνόλου $V$, δηλαδή $E \subseteq V \times V$, η οποία ερμηνεύεται ως το σύνολο των κατευθυνόμενων ακμών ενός *γράφου αλληλεπιδράσεων* ή *γράφου επικοινωνίας*. Το $E$ περιγράφει ποιοι πράκτορες ενδέχεται να αλληλεπιδράσουν κατά τη διάρκεια του υπολογισμού.

Εμείς, εδώ, θα επιχειρήσουμε μία μικρή διαφοροποίηση απ' τον αυθεντικό ορισμό. Θεωρούμε ότι ο πληθυσμός είναι το σύνολο των πρακτόρων $V$ μεγέθους $|V| = n$. Ένα πρωτόκολλο πληθυσμού τρέχει στον γράφο επικοινωνίας $G = (V, E)$ που ορίζεται από τη *συμπεριφορά* του πληθυσμού $V$. Η συμπεριφορά του πληθυσμού αποτυπώνεται στην μη-ανακλαστική δυαδική σχέση $E$ επί του συνόλου $V$, που συνίσταται από τις επιτρεπόμενες αλληλε-

πιδράσεις μεταξύ των πρακτόρων. Με άλλα λόγια, η μόνη διαφοροποίηση έγκειται στο ότι μετονομάζουμε τον όρο "πληθυσμός" σε "γράφος επικοινωνίας", έτσι ώστε με τον όρο "πληθυσμός" να αναφερόμαστε μόνο στο σύνολο των πρακτόρων και όχι και στην συμπεριφορά τους. Κατά τα άλλα, ένα πρωτόκολλο πληθυσμού τρέχει και πάλι σε ένα πεπερασμένο σύστημα που αποτελείται από κάποιους πράκτορες και όλες τις μεταξύ τους πιθανές αλληλεπιδράσεις.

Διαισθητικά, μία ακμή $(u, v) \in E$ υποδηλώνει ότι οι πράκτορες $u$ και $v$ ενδέχεται να αλληλεπιδράσουν, με τον $u$ να παίζει το ρόλο του *μυητή* και τον $v$ αυτόν του *αποκρινόμενου* στην επικοινωνία. Αξίζει να παρατηρήσει κανείς ότι οι διακριτοί ρόλοι των δύο πρακτόρων σε μία αλληλεπίδραση αποτελεί μία θεμελιώδη υπόθεση ασυμμετρίας του μοντέλου. Λόγω της υπόθεσης αυτής οι μεταβάσεις διεξάγονται με *ντετερμινιστικό τρόπο*. Αυτό σημαίνει ότι κατά αλληλεπίδραση $(u, v)$, όπου ο $u$ είναι στην κατάσταση $a$ και ο $v$ στην $b$, είμαστε βέβαιοι ότι ο $u$ θα περάσει στην $\delta_1(a, b)$ και ο $v$ στην $\delta_2(a, b)$ (μπορούμε να υποθέτουμε ότι ο καθένας ανάλογα με το ρόλο του εφαρμόζει μία εκ των $\delta_1$ και $\delta_2$). Με άλλα λόγια, δεδομένων των καταστάσεων των πρακτόρων που αλληλεπιδρούν, τον ρόλο του καθενός και της συνάρτησης μετάβασης $\delta$, δεν υπάρχει καμία αβεβαιότητα ως προς την κατάσταση που θα έχει ο κάθε πράκτορας μετά την αλληλεπίδραση.

**Ορισμός 2.** *Η σχέση μετάβασης, $\delta$, ενός πρωτοκόλλου (και κατά συνέπεια το ίδιο το πρωτόκολλο) είναι ντετερμινιστική(ό), εάν η $\delta$ είναι μία μονοσήμαντη και ολική σχέση επί του $Q^2$ (δηλαδή, όταν είναι συνάρτηση μετάβασης).*

Σε ένα *ντετερμινιστικό πρωτόκολλο*, η $\delta$ αντιστοιχίζει κάθε $(a, b) \in Q^2$ σε ένα μόνο στοιχείο του $Q^2$.

Μία *διαμόρφωση πληθυσμού* είναι μία αντιστοιχία $C : V \to Q$ (συνάρτηση) που προσδιορίζει την κατάσταση κάθε μέλους του πληθυσμού. Με άλλα λόγια, μία διαμόρφωση περιγράφει πλήρως την τρέχουσα κατάσταση του συστήματος, αφού μας ενημερώνει για την κατάσταση στην οποία βρίσκεται κάθε πράκτορας του πληθυσμού. Έστω οι διαμορφώσεις πληθυσμού $C$ και $C'$, και έστω $u$ και $v$ είναι δύο διακριτοί πράκτορες. Λέμε ότι η $C$ πηγαίνει στην $C'$ μέσω της *συνάντησης* $e = (u, v)$ και συμβολίζουμε με $C \xrightarrow{e} C'$, εάν

$$\begin{aligned} C'(u) &= \delta_1(C(u), C(v)), \\ C'(v) &= \delta_2(C(u), C(v)), \text{ και} \\ C'(w) &= C(w), \text{ για κάθε } w \in V - \{u, v\}. \end{aligned}$$

Λέμε ότι η $C$ μπορεί να πάει στην $C'$ σε ένα βήμα και συμβολίζουμε με $C \to C'$, αν $C \xrightarrow{e} C'$ για κάποια συνάντηση $e \in E$. Δηλαδή, η $C$ μπορεί να πάει στην $C'$ σε ένα βήμα, αν υπάρχει συνάντηση μέσω της οποίας η $C$ πηγαίνει στην $C'$. Έχοντας ορίσει την δυαδική σχέση "μπορεί να πάει σε ένα

βήμα στην" επί του συνόλου των διαμορφώσεων πληθυσμού, μπορούμε πολύ εύκολα να ορίσουμε την "μπορεί να πάει στην" (σε ένα ή περισσότερα βήματα) ως την μεταβατική της θήκη. Τυπικά, γράφουμε $C \xrightarrow{*} C'$, αν υπάρχει μία ακολουθία διαμορφώσεων $C = C_0, C_1, \ldots, C_t = C'$, τέτοια ώστε $C_i \to C_{i+1}$ για κάθε $i$, όπου $0 \leq i < t$, και στην περίπτωση αυτή λέμε ότι η $C'$ είναι *προσβάσιμη*[1] απ' την $C$.

Ο *γράφος μεταβάσεων* $D_{\mathcal{A},G} = (\mathcal{C}, \mathcal{E})$ ενός πρωτοκόλλου $\mathcal{A}$ που τρέχει σε ένα γράφο επικοινωνίας $G = (V, E)$ είναι ένας κατευθυνόμενος γράφος (που γενικά μπορεί να περιέχει και βρόχους) του οποίου οι κόμβοι είναι το σύνολο $\mathcal{C} = Q^V$ όλων των διαμορφώσεων πληθυσμού και του οποίου το σύνολο ακμών ορίζεται ως $\mathcal{E} = \{(C, C') \mid C, C' \in \mathcal{C} \text{ και } C \to C'\}$ (προσέξτε ότι μπορεί να ισχύει $(C, C) \in \mathcal{E}$), δηλαδή, περιέχει όλες τις δυνατές μεταβάσεις σε ένα βήμα μεταξύ των διαμορφώσεων. Μία ισχυρά συνεκτική συνιστώσα ενός κατευθυνόμενου γράφου είναι *τελική* εάν και μόνον εάν δεν υπάρχει ακμή που να ξεκινάει από κόμβο της συνιστώσας και να κατευθύνεται σε κόμβο εκτός αυτής. Μία διαμόρφωση είναι *τελική* εάν και μόνον εάν ανήκει σε μία τελική ισχυρά συνεκτική συνιστώσα του γράφου μεταβάσεων.

Μία *εκτέλεση* είναι μία πεπερασμένη ή άπειρη ακολουθία διαμορφώσεων πληθυσμού $C_0, C_1, C_2, \ldots$ τέτοια ώστε για κάθε $i$, $C_i \to C_{i+1}$. Μία άπειρη εκτέλεση είναι *δίκαιη*, εάν για κάθε ζεύγος διαμορφώσεων πληθυσμού $C$ και $C'$, τέτοιων ώστε $C \to C'$, αν η $C$ εμφανίζεται άπειρο αριθμό φορών στην εκτέλεση, τότε και η $C'$ εμφανίζεται άπειρο αριθμό φορών στην εκτέλεση. Ένας *υπολογισμός* είναι μία (άπειρη) δίκαιη εκτέλεση. Ισοδύναμα, λέμε ότι ο εχθρικός δρομολογητής είναι δίκαιος αν η ακολουθία αλληλεπιδράσεων που επιλέγει οδηγεί πάντοτε σε δίκαιη εκτέλεση. Αυτή είναι μία ισχυρή καθολική *συνθήκη δικαιοσύνης* που επιβάλλουμε στον δρομολογητή. Διαισθητικά, επιβάλλουμε στον εχθρικό δρομολογητή να είναι υπολογιστικά φιλικός μην επιτρέποντάς του να αποφεύγει ένα πιθανό βήμα για πάντα. Ένας άλλος τρόπος για να το σκεφτεί κανείς είναι ο εξής: οτιδήποτε είναι πάντοτε πιθανό να συμβεί, τελικά συμβαίνει. Αυτό είναι ισοδύναμο με το να απαιτήσουμε ότι κάθε διαμόρφωση που είναι πάντοτε προσβάσιμη τελικά επιτυγχάνεται.

**Λήμμα 1.** *Έστω $\Xi = C_0, C_1, C_2, \ldots$ ένας υπολογισμός ενός πρωτοκόλλου πληθυσμού $\mathcal{A}$ που τρέχει σε έναν γράφο επικοινωνίας $G$. Έστω $\mathcal{F} \subseteq \mathcal{C}$ το σύνολο των διαμορφώσεων που εμφανίζονται άπειρο αριθμό φορών στον $\Xi$ και έστω $D_{\mathcal{F}}$ ο υπογράφος του γράφου μεταβάσεων $D_{\mathcal{A},G}$ που επάγεται από το $\mathcal{F}$.*[2]

[1] Ο αντίστοιχος αγγλικός όρος είναι "reachable" και μεταφράζεται "προσεγγίσιμη" (διαμόρφωση) ή περιφραστικά "που μπορεί να την φτάσει η...", όμως ο όρος "προσέγγιση" θα χρησιμοποιηθεί εκτενώς στο επόμενο κεφάλαιο όταν και θα μιλήσουμε για προσεγγιστικά πρωτόκολλα και προς αποφυγή οποιασδήποτε σύγχυσης προτιμήθηκε ο όρος "προσβάσιμη".

[2] Ο επαγόμενος γράφος ορίζεται ως $D_{\mathcal{F}} = (\mathcal{F}, (\mathcal{E} \cap (\mathcal{F} \times \mathcal{F})))$.

*Ο $D_{\mathcal{F}}$ είναι μία τελική ισχυρά συνεκτική συνιστώσα του $D_{\mathcal{A},G}$ και κάθε στοιχείο του $\mathcal{F}$ είναι τελικό.*

*Απόδειξη.* Έστω $C$ και $C'$ δύο οποιαδήποτε στοιχεία του $\mathcal{F}$. Απ' τον ορισμό του $\mathcal{F}$ και οι δύο διαμορφώσεις εμφανίζονται άπειρο αριθμό φορών στον υπολογισμό άρα η μία είναι προσβάσιμη απ' την άλλη (μέσω κάποιας υποακολουθίας μεταβάσεων) και αυτό ισχύει για κάθε ζεύγος διαμορφώσεων του $\mathcal{F}$. Άρα, ο $D_{\mathcal{F}}$ είναι μία ισχυρά συνεκτική συνιστώσα του $D_{\mathcal{A},G}$. Έστω τώρα $C \in \mathcal{F}$ και $C' \notin \mathcal{F}$ τ.ώ.[3] $C \to C'$ (ή ισοδύναμα $(C, C') \in \mathcal{E}$). Λόγω του ότι κάθε υπολογισμός είναι εξ' ορισμού δίκαιος, αφού η $C$ εμφανίζεται άπειρο αριθμό φορών σε αυτόν το ίδιο θα πρέπει να ισχύει και για τη $C'$, δηλαδή, θα πρέπει να ισχύει επίσης $C' \in \mathcal{F}$, το οποίο όμως είναι άτοπο και συνεπώς για κάθε $C \in \mathcal{F}$ και $C' \notin \mathcal{F}$ δεν μπορεί να ισχύει $C \to C'$. Άρα, η συνιστώσα $D_{\mathcal{F}}$ είναι και τελική και κάθε στοιχείο του $\mathcal{F}$ είναι επίσης τελικό. □

Η βασική υπόθεση που διαφοροποιεί το μοντέλο των πρωτοκόλλων πληθυσμών από τα παραδοσιακά κατανεμημένα συστήματα είναι ότι οι περιγραφές των πρωτοκόλλων είναι ανεξάρτητες από το μέγεθος του πληθυσμού (δηλαδή, χρειάζονται $\mathcal{O}(1)$ συνολική χωρητικότητα μνήμης σε κάθε πράκτορα), η οποία είναι γνωστή ως ιδιότητα *ομοιομορφίας* των πρωτοκόλλων πληθυσμών. Επιπλέον, τα πρωτόκολλα πληθυσμών είναι *ανώνυμα*, αφού οι καταστάσεις των πρακτόρων δεν διαθέτουν επαρκή χώρο για την αποθήκευση ενός *μοναδικού προσδιοριστή* (ταυτότητας) και ως εκ τούτου η συνάρτηση μετάβασης μεταχειρίζεται όλους τους πράκτορες με τον ίδιο τρόπο.

Αξίζει, επίσης, να παρατηρήσουμε ότι σε ένα πραγματικό τέτοιο κατανεμημένο σύστημα, πολλές αλληλεπιδράσεις μπορούν να συμβαίνουν ταυτόχρονα (φυσικά, κάθε πράκτορας μπορεί να συμμετέχει το πολύ σε μία αλληλεπίδραση κάθε δεδομένη χρονική στιγμή), όμως για να πάρουμε την ακολουθία διαμορφώσεων του υπολογισμού, μπορούμε να διατάξουμε αυθαίρετα τις ταυτόχρονες αλληλεπιδράσεις. Συνεπώς, μπορούμε χ.β.τ.γ.[4] να υποθέτουμε ότι κάθε εκτέλεση μπορεί να μοντελοποιηθεί από έναν δίκαιο εχθρικό δρομολογητή που επιλέγει ένα μόνο ζεύγος αλληλεπίδρασης σε κάθε βήμα.

**Λήμμα 2.** *Έστω ένας υπολογισμός $C_0, C_1, C_2, \ldots$ και έστω δύο διαδοχικές διαμορφώσεις $C_i$ και $C_{i+1}$ του υπολογισμού τέτοιες ώστε η $C_{i+1}$ έχει προκύψει απ' την $C_i$ απ' τις ταυτόχρονες αλληλεπιδράσεις $l$ διατεταγμένων ζευγών $D = \{e_1, e_2, \ldots, e_l\}$. Οποιαδήποτε διάταξη των στοιχείων του $D$ αν εφαρμοσθεί ακολουθιακά ξεκινώντας απ' τη διαμόρφωση $C_i$ (δηλαδή στην $C_i$ εφαρμόζεται το πρώτο στοιχείο της διάταξης και προκύπτει μία νέα διαμόρφωση στην οποία εφαρμόζεται το δεύτερο στοιχείο της διάταξης κ.ο.κ.) θα δώσει μία ακολουθία*

[3] τέτοιες ώστε

[4] χωρίς βλάβη της γενικότητας

*$l$ διαμορφώσεων $C_1^i, C_2^i, \ldots, C_l^i$ η τελευταία εκ των οποίων θα είναι πάντοτε η $C_{i+1}$ (δηλαδή $C_l^i = C_{i+1}$).*

*Απόδειξη.* Έστω $V'$ το σύνολο των $2l$ κόμβων που αποτελούν άκρα κάποιας ακμής του $D$ και ορίζεται ως $V' = V_l' \cup V_r'$, όπου $V_l' = \{u \mid (u, v) \in D\}$ και $V_r' = \{v \mid (u, v) \in D\}$. Τα $V_l'$ και $V_r'$ αποτελούν μία διαμέριση του $V'$, αφού κάθε στοιχείο του είναι ή μυητής ή αποκρινόμενος σε μία μόνο απ' τις ταυτόχρονες αλληλεπίδρασεις. Για κάθε $w \in V - V'$, $C_{i+1}(w) = C_i(w)$. Για κάθε $u \in V'$, $C_{i+1}(u) = \delta_1(C_i(u), C_i(v))$ αν $\exists (u, v) \in D$ και $C_{i+1}(u) = \delta_2(C_i(v), C_i(u))$ αν $\exists (v, u) \in D$. Παρατηρούμε ότι η $C_{i+1}$ είναι η $C_i$ στην οποία για κάθε $(u, v) \in D$ έχουμε εφαρμόσει $\delta(C_i(u), C_i(v))$. Η σειρά με την οποία θα επιλέξουμε τα στοιχεία του $D$ για να πάρουμε την $C_{i+1}$ απ' την $C_i$ δεν έχει καμία σημασία, καθώς κάθε $u \in V'$ εμφανίζεται σε ένα ακριβώς στοιχείο του $D$. □

**Θεώρημα 1.** *Κάθε δρομολογητής $A$ που επιλέγει ένα ή περισσότερα ζεύγη προς αλληλεπίδραση σε κάθε βήμα μπορεί να εξομοιωθεί από έναν δρομολογητή $A'$ που επιλέγει σε κάθε βήμα ένα μόνο ζεύγος.*

*Απόδειξη.* Για κάθε σύνολο ταυτόχρονων αλληλεπιδράσεων $D$ του $A$, ο $A'$ διατάσσει το $D$ αυθαίρετα και εφαρμόζει τη $\delta$ ακολουθιακά στα στοιχεία της διάταξης. Σύμφωνα με το Λήμμα 2 ο υπολογισμός διεξάγεται κατά τον ίδιο τρόπο. □

**Θεώρημα 2.** *Κάθε δρομολογητής $A'$ που επιλέγει ένα μόνο ζεύγος προς αλληλεπίδραση σε κάθε βήμα μπορεί να εξομοιωθεί από έναν δρομολογητή $A$ που επιλέγει σε κάθε βήμα ένα ή περισσότερα ζεύγη.*

*Απόδειξη.* Ο $A'$ είναι ειδική περίπτωση του $A$. □

Απ' τον συνδυασμό των Θεωρημάτων 1 και 2 προκύπτει το ακόλουθο πολύ ενδιαφέρον Πόρισμα:

**Πόρισμα 1.** *Το μοντέλο των πρωτοκόλλων πληθυσμών στο οποίο ο δρομολογητής μπορεί να επιλέγει προς αλληλεπίδραση ένα ή περισσότερα ζεύγη πρακτόρων σε κάθε βήμα είναι ισοδύναμο ως προς την υπολογιστική του ισχύ με το μοντέλο των πρωτοκόλλων πληθυσμών στο οποίο ο δρομολογητής μπορεί να επιλέγει προς αλληλεπίδραση ένα μόνο ζεύγος σε κάθε βήμα.*

## 2.3 Ο Υπολογισμός στα Πρωτόκολλα Πληθυσμών

Τα πρωτόκολλα πληθυσμών, σε αντίθεση με τις μηχανές Turing, δεν τερματίζουν. Εξαιτίας αυτού, δεν υπάρχει προκαθορισμένος χρόνος για να διαβάσει

κανείς την έξοδο του πληθυσμού. Τη θέση του τερματισμού παίρνει μία πολύ ενδιαφέρουσα ιδιότητα των πρωτοκόλλων πληθυσμού που ονομάζεται *σταθερότητα*.

**Ορισμός 3.** *Λέμε ότι η έξοδος ενός υπολογισμού σταθεροποιείται, εάν φτάνει σε ένα σημείο (σε μία διαμόρφωση) μετά το οποίο κανείς πράκτορας δεν μπορεί να αλλάξει την τιμή εξόδου του ανεξαρτήτως του πώς θα εξελιχθεί ο υπολογισμός από εκεί και έπειτα.*

Η σταθερότητα είναι μία καθολική ιδιότητα της διαμόρφωσης πληθυσμού και γενικά οι πράκτορες δεν μπορούν να γνωρίζουν πότε αυτή έχει επιτευχθεί. Αξίζει να παρατηρήσουμε ότι αν το γνώριζαν, θα μπορούσαν να ειδοποιήσουν ένα σταθμό βάσης ότι ο υπολογισμός έχει ολοκληρωθεί, αφού η τρέχουσα έξοδος δεν γίνεται να μεταβληθεί σε καμία από τις δυνατές μετέπειτα επιλογές του δρομολογητή και, συνεπώς, είναι η τελική έξοδος. Αργότερα θα δούμε ότι με κατάλληλες στοχαστικές υποθέσεις για τον ρυθμό με τον οποίο συμβαίνουν οι αλληλεπιδράσεις, είναι δυνατόν να φράξουμε το αναμενόμενο πλήθος αλληλεπιδράσεων μέχρι να σταθεροποιηθεί η έξοδος.

Μία *ανάθεση εισόδου* είναι μία συνάρτηση $x : V \to X$ που περιγράφει τις εισόδους που παρέχονται σε ένα πρωτόκολλο πληθυσμού (για κάθε $u \in V$ το $x(u) \in X$ είναι η είσοδος του πράκτορα $u$). Με άλλα λόγια, αν $V = \{1, 2, \ldots, n\}$, μία ανάθεση εισόδου είναι μία διάταξη, $(x_1, x_2, \ldots, x_n)$, $n$ στοιχείων επιλεγμένων από το αλφάβητο εισόδου $X$, όπου $x_i$, για $1 \leq i \leq n$, συμβολίζει το σύμβολο εισόδου που διαβάζει ο αισθητήρας του πράκτορα $i$. Έστω $\mathcal{X} = X^V$ το σύνολο όλων των δυνατών αναθέσεων εισόδου και $\mathcal{C} = Q^V$ το σύνολο όλων των δυνατών διαμορφώσεων πληθυσμού.[5] Οι είσοδοι μπορούν να αναπαρασταθούν από μία *διαμόρφωση εισόδου* ή *αρχική διαμόρφωση* $C_x$ ($C_x : V \to Q$), όπου $C_x(w) = I(x(w))$, για κάθε $w \in V$ (δηλαδή, η $C_x$ είναι η σύνθετη συνάρτηση $I \circ x$). Η διαμόρφωση εισόδου είναι κατά κάποιον τρόπο το αποτέλεσμα της εφαρμογής της συνάρτησης εισόδου στο σύμβολο εισόδου που διάβασε ο αισθητήρας κάθε πράκτορα και αποτυπώνει την αρχική κατάσταση κάθε πράκτορα ακριβώς πριν το πρώτο βήμα του υπολογισμού (αν υποθέσουμε ότι όλοι οι πράκτορες εφαρμόζουν την $I$ ταυτόχρονα και αφού έχουν όλοι αισθανθεί το περιβάλλον τους). Επεκτείνουμε την $I$ σε μία αντιστοιχία από αναθέσεις εισόδου σε διαμορφώσεις πληθυσμού, $I : \mathcal{X} \to \mathcal{C}$, γράφοντας $I(x) = C_x$. Δηλαδή, αν $x : V \to X$ είναι μία ανάθεση εισόδου, τότε $I(x)$ (όπου $I : \mathcal{X} \to \mathcal{C}$) είναι η αρχική διαμόρφωση, $C_x$, που προκύπτει από την $x$ δεδομένης της συνάρτησης εισόδου $I : X \to Q$. Επομένως, αν μία ανάθεση εισόδου $x$ αναθέτει το σύμβολο $\sigma$ στον πράκτορα $u$ (δηλαδή,

[5] Γενικά, στην Θεωρία Συνόλων, το σύνολο όλων των συναρτήσεων με πεδίο ορισμού ένα σύνολο $D$ και πεδίο τιμών ένα σύνολο $R$ συμβολίζεται ως $R^D$.

$x(u) = \sigma$), τότε η κατάσταση του πράκτορα $u$ στην αρχική διαμόρφωση $I(x)$ είναι η $I(\sigma)$ (είναι εύκολο να διαπιστώσουμε πώς χρησιμοποιείται η $I$, απ' το αν η είσοδός της είναι ανάθεση εισόδου ή σύμβολο εισόδου).

Μία *ανάθεση εξόδου* είναι μία συνάρτηση $y : V \to Y$ που περιγράφει τις εξόδους ενός πρωτοκόλλου πληθυσμού. Όπως και πριν, έστω ότι το $\mathcal{Y} = Y^V$ συμβολίζει το σύνολο όλων των αναθέσεων εξόδου. Κάθε διαμόρφωση $C$ αντιστοιχεί σε μία ανάθεση εξόδου $y_C$ που προκύπτει εφαρμόζοντας τη συνάρτηση εξόδου $O$ στην κατάσταση που έχει κάθε πράκτορας υπό τη διαμόρφωση $C$. Συνεπώς, η $y_C$ είναι η σύνθετη συνάρτηση $O \circ C$, δηλαδή $y_C(u) = O(C(u))$, για κάθε $u \in V$. Όπως κάναμε και με την $I$, επεκτείνουμε την $O$ σε μία αντιστοιχία από διαμορφώσεις σε αναθέσεις εξόδου, $O : \mathcal{C} \to \mathcal{Y}$, γράφοντας $O(C) = y_C$. Επομένως, αν $q$ είναι η κατάσταση που έχει ο πράκτορας $u$ στη διαμόρφωση $C$ (δηλαδή, $C(u) = q$), τότε το σύμβολο εξόδου του πράκτορα $u$ στην ανάθεση εξόδου $O(C)$ είναι $O(q)$.

Μία διαμόρφωση $C$ θα καλείται *σταθερής-εξόδου*, εάν $O(C') = O(C)$, για κάθε $C'$ που είναι προσβάσιμη απ' την $C$. Διαισθητικά, το να φτάσει ο υπολογισμός σε μία σταθερής-εξόδου διαμόρφωση $C$ σημαίνει ότι όποιο μονοπάτι διαμορφώσεων και να ακολουθήσει ο υπολογισμός από εκεί και έπειτα, οι διαμορφώσεις αυτές θα αντιστοιχούν πάντοτε στην ίδια ανάθεση εξόδου $O(C)$, δηλαδή η έξοδος κάθε πράκτορα θα παραμένει σε κάθε βήμα αμετάβλητη (η μεταβολή της εξόδου ενός πράκτορα θα σήμαινε διαφορετική ανάθεση εξόδου). Αξίζει να παρατηρήσουμε ότι δύο διαμορφώσεις $C$ και $C'$, όπου υπάρχει τουλάχιστον ένα $u \in V$, τ.ώ. $C(u) \neq C'(u)$ (δηλαδή, $C \neq C'$), μπορεί να αντιστοιχούν στην ίδια διαμόρφωση εξόδου $O(C)$. Για να συμβαίνει αυτό, θα πρέπει για κάθε $u \in V$ στο οποίο οι διαμορφώσεις $C$ και $C'$ διαφωνούν δίνοντας καταστάσεις $q_u$ και $q'_u$, αντίστοιχα, με $q_u \neq q'_u$, να ισχύει $O(q_u) = O(q'_u)$. Με άλλα λόγια, παρατηρούμε ότι για να είναι μία διαμόρφωση $C$ *σταθερής-εξόδου*, δεν απαιτούμε να ισχύει $C = C'$ για κάθε $C'$ που είναι προσβάσιμη απ' την $C$, αλλά απλώς απαιτούμε να έχουν τις ίδιες εξόδους.

Ένας άπειρος υπολογισμός *σταθεροποιείται ως προς την έξοδό του* εάν περιέχει μία σταθερής-εξόδου διαμόρφωση $C$ και στην περίπτωση αυτή θα λέμε ότι *σταθεροποιείται στην έξοδο* $y = O(C)$ (ο αναγνώστης αξίζει να παρατηρήσει ότι οι διαμορφώσεις που "περιέχει" ο υπολογισμός είναι οι διαμορφώσεις απ' τις οποίες περνάει ο υπολογισμός και όχι το σύνολο όλων των δυνατών διαμορφώσεων $\mathcal{C}$). Ένας άπειρος υπολογισμός που δεν σταθεροποιείται ως προς την έξοδό του θα καλείται *ασταθής*.

**Παρατήρηση 1.** *Κάθε άπειρος υπολογισμός στο μοντέλο των πρωτοκόλλων πληθυσμών σταθεροποιείται το πολύ σε μία έξοδο (ανάθεση εξόδου).*

Η έξοδος ενός πεπερασμένου υπολογισμού είναι η έξοδος της τελευταίας

του διαμόρφωσης. Η έξοδος ενός άπειρου υπολογισμού που σταθεροποιείται στην έξοδο $y$ είναι $y$. Φυσικά, παρότι ο υπολογισμός είναι άπειρος, ευελπιστούμε ότι η σταθεροποίηση επιτυγχάνεται σε πεπερασμένο πλήθος βημάτων, έτσι ώστε να έχει νόημα ο υπολογισμός (από εκεί και πέρα, για άπειρο πλήθος βημάτων, τίποτα δεν αλλάζει ως προς την έξοδο). Η έξοδος είναι ακαθόριστη εάν ο υπολογισμός είναι ασταθής.

Ακόμα και πολύ απλά πρωτόκολλα που τρέχουν σε πολύ μικρούς πληθυσμούς μπορεί να οδηγούν πάντοτε σε ασταθή υπολογισμό. Έχει αξία να παρουσιάσουμε ένα τέτοιο παράδειγμα. Έστω ένα πληθυσμός, $V = \{u, v\}$, μεγέθους 2 και $E = \{(u, v)\}$. Το μόνο σύμβολο εισόδου είναι το $0$ το οποίο αντιστοιχίζεται από την $I$ στην κατάσταση $a \in Q = \{a, b\}$. Άρα, αρχικά και οι δύο πράκτορες βρίσκονται στην κατάσταση $a$. Η συνάρτηση μετάβασης $\delta$ ορίζεται ως

$$(a, a) \to (a, b)$$
$$(a, b) \to (b, a)$$
$$(b, a) \to (a, b)$$

και η συνάρτηση εξόδου ως $O(a) = 0$, $O(b) = 1$. Το ζεύγος αλληλεπίδρασης $(b, b)$ δεν μπορεί ποτέ να προκύψει γι' αυτό και δεν το συμπεριλάβαμε στον ορισμό της $\delta$ (όπως και να οριστεί, η λειτουργία του πρωτοκόλλου δεν μεταβάλλεται), όπως θα κάνουμε και σε κάθε άλλη παρόμοια περίπτωση. Αξίζει, πρώτα απ' όλα, να παρατηρήσουμε ότι λόγω της ύπαρξης μίας μόνο ακμής στο γράφο επικοινωνίας, πέραν του ντετερμινιστικού πρωτοκόλλου, ακόμα και οι επιλογές του δρομολογητή είναι ντετερμινιστικές αφού πάντα θα επιλέγει την ακμή $(u, v)$ και συνεπώς, μπορούμε να γνωρίζουμε, δεδομένης μιας ανάθεσης εισόδου, την ακριβή εξέλιξη του υπολογισμού (σπανίως παρουσιάζεται τέτοια ντετερμινιστική πληρότητα σε αυτά τα συστήματα). Αρχικά, και οι δύο πράκτορες βρίσκονται στην κατάσταση $a$. Ο δρομολογητής επιλέγει την $e = (u, v)$ (υποχρεωτικά) και εφαρμόζεται ο πρώτος κανόνας της $\delta$, επομένως το νέο ζεύγος καταστάσεων είναι $(a, b)$ για τους $(u, v)$, αντίστοιχα. Το ζεύγος αυτό αντιστοιχεί στην διαμόρφωση $C_1$ που ορίζεται ως $C_1(u) = a$, $C_1(v) = b$ και η $C_1$ με τη σειρά της αντιστοιχίζεται από την επεκταθείσα $O$ στην ανάθεση εξόδου $O(C_1) = y_{C_1}$ που ορίζεται ως $y_{C_1}(u) = 0$, $y_{C_1}(v) = 1$. Στην επόμενη επιλογή της $e$, το νέο ζεύγος καταστάσεων που ανατίθεται στους πράκτορες, λόγω του τρίτου κανόνα, είναι το $(b, a)$ που με παρόμοιο τρόπο αντιστοιχεί στην διαμόρφωση εξόδου $C_2$ με $y_{C_2}(u) = 1$, $y_{C_2}(v) = 0$. Παρατηρούμε ότι, από εδώ και στο εξής, εφαρμόζονται εναλλάξ οι κανόνες 2 και 3, με αποτέλεσμα οι αναθέσεις εξόδου $y_{C_1}$ και $y_{C_2}$, όπου $y_{C_1} \neq y_{C_2}$, να διαδέχονται συνεχώς η μία την άλλη οδηγώντας πάντοτε σε ασταθή υπολογισμό.

Γενικά πάντως, ακόμα και αν ένα πρωτόκολλο είναι ντετερμινιστικό, ο υπολογισμός είναι μη-ντετερμινιστικός λόγω του μη-ντετερμινισμού που υπεισέρχεται στο μοντέλο απ' τις επιλογές του δρομολογητή. Αυτό πρακτικά σημαίνει ότι το ίδιο πρωτόκολλο ξεκινώντας από την ίδια αρχική διαμόρφωση μπορεί οδηγείται λόγω των επιλογών του δρομολογητή σε διαφορετικούς υπολογισμούς κάθε φορά, που σταθεροποιούνται σε διαφορετικές εξόδους. Θα λέμε ότι ένα πρωτόκολλο $\mathcal{A}$ είναι *πάντα-σταθεροποιούμενο* εάν κάθε υπολογισμός κάθε ανάθεσης εισόδου $x$ σταθεροποιείται.

**Ορισμός 4.** *Θα λέμε ότι ένα πρωτόκολλο πληθυσμού $\mathcal{A}$ που τρέχει σε ένα γράφο επικοινωνίας $G = (V, E)$* ***υπολογίζει σταθερά μία σχέση εισόδου-εξόδου*** *$R_{\mathcal{A}} \subseteq \mathcal{X} \times \mathcal{Y}$ εάν, για κάθε ανάθεση εισόδου $x \in \mathcal{X}$ και ανάθεση εξόδου $y \in \mathcal{Y}$, η $x$ σχετίζεται με την $y$ μέσω της $R_{\mathcal{A}}$ (δηλαδή, $R_{\mathcal{A}}(x, y)$) εάν και μόνον εάν υπάρχει ένας υπολογισμός του $\mathcal{A}$ που ξεκινάει απ' την αρχική διαμόρφωση $I(x)$ και σταθεροποιείται στην έξοδο $y$.*

Στην ειδική περίπτωση που η $R_{\mathcal{A}}$ είναι μονοσήμαντη, γράφουμε $F_{\mathcal{A}}(x) = y$ για κάθε $(x, y) \in R_{\mathcal{A}}$ και λέμε ότι το πρωτόκολλο $\mathcal{A}$ *υπολογίζει σταθερά τη μερική συνάρτηση* $F_{\mathcal{A}} : \mathcal{X} \to \mathcal{Y}$.

Ο ορισμός για την περίπτωση που το $\mathcal{A}$ υπολογίζει σταθερά μία συνάρτηση απαιτεί για κάθε $x \in \mathcal{X}$ να μην υπάρχουν περισσότεροι από ένας υπολογισμοί που ξεκινούν απ' την αρχική διαμόρφωση $I(x)$ και σταθεροποιούνται σε διαφορετικές εξόδους, καθώς τότε η $R_{\mathcal{A}}$ δεν θα είναι μονοσήμαντη. Άρα, για κάθε $x$ ή υπάρχουν ένας οι περισσότεροι υπολογισμοί που ξεκινώντας απ᾽ την $I(x)$ σταθεροποιούνται στην ίδια έξοδο ή δεν υπάρχει κανένας υπολογισμός που να σταθεροποιείται ξεκινώντας απ' την $I(x)$. Η τελευταία περίπτωση καθορίζει για ποιά $x$ δεν ορίζεται η έξοδος της $F_{\mathcal{A}}$ και αυτός είναι ο λόγος που λέμε ότι πρόκειται για μερική συνάρτηση. Στην πρώτη όμως περίπτωση, παρατηρούμε ότι υπάρχει το ενδεχόμενο για κάποια ανάθεση εισόδου $x$ να υπάρχουν τόσο ένας οι περισσότεροι υπολογισμοί που ξεκινώντας απ᾽ την $I(x)$ σταθεροποιούνται στην ίδια έξοδο $y$, όσο και κάποιοι υπολογισμοί που δεν σταθεροποιούνται σε καμία έξοδο και παρ' όλα αυτά εμείς λόγω του ορισμού θεωρούμε ότι $F_{\mathcal{A}}(x) = y$ το οποίο δεν είναι ορθό, αφού αυτό διαισθητικά σημαίνει ότι σε κάποιους υπολογισμούς που ξεκινούν απ' την $I(x)$ ναι μεν δεν θα παίρνουμε λάθος απάντηση αλλά ίσως να μην παίρνουμε καμία απάντηση παρότι η $F_{\mathcal{A}}$ ορίζεται για το $x$. Ο ακόλουθοι είναι δύο πιο αυστηροί ορισμοί που επιχειρούν να διορθώσουν αυτό που μόλις αναφέραμε:

**Ορισμός 5.** *Θα λέμε ότι ένα πρωτόκολλο πληθυσμού $\mathcal{A}$ που τρέχει σε ένα γράφο επικοινωνίας $G = (V, E)$* ***υπολογίζει σταθερά μία σχέση εισόδου-εξόδου*** *$R_{\mathcal{A}} \subseteq \mathcal{X} \times \mathcal{Y}$ εάν, για κάθε ανάθεση εισόδου $x \in \mathcal{X}$ και ανάθεση εξόδου $y \in \mathcal{Y}$, η $x$ σχετίζεται με την $y$ μέσω της $R_{\mathcal{A}}$ (δηλαδή, $R_{\mathcal{A}}(x, y)$) εάν και μόνον*

*εάν υπάρχει ένας υπολογισμός του $\mathcal{A}$ που ξεκινάει απ' την αρχική διαμόρφωση $I(x)$ και σταθεροποιείται στην έξοδο $y$ και δεν υπάρχει υπολογισμός του $\mathcal{A}$ που ξεκινάει απ' την αρχική διαμόρφωση $I(x)$ και δεν σταθεροποιείται.*

**Ορισμός 6.** *Θα λέμε ότι ένα πρωτόκολλο πληθυσμού $\mathcal{A}$ που τρέχει σε ένα γράφο επικοινωνίας $G = (V, E)$* ***υπολογίζει σταθερά μία μερική συνάρτηση*** *$F_{\mathcal{A}} : \mathcal{X} \to \mathcal{Y}$ αυν[6], για κάθε $x \in \mathcal{X}_s$ (αν θεωρήσουμε ότι $\mathcal{X}_s$ είναι το υποσύνολο του $\mathcal{X}$ στο οποίο ορίζεται η $F_{\mathcal{A}}$) και κάθε υπολογισμό που ξεκινάει απ' την αρχική διαμόρφωση $I(x)$, ο υπολογισμός σταθεροποιείται στην έξοδο $F_{\mathcal{A}}(x)$.*

Αξίζει να αναφέρουμε ότι ένα θεώρημα που θα αποδείκνυε ότι, αν κάποιος υπολογισμός ενός πρωτοκόλλου με είσοδο $x$ σταθεροποιείται τότε κάθε υπολογισμός του πρωτοκόλλου με είσοδο $x$ σταθεροποιείται, θα καθιστούσε τους αυστηρότερους Ορισμούς 5 και 6 ισοδύναμους με τους προηγούμενους, αλλά αυτό δεν γνωρίζουμε αν ισχύει.

Παρατηρούμε ότι για να είναι ορθό ένα πρωτόκολλο που υπολογίζει σταθερά μία συνάρτηση, θα πρέπει, για κάθε ανάθεση εισόδου στην οποία ορίζεται η συνάρτηση και ανεξαρτήτως του τί επιλογές θα κάνει ένας δίκαιος δρομολογητής, η έξοδος του υπολογισμού να είναι πάντοτε ίδια με την τιμή της συνάρτησης για την ανάθεση αυτή. Αντίθετα, στην περίπτωση της σχέσης $R_{\mathcal{A}}$ η ίδια ανάθεση εισόδου μπορεί να σχετίζεται με περισσότερες από μία αναθέσεις εξόδου και συνεπώς για την ορθότητα του πρωτοκόλλου εδώ αρκεί, για δεδομένη ανάθεση εισόδου $x$, να υπάρχει τουλάχιστον ένας δυνατός υπολογισμός για κάθε ανάθεση εξόδου $y$ με την οποία σχετίζεται η $x$ μέσω της $R_{\mathcal{A}}$ που να σταθεροποιείται στην έξοδο $y$ και για κάθε $x$ το οποίο σχετίζεται με ένα ή περισσότερα $y$ μέσω της $R_{\mathcal{A}}$ ο υπολογισμός να συγκλίνει πάντοτε σε κάποιο απ' αυτά τα $y$ και φυσικά για κάθε $y$ να υπάρχει τουλάχιστον ένας υπολογισμός που συγκλίνει σε αυτό.

Τέλος δίνουμε έναν ορισμό για την συνήθη περίπτωση των πάντα-σταθεροποιούμενων πρωτοκόλλων (ο αναγνώστης αξίζει να παρατηρήσει ότι εδώ η συνάρτηση που υπολογίζεται είναι υποχρεωτικά ολική, καθώς κάθε υπολογισμός του πρωτοκόλλου για κάθε είσοδο θα πρέπει να σταθεροποιείται).

**Ορισμός 7.** *Θα λέμε ότι ένα πάντα-σταθεροποιούμενο πρωτόκολλο πληθυσμού $\mathcal{A}$ που τρέχει σε ένα γράφο επικοινωνίας $G = (V, E)$* ***υπολογίζει σταθερά μία σχέση εισόδου-εξόδου*** *$R_{\mathcal{A}} \subseteq \mathcal{X} \times \mathcal{Y}$ εάν, για κάθε ανάθεση εισόδου $x \in \mathcal{X}$ και ανάθεση εξόδου $y \in \mathcal{Y}$, η $x$ σχετίζεται με την $y$ μέσω της $R_{\mathcal{A}}$ (δηλαδή, $R_{\mathcal{A}}(x, y)$) εάν και μόνον εάν υπάρχει ένας υπολογισμός του $\mathcal{A}$ που ξεκινάει απ' την αρχική διαμόρφωση $I(x)$ και σταθεροποιείται στην έξοδο $y$. Στην ειδική περίπτωση που η $R_{\mathcal{A}}$ είναι μονοσήμαντη, γράφουμε $F_{\mathcal{A}}(x) = y$ για κάθε*

[6] εάν και μόνον εάν

$(x, y) \in R_{\mathcal{A}}$ *και λέμε ότι το πρωτόκολλο* $\mathcal{A}$ ***υπολογίζει σταθερά την ολική συνάρτηση*** $F_{\mathcal{A}} : \mathcal{X} \to \mathcal{Y}$.

**Ορισμός 8.** *Θα λέμε ότι μία σχέση εισόδου-εξόδου* $R$ *είναι* ***σταθερά υπολογίσιμη*** *ανν υπάρχει κάποιο πρωτόκολλο που υπολογίζει σταθερά την* $R$.

Ας δούμε ένα παράδειγμα για να γίνουν πιο κατανοητοί οι ορισμοί. Έστω ότι στο παράδειγμα του ιχθυοτροφείου υπάρχουν τα ψάρια $u_1, \ldots, u_{101}$ και ότι ο γράφος επικοινωνίας είναι πλήρης. Έστω ότι η ανάθεση εισόδου $x$ περιγράφεται από το διάνυσμα $(1, \ldots, 1, 0, 0)$, δηλαδή αναθέτει στους πράκτορες $u_1, \ldots, u_{99}$ την τιμή $1$ και στους $u_{100}$, $u_{101}$ την τιμή $0$. Η αντίστοιχη διαμόρφωση εισόδου $I(x)$ περιγράφεται από το διάνυσμα $(q_1, \ldots, q_1, q_0, q_0)$. Οποιοσδήποτε υπολογισμός και να διεξαχθεί ξεκινώντας από την $I(x)$ βάσει του πρωτοκόλλου που δώσαμε για το πρόβλημα αυτό και βάσει των επιλογών του εχθρικού δρομολογητή θα καταλήξει σε μία διαμόρφωση $C$ υπό την οποία ένας πράκτορας, έστω χ.β.τ.γ. ο $u_{50}$, θα βρίσκεται στην κατάσταση $q_{99}$, ενώ όλοι οι υπόλοιποι πράκτορες θα βρίσκονται στην κατάσταση $q_0$. Επειδή $O(q_0) = O(q_{99}) = 0$ η διαμόρφωση εξόδου $O(C)$ περιγράφεται από το διάνυσμα $(0, \ldots, 0)$ διάστασης $101$. Επιπρόσθετα, οι μόνοι κανόνες που μπορούν να εφαρμοσθούν από εδώ και πέρα είναι οι $(q_0, q_0) \to (q_0, q_0)$, $(q_{99}, q_0) \to (q_{99}, q_0)$ και $(q_0, q_{99}) \to (q_{99}, q_0)$ πράγμα το οποίο σημαίνει ότι οποιαδήποτε διαμόρφωση προσβάσιμη από την $C$ αντιστοιχεί στην διαμόρφωση εξόδου $(0, 0, \ldots, 0)$. Αυτό σημαίνει ότι η $C$ είναι μία σταθερής-εξόδου διαμόρφωση και ότι ο υπολογισμός σταθεροποιείται στην έξοδο $(0, 0, \ldots, 0)$ (είναι η ανάθεση εξόδου $y_C$ που ορίζεται ως $y_C = 0$ για κάθε $u \in \{u_1, \ldots, u_{101}\}$). Επομένως, ισχύει $R((1, \ldots, 1, 0, 0), (0, 0, \ldots, 0))$, όπου $R$ είναι η σχέση εισόδου-εξόδου που υπολογίζεται απ' το πρωτόκολλο, αφού δείξαμε ότι υπάρχει κάποιος υπολογισμός του πρωτοκόλλου που ξεκινάει από την $(1, \ldots, 1, 0, 0)$ και σταθεροποιείται στην $(0, 0, \ldots, 0)$. Στην πραγματικότητα, αξίζει να παρατηρήσει κανείς ότι η $R$ είναι μονοσήμαντη (και επιπλέον ικανοποιεί την πρόσθετη απαίτηση σύγκλισης που θέσαμε στον Ορισμό 6) και, επομένως, μπορούμε να γράψουμε

$$F(1, \ldots, 1, 0, 0) = (0, 0, \ldots, 0).$$

Το ότι η $R$ είναι μονοσήμαντη σε συνδυασμό με την πρόσθετη απαίτηση σύγκλισης που θέσαμε στον Ορισμό 6, στην περίπτωση της ανάθεσης εισόδου $(1, \ldots, 1\ , 0, 0)$ συνεπάγεται ότι οποιοσδήποτε υπολογισμός δίνει ως έξοδο την ανάθεση εξόδου $(0, 0, \ldots, 0)$ (αξίζει να αναφέρουμε ότι χωρίς την πρόσθετη απαίτηση, το πρωτόκολλο μπορεί ορισμένες φορές με είσοδο $(1, \ldots, 1\ , 0, 0)$ να μην συνέκλινε σε καμία έξοδο). Επιπρόσθετα, επειδή το πρωτόκολλο αυτό είναι πάντα-σταθεροποιούμενο, εφαρμόζεται και ο Ορισμός 7 και η $F$

είναι στην πραγματικότητα ολική συνάρτηση. Επίσης, παρατηρούμε ότι η σταθερής-εξόδου διαμόρφωση $C$ μπορεί να παράγει διαμορφώσεις με διαφορετικές καταστάσεις, αφού π.χ. η κατάσταση $q_{99}$ μπορεί να περιφέρεται στο δίκτυο. Όμως, αυτό δεν έχει καμία σημασία ως προς την έξοδο του υπολογισμού, αφού αυτή δεν μεταβάλλεται σε καμία από τις διαμορφώσεις που είναι προσβάσιμες απ' την $C$.

## 2.4 Συναρτήσεις με άλλα πεδία ορισμού

Όπως είδαμε, τα πρωτόκολλα πληθυσμών μπορούν να υπολογίσουν μερικές συναρτήσεις από το $\mathcal{X}$ στο $\mathcal{Y}$. Το $\mathcal{X}$ ορίστηκε ως το σύνολο όλων των συναρτήσεων από το $V$ στο $X$. Θα καλούμε το $\mathcal{X}$ *φυσικό πεδίο ορισμού εισόδου* και το $\mathcal{Y}$ *φυσικό πεδίο τιμών εξόδου*.

Για να κάνουμε τα πρωτόκολλα πληθυσμών ικανά να υπολογίζουν συναρτήσεις πάνω σε άλλα πεδία ορισμού και τιμών, χρειαζόμαστε κατάλληλες *παραδοχές εισόδου και εξόδου*. Μία *παραδοχή κωδικοποίησης εισόδου* για το πεδίο ορισμού $D_I$ είναι μία συνάρτηση $E_I : \mathcal{X} \to D_I$ και μία *παραδοχή κωδικοποίησης εξόδου* για το πεδίο τιμών $D_O$ είναι μία συνάρτηση $E_O : \mathcal{Y} \to D_O$. Εάν $E_I(x) = u$ (και αντιστοίχως $E_O(y) = \nu$), λέμε ότι η διαμόρφωση εισόδου $x$ αναπαριστά το $u$ (αντιστοίχως, η διαμόρφωση εξόδου $y$ αναπαριστά το $\nu$). Βάσει αυτής της ορολογίας μπορούμε να ορίσουμε τις φυσικές παραδοχές κωδικοποίησης εισόδου και εξόδου ως τις ταυτοτικές συναρτήσεις πάνω στα $\mathcal{X}$ και $\mathcal{Y}$, αντίστοιχα (στις οποίες κάθε στοιχείο αναπαριστά τον εαυτό του).

Οι παραδοχές $E_I$ και $E_O$ δεν χρειάζεται ούτε να είναι ένα-προς-ένα ούτε επί συναρτήσεις. Συνεπώς, κάθε στοιχείο του $D_I$ (αντιστοίχως του $D_O$) μπορεί να αναπαρίσταται από κανένα, ένα ή και περισσότερα στοιχεία του φυσικού πεδίου ορισμού εισόδου $\mathcal{X}$ (αντιστοίχως του $\mathcal{Y}$). Με φυσικό τρόπο σχετίζουμε με τη σχέση εισόδου-εξόδου $R_\mathcal{A}$ την *αναπαριστάμενη σχέση εισόδου-εξόδου* $S_\mathcal{A} \subseteq D_I \times D_O$, όπου η $S_\mathcal{A}(u, \nu)$ ισχύει εάν και μόνον εάν υπάρχουν $x \in \mathcal{X}$ και $y \in \mathcal{Y}$ τ.ώ. να ικανοποιείται η $R_\mathcal{A}(x, y)$ και επιπλέον $E_I(x) = u$ και $E_O(y) = \nu$ (δηλαδή, η $x$ αναπαριστά την $u$ και η $y$ την $\nu$ βάσει των παραδοχών εισόδου και εξόδου $E_I$ και $E_O$, αντίστοιχα). Λέμε ότι η $R_\mathcal{A}$ είναι (βάσει των παραδοχών κωδικοποίησης $E_I$ και $E_O$) *αντιπροσωπευτικά ανεξάρτητη* (και αντίστοιχα το πρωτόκολλο $\mathcal{A}$ θα καλείται *αντιπροσωπευτικά ανεξάρτητο*) ανν για κάθε $x_1, x_2 \in \mathcal{X}$ τ.ώ. $E_I(x_1) = E_I(x_2)$ (δηλαδή, τα $x_1$, $x_2$ αναπαριστούν το ίδιο στοιχείο του $D_I$),

$$\{E_O(y) | R(x_1, y)\} = \{E_O(y) | R(x_2, y)\}.$$

Με άλλα λόγια, αν δύο αναθέσεις εισόδου $x_1$ και $x_2$ αναπαριστούν το ίδιο στοιχείο $u$ του $D_I$, τότε αν $Y_1$ είναι το σύνολο των αναθέσεων εξόδου για τις

οποίες ισχύει $R(x_1, y)$ και $Y_2$ αυτές για τις οποίες ισχύει $R(x_2, y)$ τότε τα $Y_1$ και $Y_2$ θα πρέπει να έχουν την ίδια εικόνα στο $D_O$ βάσει της $E_O$. Αξίζει να παρατηρήσουμε ότι αν δεν συνέβαινε αυτό, τότε μπορεί να υπήρχαν $x_1$ και $x_2$ που αναπαριστούν και τα δύο το $u$, και η $S_{\mathcal{A}}(u, \nu)$ να ίσχυε μόνο λόγω του $x_1$, δηλαδή να ίσχυε $\nu \in \{E_O(y)|R(x_1, y)\}$ και $\nu \notin \{E_O(y)|R(x_2, y)\}$. Στην περίπτωση αυτή ξεκινώντας από την αρχική διαμόρφωση $I(x_2)$ δεν θα μπορούσαμε ποτέ να πάρουμε ως έξοδο το $\nu$, αφού δεν υπάρχει ανάθεση εξόδου $y$ που να αναπαριστά το $\nu$ τ.ώ. $R(x_2, y)$, παρότι η $x_2$ αναπαριστά το $u$ και παρότι λόγω της $x_1$ ισχύει $S_{\mathcal{A}}(u, \nu)$. Αντίθετα, εάν η $R_{\mathcal{A}}$ είναι αντιπροσωπευτικά ανεξάρτητη και ισχύει η $S_{\mathcal{A}}(u, \nu)$, τότε για κάθε $x$ που αναπαριστά το $u$, υπάρχει $y$ που αναπαριστά το $\nu$ τ.ώ. να ισχύει η $R_{\mathcal{A}}(x, y)$. Θα λέμε ότι το πρωτόκολλο $\mathcal{A}$ *υπολογίζει σταθερά την αναπαριστάμενη σχέση εισόδου-εξόδου* $S_{\mathcal{A}}$ εάν το $\mathcal{A}$ σταθεροποιείται σε κάθε υπολογισμό (εδώ προϋποθέτουμε τη σταθεροποίηση σε κάθε υπολογισμό αντίθετα με ό, τι κάναμε πριν) και είναι αντιπροσωπευτικά ανεξάρτητο. Στην ειδική περίπτωση που η $S_{\mathcal{A}}$ είναι μονοσήμαντη, λέμε ότι το $\mathcal{A}$ *υπολογίζει σταθερά την μερική συνάρτηση* $F_{\mathcal{A}} : D_I \to D_O$.

Με απλά λόγια, εάν το $\mathcal{A}$ υπολογίζει σταθερά την $S_{\mathcal{A}}$, τότε η $S_{\mathcal{A}}(u, \nu)$ ισχύει ανν για κάθε αναπαράσταση του $u$, υπάρχει κάποιος υπολογισμός του $\mathcal{A}$ που ξεκινάει από αυτή την αναπαράσταση και σταθεροποιείται σε μία έξοδο που αναπαριστά το $\nu$. Επιπρόσθετα, αφού όπως υποθέσαμε κάθε υπολογισμός του $\mathcal{A}$ σταθεροποιείται, εάν το $\mathcal{A}$ ξεκινάει με μία αναπαράσταση κάποιου $u \in D_I$, ο υπολογισμός σταθεροποιείται σε μία έξοδο που αναπαριστά κάποιο $\nu \in D_O$. Όταν η $S_{\mathcal{A}}$ είναι μονοσήμαντη, κάθε υπολογισμός που ξεκινάει από μία αναπαράσταση του $u$ σταθεροποιείται πάντοτε σε μία έξοδο που αναπαριστά την $F_{\mathcal{A}}(u)$.

### 2.4.1 Συναρτήσεις πολλών μεταβλητών

Κάθε στοιχείο του $\mathcal{X}$ μπορεί να περιγραφεί από ένα διάνυσμα διάστασης $n$, όπου η $i$-στή συνιστώσα του αντιστοιχεί στην είσοδο του πράκτορα $i$ δεδομένης μίας ολικής διάταξης των πρακτόρων $V = \{1, 2, \ldots, n\}$. Κάθε τέτοιο διάνυσμα είναι ένα στοιχείο του $X^n$. Παρατηρούμε ότι για να μπορέσουμε να πούμε ότι ένα πρωτόκολλο υπολογίζει (σταθερά) μία συνάρτηση πολλών μεταβλητών $f : X^n \to Y^n$ θα πρέπει να κάνουμε δύο παραδοχές. Η πρώτη καλείται *παραδοχή εισόδου-πρακτόρων*, υποθέτει ένα ολικά διατεταγμένο σύνολο $n$ πρακτόρων και αναθέτει το $i$-στό όρισμα της $f$ στον $i$-στό πράκτορα, όπου $1 \leq i \leq n$. Η παραδοχή αυτή είναι απαραίτητη αν θέλουμε ένα πρωτόκολλο να υπολογίζει μία μη-συμμετρική συνάρτηση πολλών μεταβλητών, καθώς από μόνα τους τα στοιχεία του πεδίου ορισμού της δεν δίνουν καμία πληροφορία για το που ανατίθεται κάθε σύμβολο του διατεταγμένου συνόλου που τα περιγράφει. Η δεύτερη καλείται *παραδοχή εξόδου-πρακτόρων*,

υποθέτει την ίδια διάταξη και παίρνει το $i$-στό στοιχείο της τιμής της $f$ από την έξοδο του $i$-στού πράκτορα. Η παραδοχές αυτές δεν χρειάζονταν στην περίπτωση των συνόλων $\mathcal{X}$ και $\mathcal{Y}$, καθώς κάθε στοιχείο του $\mathcal{X}$ ($\mathcal{Y}$) καθορίζει πλήρως την τιμή εισόδου (εξόδου) κάθε πράκτορα του πληθυσμού.

### 2.4.2 Κατηγορήματα πάνω στο $\mathcal{X}$

Ένα κατηγόρημα με πεδίο ορισμού το $\mathcal{X}$ είναι ουσιαστικά μία συνάρτηση από το $\mathcal{X}$ στο $\{0,1\}$. Η *παραδοχή εξόδου κατηγορημάτων* υποθέτει ότι $Y = \{0,1\}$ και απαιτεί όλοι οι πράκτορες να συμφωνούν ως προς την έξοδό τους.

**Ορισμός 9.** *Ένα πρωτόκολλο $\mathcal{A}$ **υπολογίζει σταθερά ένα κατηγόρημα** $p : \mathcal{X} \to \{0,1\}$ αν η σχέση εισόδου-εξόδου του πρωτοκόλλου είναι μονοσήμαντη και για κάθε ανάθεση εισόδου $x \in \mathcal{X}$, αν $p(x) = 1$ τότε $F_{\mathcal{A}}(x)$ είναι η ανάθεση εξόδου που αντιστοιχίζει κάθε πράκτορα στην τιμή 1, αλλιώς $F_{\mathcal{A}}(x)$ είναι η ανάθεση εξόδου που αντιστοιχίζει κάθε πράκτορα στην τιμή 0.*

Να θυμίσουμε ότι με $F_{\mathcal{A}}(x)$ συμβολίζουμε την ανάθεση εξόδου στην οποία σταθεροποιείται κάθε υπολογισμός του πρωτοκόλλου $\mathcal{A}$ με είσοδο $x \in \mathcal{X}$ (επιτρέπεται να μιλήσουμε για σταθεροποίηση κάθε υπολογισμού επειδή η σχέση εισόδου-εξόδου του $\mathcal{A}$ είναι μονοσήμαντη, επομένως μερική συνάρτηση και εφαρμόζεται ο Ορισμός 6).

Διαισθητικά, ένα κατηγόρημα πάνω στο σύνολο των αναθέσεων εισόδου $\mathcal{X}$ διαμερίζει το $\mathcal{X}$ σε δύο υποσύνολα $T_{\mathcal{X}}$ και $F_{\mathcal{X}}$ (διαμερίζει σημαίνει ότι $T_{\mathcal{X}} \cup F_{\mathcal{X}} = \mathcal{X}$ και $T_{\mathcal{X}} \cap F_{\mathcal{X}} = \emptyset$) και είναι *αληθές* για όλα τα στοιχεία του $T_{\mathcal{X}}$ (τα αντιστοιχίζει στην τιμή 1) και *ψευδές* για όλα τα στοιχεία του $F_{\mathcal{X}}$ (τα αντιστοιχίζει στην τιμή 0).

Στο παράδειγμα του ιχθυοτροφείου, το πρωτόκολλο που παρουσιάσαμε υπολογίζει σταθερά το κατηγόρημα που θεωρεί αληθή κάθε ανάθεση εισόδου που αντιστοιχίζει τουλάχιστον 100 πράκτορες στην τιμή 1 (ο ιός $J$ έχει μολύνει τουλάχιστον 100 πράκτορες και το 1 σημαίνει συναγερμός) και ψευδή κάθε άλλη ανάθεση εισόδου. Μία αρκετά απλή απόδειξη ορθότητας του πρωτοκόλλου θα έδειχνε ότι για κάθε $x \in T_{\mathcal{X}}$ το πρωτόκολλο ξεκινώντας από την $I(x)$ καταλήγει πάντοτε (ανεξαρτήτως των επιλογών του δίκαιου δρομολογητή) σε μία σταθερής-εξόδου διαμόρφωση όπου όλοι οι πράκτορες δίνουν ως έξοδο την τιμή 1, ειδοποιούν δηλαδή όλοι για το συναγερμό, ενώ για κάθε $x \in F_{\mathcal{X}}$ πάντοτε όλοι οι πράκτορες δίνουν *τελικά*[7] ως έξοδο την τιμή 0, ειδοποιώντας ότι λιγότερα από 100 ψάρια βρέθηκαν μολυσμένα.

[7]Επειδή ο χρόνος που απαιτείται για να συμβεί κάποιο γεγονός στο υπό εξέταση μοντέλο είναι άγνωστος, θα χρησιμοποιούμε συχνά τη φράση "τελικά συμβαίνει" για να εκφράσουμε τη βεβαιότητα ότι κάποια στιγμή το γεγονός αυτό θα συμβεί ανεξαρτήτως των επιλογών του δρομολογητή.

Έχοντας ορίσει τον σταθερό υπολογισμό κατηγορημάτων είναι εύκολο να δει κανείς ότι η παραδοχή εξόδου κατηγορημάτων γενικεύει στην περίπτωση συναρτήσεων από τις αναθέσεις εισόδου $\mathcal{X}$ στο αλφάβητο εξόδου $Y$. Στην περίπτωση αυτή η *παραδοχή αλφαβήτου εξόδου* υποθέτει οποιοδήποτε πεπερασμένο αλφάβητο εξόδου $Y$ και απαιτεί όλοι οι πράκτορες να συμφωνούν ως προς την εξόδό τους (γενίκευση της παραδοχής εξόδου κατηγορημάτων). Ομοίως με πριν, ένα πρωτόκολλο υπολογίζει σταθερά μία συνάρτηση $f : \mathcal{X} \to Y$ (το $Y$ είναι το αλφάβητο εξόδου και όχι το σύνολο των αναθέσεων εξόδου $\mathcal{Y}$) αν, για κάθε $x \in \mathcal{X}$ τ.ώ. $f(x) = y$, σε κάθε υπολογισμό που ξεκινάει απ' την $I(x)$ τελικά όλοι οι πράκτορες δίνουν ως έξοδο το σύμβολο (τιμή) $y$.

### 2.4.3 Ακέραιες συναρτήσεις

Έστω $f : \mathbb{Z}^k \to \mathbb{Z}^l$ μία μερική συνάρτηση πάνω σε ακέραια διανύσματα. Αυτό που επιθυμούμε είναι να ορίσουμε μία παραδοχή που να μας βοηθάει να χρησιμοποιούμε ως *κωδικοποιήσεις* τα στοιχεία των συνόλων $X$, $Y$ και $Q$ για να διασκορπίσουμε τις ακέραιες τιμές σε όλο τον πληθυσμό. Για παράδειγμα, επιθυμούμε κάθε σύμβολο εισόδου να κωδικοποιεί ένα $k$-διάνυσμα ακεραίων κατά τέτοιον τρόπο ώστε για κάθε ακέραιο διάνυσμα $r$ που ανήκει στο πεδίο ορισμού της $f$, να υπάρχει ανάθεση εισόδου $x \in \mathcal{X}$ τ.ώ. αν αθροίσουμε τις διανυσματικές αναπαραστάσεις των συμβόλων εισόδου που η $x$ αναθέτει στους πράκτορες να προκύπτει το $r$. Παρόμοια *διάχυτη αναπαράσταση* θέλουμε να διατηρείται τόσο κατά την εκτέλεση του υπολογισμού όσο και κατά την ανάγνωση της εξόδου, επομένως, με παρόμοιο τρόπο θα πρέπει να ορίσουμε τα διανύσματα τα οποία κωδικοποιούν οι καταστάσεις και τα σύμβολα εξόδου.

Όπως είπαμε, στο μοντέλο των πρωτοκόλλων πληθυσμών κάθε πράκτορας έχει $\mathcal{O}(1)$ συνολική χωρητικότητα μνήμης και ως εκ τούτου μπορεί να αποθηκεύσει το πολύ $\mathcal{O}(1)$ ακεραίους απόλυτης τιμής το πολύ $\mathcal{O}(1)$ ο καθένας. Με την διάχυτη αναπαράσταση κάθε ακέραιος σπάει σε $\mathcal{O}(1)$ συνιστώσες (αυτές που θα αθροιστούν για να δώσουν τον ακέραιο) κάθε μία εκ των οποίων αποθηκεύεται σε έναν διαφορετικό πράκτορα του πληθυσμού. Αφού κάθε συνιστώσα μπορεί να έχει απόλυτη τιμή το πολύ $\mathcal{O}(1)$ και οι πράκτορες είναι $n$, με την διάχυτη αναπαράσταση ο πληθυσμός μπορεί να αποθηκεύσει έναν ακέραιο απόλυτης τιμής το πολύ $\mathcal{O}(n)$ και επιπρόσθετα κάθε πράκτορας μπορεί να κρατάει $\mathcal{O}(1)$ τέτοιες συνιστώσες από $\mathcal{O}(1)$ διαφορετικούς ακεραίους, άρα η διάχυτη αναπαράσταση μας δίνει τη δυνατότητα να αποθηκεύσουμε στον πληθυσμό ένα διάνυσμα $k = \mathcal{O}(1)$ ακεραίων με την απόλυτη τιμή του κάθε ακεραίου να φράσσεται εκ των άνω από $\mathcal{O}(n)$. Επομένως, στην $f : \mathbb{Z}^k \to \mathbb{Z}^l$ οι διαστάσεις των διανυσμάτων $k$, $l$ εκφράζουν το πλήθος των ακεραίων που καλείται να αποθηκεύσει ο πληθυσμός και ως εκ τούτου πρέπει

να είναι σταθεροί αριθμοί και ανεξάρτητοι του $n$. Αντίθετα, κάθε ακέραιος του διανύσματος θα διασκορπιστεί στον πληθυσμό και συνεπώς μπορεί να έχει απόλυτη τιμή το πολύ $\mathcal{O}(n)$.

Έστω $J$ ένα σύνολο το οποίο θα χρησιμοποιούμε για να συμβολίζουμε είτε το $X$, είτε το $Y$ είτε το $Q$. Μία *$k$-θέσεων παραδοχή κωδικοποίησης ακεραίων πάνω στο $J$* είναι μία αντιστοιχία $\rho : J \to \mathbb{Z}^k$. Επομένως, η $\rho$ αντιστοιχίζει κάθε στοιχείο $j \in J$ σε ένα $k$-διάνυσμα ακεραίων $\vec{z} = (z_1, z_2 \ldots, z_k) \in \mathbb{Z}^k$ και θα λέμε ότι το $j$ *κωδικοποιεί* το διάνυσμα $\vec{z}$. Για παράδειγμα, αν $J = X$ τότε η $\rho^X : X \to \mathbb{Z}^k$ αντιστοιχίζει κάθε σύμβολο εισόδου $x \in X$ στο $k$-διάνυσμα ακεραίων το οποίο θα κωδικοποιεί (ομοίως για $J = Y$ και $J = Q$). Έστω $\mathcal{J} = J^V$ το σύνολο όλων των συναρτήσεων από το $V$ στο $J$. Για παράδειγμα, αν $J = X$ τότε $\mathcal{J} = \mathcal{X}$, δηλαδή το σύνολο όλων των δυνατών αναθέσεων εισόδου (αν $J = Y$ τότε $\mathcal{J} = \mathcal{Y}$, ενώ αν $J = Q$ τότε $\mathcal{J} = \mathcal{C}$, δηλαδή, το σύνολο όλων των δυνατών διαμορφώσεων πληθυσμού). Επεκτείνουμε την $\rho$ σε μία αντιστοιχία από το $\mathcal{J}$ στο $\mathbb{Z}^k$, η οποία για κάθε $\gamma \in \mathcal{J}$ ορίζεται ως:

$$\rho(\gamma) = \sum_{u \in V} \rho(\gamma(u)) \tag{2.1}$$

Ας δούμε πώς ερμηνεύεται ο τύπος (2.1) στην περίπτωση που $J = X$. Στην περίπτωση αυτή η επεκταθείσα $\rho^X$ παίρνει ως είσοδο μία ανάθεση εισόδου $x \in \mathcal{X}$. Για κάθε πράκτορα $u \in V$, $x(u)$ είναι το σύμβολο εισόδου που η $x$ αναθέτει στον $u$. Επομένως, για κάθε $u \in V$, $\rho^X(x(u))$ είναι το $k$-διάνυσμα ακεραίων το οποίο κωδικοποιείται από το σύμβολο που έχει ανατεθεί στον πράκτορα $u$. Συνεπώς, στην περίπτωση αυτή, το $\rho^X(x)$ (τώρα αναφερόμαστε και πάλι στην επεκταθείσα $\rho^X$) δεν είναι τίποτα άλλο από το $k$-διάνυσμα ακεραίων που προκύπτει αθροίζοντας πάνω σε όλους τους πράκτορες το $k$-διάνυσμα ακεραίων που αναπαρίσταται από το σύμβολο εισόδου του κάθε πράκτορα. Θα λέμε ότι το $\rho^X(x)$, που προκύπτει από το άθροισμα των διασκορπισμένων διανυσμάτων, είναι το διάνυσμα που *αναπαρίσταται από* την ανάθεση εισόδου $x$.

Ένα ακέραιο $k$-διάνυσμα εισόδου κωδικοποιείται από μία $k$-θέσεων παραδοχή κωδικοποίησης $\rho^X$ πάνω στο αλφάβητο εισόδου $X$. Ένα ακέραιο $l$-διάνυσμα εξόδου κωδικοποιείται από μία $l$-θέσεων παραδοχή κωδικοποίησης $\rho^Y$ πάνω στο αλφάβητο εξόδου $Y$. Κατά τη διάρκεια του υπολογισμού, ο πληθυσμός μπορεί να διατηρεί ένα ακέραιο $m$-διάνυσμα που, αντιστοίχως, κωδικοποιείται από την $\rho^Q$ πάνω στο σύνολο καταστάσεων $Q$.

Δεδομένων των προαναφερθέντων παραδοχών κωδικοποίησης μπορούμε να δώσουμε τον ακόλουθο ορισμό για τον σταθερό υπολογισμό ακέραιων συναρτήσεων απ' τα πρωτόκολλα πληθυσμών:

**Ορισμός 10.** *Ένα πρωτόκολλο πληθυσμού $\mathcal{A}$ υπολογίζει σταθερά μία συνάρτηση $f : \mathbb{Z}^k \to \mathbb{Z}^l$ αν ικανοποιούνται οι ακόλουθες συνθήκες:*

1. *Για κάθε* $r \in \mathbb{Z}^k$ *στο πεδίο ορισμού της* $f$*, υπάρχει ανάθεση εισόδου* $x \in \mathcal{X}$ *τ.ώ.* $\rho^X(x) = r$*.*

2. *Για κάθε* $x \in \mathcal{X}$*, αν το* $\rho^X(x)$ *ανήκει στο πεδίο ορισμού της* $f$ *τότε υπάρχει ανάθεση εξόδου* $y \in \mathcal{Y}$ *τ.ώ. να ικανοποιείται η* $R_{\mathcal{A}}(x, y)$*.*

3. *Για κάθε* $x \in \mathcal{X}$ *και* $y \in \mathcal{Y}$*, αν ικανοποιείται η* $R_{\mathcal{A}}(x, y)$ *τότε* $\rho^Y(y) = f(\rho^X(x))$*.*

Η πρώτη συνθήκη εξασφαλίζει ότι κάθε ακέραιο διάνυσμα στο πεδίο ορισμού της $f$ αναπαρίσταται (μέσω της επεκταθείσας $\rho^X$) από κάποια ανάθεση εισόδου. Η δεύτερη συνθήκη εξασφαλίζει ότι εάν μια ανάθεση εισόδου $x$ αναπαριστά κάποιο ακέραιο διάνυσμα απ' το πεδίο ορισμού της $f$ (κάποιες αναθέσεις εισόδου μπορεί να μην αναπαριστούν κανένα διάνυσμα) τότε υπάρχει ανάθεση εξόδου στην οποία σταθεροποιείται κάποιος υπολογισμός του $\mathcal{A}$ που ξεκινάει απ' την $I(x)$ και δεν υπάρχει υπολογισμός που ξεκινάει απ' την $I(x)$ και δεν σταθεροποιείται (αν υπήρχε τέτοιος τότε σε ορισμένες περιπτώσεις το πρωτόκολλο δεν θα υπολόγιζε καμία έξοδο). Παρατηρούμε ότι η δεύτερη συνθήκη επιτρέπει την ύπαρξη ενός υποσυνόλου $\{y_1, y_2, \ldots, y_t\} \subseteq \mathcal{Y}$ τ.ώ. για κάθε $y \in \{y_1, y_2, \ldots, y_t\}$ να ικανοποιείται η $R_{\mathcal{A}}(x, y)$. Δεδομένου αυτού, η τρίτη συνθήκη εξασφαλίζει ότι κάθε $y \in \{y_1, y_2, \ldots, y_t\}$, δηλαδή κάθε $y$ για το οποίο υπάρχει υπολογισμός του $\mathcal{A}$ που ξεκινάει απ' την $I(x)$ και δίνει έξοδο $y$, αναπαριστά το ακέραιο διάνυσμα που επιστρέφει η $f$ με είσοδο $\rho^X(x)$. Το ότι η ίδια ανάθεση εισόδου $x$ μπορεί να οδηγεί σε πολλές αναθέσεις εξόδου $\{y_1, y_2, \ldots, y_t\}$ για διαφορετικούς υπολογισμούς δείχνει ότι ένα πρωτόκολλο $\mathcal{A}$ μπορεί να υπολογίζει σταθερά μία ακέραια συνάρτηση $f$ ακόμα και αν η σχέση εισόδου-εξόδου $R_{\mathcal{A}}$ δεν είναι μονοσήμαντη. Για παράδειγμα, μπορεί να ισχύει $r = \rho^X(x) \in \mathbb{Z}^k$ και $R_A(x, y_1), R_A(x, y_2), \ldots, R_A(x, y_t)$ για $y_1 \neq y_2 \neq \ldots \neq y_t$, αλλά $\rho^Y(y_1) = \rho^Y(y_2) = \ldots = \rho^Y(y_t) = f(r)$ (συνεπώς, παρότι η ίδια ανάθεση εξόδου $x$ που αναπαριστά κάποιο $r$ απ' το πεδίο ορισμού της $f$ οδηγεί σε αρκετές αναθέσεις εξόδου για διαφορετικούς υπολογισμούς, όλες αναπαριστούν την $f(r)$).

Συνοψίζοντας, για να υπολογίζει σταθερά ένα πρωτόκολλο $\mathcal{A}$ μία ακέραια συνάρτηση $f$, θα πρέπει, πρώτα απ' όλα, κάθε στοιχείο του πεδίου ορισμού της $f$ να αναπαρίσταται από κάποια ανάθεση εισόδου. Επιπρόσθετα, για κάθε ανάθεση εισόδου που αναπαριστά ένα στοιχείο του πεδίου ορισμού της $f$, θα πρέπει κάθε υπολογισμός του $\mathcal{A}$ ξεκινώντας απ' την αρχική διαμόρφωση που αντιστοιχεί στην ανάθεση αυτή να σταθεροποιείται σε κάποια ανάθεση εξόδου (ίσως σε διαφορετική κάθε υπολογισμός) και, τέλος, όλες αυτές οι αναθέσεις εξόδου θα πρέπει να αναπαριστούν την τιμή της $f$ με είσοδο το στοιχείο του πεδίου ορισμού της που αναπαριστά η ανάθεση εισόδου.

### 2.4.4 Συμβολοσειρές

Είσοδοι που είναι συμβολοσειρές αναπαρίστανται διάχυτα στον πληθυσμό, με το $i$-στό σύμβολο να ανατίθεται στον $i$-στό πράκτορα. Για το λόγω αυτό υποθέτουμε ένα διατεταγμένο σύνολο πρακτόρων της μορφής $V = \{u_1, \ldots, u_n\}$ και ένα αυθαίρετο αλφάβητο εισόδου $X = \{\sigma_1, \ldots, \sigma_k\}$. Η *παραδοχή συμβολοσειράς εισόδου* ορίζει $D_I = X^*$ και $E_I(x) = x(u_1)x(u_2)\cdots x(u_n)$, όπου $x \in \mathcal{X}$. Για παράδειγμα, αν η ανάθεση εισόδου $x$ αναθέτει στον $u_1$ το σύμβολο $a$, στον $u_2$ το σύμβολο $b$, στον $u_3$ το σύμβολο $c$ και σε όλους τους υπόλοιπους πράκτορες το σύμβολο $d$ τότε η $x$ αναπαριστά τη συμβολοσειρά $abcddddd\cdots d$.

## 2.5 Βασικό Μοντέλο Πρωτοκόλλων Πληθυσμών

Στην ενότητα αυτή θα επικεντρώσουμε το ενδιαφέρον μας στην όλων-των-ζευγών οικογένεια κατευθυνόμενων γράφων επικοινωνίας ($G^d_{All}$).

**Ορισμός 11.** *Το μοντέλο των πρωτοκόλλων πληθυσμών που υποθέτει γράφους επικοινωνίας από την οικογένεια $G^d_{All}$ καλείται* ***βασικό μοντέλο πρωτοκόλλων πληθυσμών***.[8]

Σε αυτή την ενότητα θα παρουσιάσουμε κάποια πρώτα αποτελέσματα σχετικά με την υπολογιστική ισχύ του βασικού μοντέλου πρωτοκόλλων πληθυσμών (βλέπε [3] και [4]), ενώ στο επόμενο κεφάλαιο θα ασχοληθούμε εξ' ολοκλήρου με το θέμα αυτό, όπου και θα παρουσιάσουμε τα αποτελέσματα του πλήρους χαρακτηρισμού της κλάσης κατηγορημάτων που υπολογίζονται απ' το βασικό μοντέλο σύμφωνα με το [6].

Έστω $\pi$ μία αντιμετάθεση του $V$, δηλαδή, μία ένα-προς-ένα συνάρτηση από το $V$ στο $V$.[9] Παρατηρούμε ότι λόγω της απόλυτης συμμετρίας μεταξύ των πρακτόρων του βασικού μοντέλου πρωτοκόλλων πληθυσμών, οι σχέσεις εισόδου-εξόδου που υπολογίζονται σταθερά παραμένουν αμετάβλητες κάτω από οποιαδήποτε μετονομασία των πρακτόρων, δηλαδή αν $R_{\mathcal{A}}(x, y)$, τότε $R_{\mathcal{A}}(x \circ \pi, y \circ \pi)$ για κάθε αντιμετάθεση $\pi$ του $V$. Στην ειδική περίπτωση των κατηγορημάτων η ανάθεση εξόδου $y : V \to Y$ είναι μία σταθερή συνάρτηση, αφού είτε αντιστοιχίζει όλους τους πράκτορες στην τιμή $0$ είτε όλους τους πράκτορες στην τιμή $1$. Αυτό συνεπάγεται ότι σε αυτή την περίπτωση $y \circ \pi = y$ για κάθε αντιμετάθεση $\pi$ του $V$ και η έξοδος αποφασίζεται από το πολυσύνολο των συμβόλων εισόδου (αφού, λόγω της συμμετρίας, δεν έχει

[8] Στο [4] αναφέρεται και ως *τυπικό μοντέλο*.

[9] Επειδή το πεδίο ορισμού και το σύνολο τιμών της $\pi$ έχουν τον ίδιο πληθάριθμο, μία ένα-προς-ένα συνάρτηση από το $V$ στο $V$ είναι μία αμφιμονοσήμαντη αντιστοιχία από το $V$ στο $V$ (δηλαδή η $\pi$ είναι και επί συνάρτηση).

καμία σημασία σε ποιόν πράκτορα ανατίθεται αρχικά κάθε σύμβολο). Επομένως, στο βασικό μοντέλο, τα κατηγορήματα που υπολογίζονται σταθερά είναι της μορφής $p : X^n \to \{0,1\}$, όπου $p(x_1) = p(x_2)$ για κάθε $x_1, x_2 \in X^n$ με $x_1 \neq x_2$, τ.ώ. τα $x_1$ και $x_2$ περιέχουν τα ίδια σύμβολα εισόδου με διαφορετική διάταξη και συνεπώς τα κατηγορήματα που υπολογίζονται σταθερά από το βασικό μοντέλο είναι *συμμετρικά*. Είναι πολύ σημαντικό να παρατηρήσει κανείς ότι το βασικό μοντέλο δεν μπορεί να υπολογίσει σταθερά ένα μη-συμμετρικό κατηγόρημα αφού, λόγω της ανωνυμίας των πρακτόρων και της συμμετρίας του πλήρους γράφου επικοινωνίας, δεν μπορεί να ξεχωρίσει μία ανάθεση εισόδου από κάποια αντιμετάθεσή της.

Υποθέτουμε ότι ο πληθυσμός είναι $V_n = \{1, 2, \ldots, n\}$ και ο γράφος επικοινωνίας είναι $G_n = (V_n, E_n)$, όπου $E_n = \{(u, v) \mid u, v \in V \text{ και } u \neq v\}$, δηλαδή, ο $G_n$ είναι ο πλήρης κατευθυνόμενος γράφος πάνω στο σύνολο $V_n$.

Έστω $\{f_n\}$ μία οικογένεια Boolean συναρτήσεων τ.ώ. $f_n : \{0,1\}^n \to \{0,1\}$ για κάθε $n \geq 1$. Ένα πρωτόκολλο πληθυσμού $\mathcal{A}$ *υπολογίζει σταθερά την οικογένεια* $\{f_n\}$, εάν για κάθε $n \geq 1$, όταν το $\mathcal{A}$ τρέχει στο γράφο $G_n$ υπολογίζει σταθερά τη συνάρτηση $f_n$ δεδομένης της παραδοχής εισόδου-πρακτόρων (ο πράκτορας $i$ παίρνει το $i$-στό όρισμα) και της παραδοχής εξόδου κατηγορημάτων (τελικά όλοι οι πράκτορες συμφωνούν στη σωστή έξοδο). Σύμφωνα με τα προαναφερθέντα, κάθε σταθερά υπολογίσιμη οικογένεια Boolean συναρτήσεων είναι συμμετρική.

Γενικότερα, μπορούμε να θεωρήσουμε και γλώσσες αντί για κατηγορήματα αφού κάθε γλώσσα $L$ με στοιχεία από το $X^*$ (το σύνολο όλων των πεπερασμένων συμβολοσειρών που σχηματίζονται από τα σύμβολα εισόδου), που δηλαδή είναι $L \subseteq X^*$, αντιστοιχεί στο κατηγόρημα $p_L : X^n \to \{0,1\}$ που ορίζεται ως $p_L(x_1, \ldots, x_n) = 1$ ανν $x_1 x_2 \cdots x_n \in L$. Θα λέμε ότι ένα πρωτόκολλο $\mathcal{A}$ *αποδέχεται τη γλώσσα* $L$ αν, για κάθε $n \geq 1$, όταν το $\mathcal{A}$ τρέξει στο γράφο επικοινωνίας $G_n$, υπολογίζει σταθερά το κατηγόρημα $p_{n,L} : X^n \to \{0,1\}$, που ορίζεται ως $p_{n,L}(x) = p_L(x)$ για κάθε $x \in X^n$ (δηλαδή, το κατηγόρημα που ορίζει ποιες συμβολοσειρές μεγέθους $n$ περιλαμβάνει η $L$, επιστρέφοντας γι' αυτές την τιμή 1), δεδομένων των παραδοχών εισόδου-πρακτόρων και εξόδου κατηγορημάτων.

Ένας παρόμοιος ορισμός που λαμβάνει υπ' όψιν την παραδοχή συμβολοσειράς εισόδου είναι ο εξής: Έστω $\chi_L$ η χαρακτηριστική συνάρτηση της γλώσσας $L$, δηλαδή $\chi_L(\sigma) = 1$ ανν $\sigma \in L$. Λέμε ότι ένα πρωτόκολλο $\mathcal{A}$ αποδέχεται την $L$ ανν το $\mathcal{A}$ υπολογίζει σταθερά το κατηγόρημα $\chi_L$ υπό την παραδοχή συμβολοσειράς εισόδου, δηλαδή, για κάθε $x \in \mathcal{X}$, το $\mathcal{A}$ αποδέχεται την $x$ ανν η συμβολοσειρά $E_I(x)$ την οποία αναπαριστά η $x$ βάσει της παραδοχής συμβολοσειράς εισόδου $E_I$ ανήκει στην $L$.

Μία γλώσσα $L$ είναι *αποδεκτή* απ' το βασικό μοντέλο ανν υπάρχει βασικό πρωτόκολλο (βασικό πρωτόκολλο θα λέμε ένα πρωτόκολλο που τρέχει στο

βασικό μοντέλο) που την αποδέχεται.

**Πόρισμα 2.** *Αν η μία γλώσσα $L \subseteq X^*$ είναι αποδεκτή από το βασικό μοντέλο πρωτοκόλλων πληθυσμών, τότε, για κάθε συμβολοσειρά $x \in L$, η $L$ περιέχει και όλες τις αντιμεταθέσεις της $x$ (δηλαδή, η $L$ είναι **συμμετρική**).*

*Απόδειξη.* Αφού η $L$ είναι σταθερά υπολογίσιμη από το βασικό μοντέλο, υπάρχει πρωτόκολλο $\mathcal{A}$ που για κάθε $n$ υπολογίζει σταθερά το $p_{n,L}$ στον $G_n$. Όμως, τα κατηγορήματα που υπολογίζονται σταθερά από το βασικό μοντέλο είναι συμμετρικά. Άρα, αν $p_{n,L}(x) = 1$ για κάποιο $x \in X^n$ τότε $p_{n,L}(x') = 1$ για κάθε αντιμετάθεση $x'$ του $x$. Για κάθε συμβολοσειρά $x_1x_2 \dots x_n$ της $L$ μεγέθους $n$, ισχύει ότι $p_{n,L}(x_1, x_2, \dots, x_n) = 1$ και, για κάθε $x' = (x'_1, x'_2, \dots, x'_n)$, αν $p_{n,L}(x') = 1$ τότε η συμβολοσειρά $x'_1x'_2 \dots x'_n$ ανήκει στην $L$. Επίσης, όλες οι αντιμεταθέσεις της $(x_1, x_2, \dots, x_n)$ αντιστοιχούν σε όλες τις αντιμεταθέσεις της συμβολοσειράς $x_1x_2 \dots x_n$ και αντιστρόφως. Σύμφωνα με τα παραπάνω, αν $x_1x_2 \dots x_n \in L$ τότε, αν $x = (x_1, x_2, \dots, x_n)$, $p_{n,L}(x) = 1$, άρα $p_{n,L}(x') = 1$ για κάθε αντιμετάθεση της $x$ (αφού το $p_{n,L}$ είναι συμμετρικό) και εφόσον κάθε $x'$ αντιστοιχεί σε μία διαφορετική αντιμετάθεση της συμβολοσειράς $x_1x_2 \dots x_n$, κάθε αντιμετάθεση της $x_1x_2 \dots x_n$ ανήκει στην $L$. □

Το μόνο που έχει σημασία σχετικά με την αποδοχή συμμετρικών γλωσσών είναι το πλήθος των εμφανίσεων κάθε συμβόλου στην είσοδο. Έστω $X = \{\sigma_1, \dots, \sigma_k\}$ και $\sigma \in X^*$. Η *αντιστοιχία Parikh*, $\Psi : X^* \to \mathbb{N}^k$, αντιστοιχίζει τη $\sigma$ στο διάνυσμα $(n_1, \dots, n_k)$, όπου το $n_i$ είναι ίσο με το πλήθος των εμφανίσεων του συμβόλου $\sigma_i$ στη $\sigma$.

**Λήμμα 3.** *Έστω $L$ μία συμμετρική γλώσσα πάνω στο αλφάβητο $\Sigma$ μεγέθους $k$. Τότε ένα πρωτόκολλο πληθυσμού $\mathcal{A}$ αποδέχεται την $L$ ανν το $\Psi(L)$ υπολογίζεται σταθερά από το $\mathcal{A}$ υπό την παραδοχή καταμέτρησης συμβόλων εισόδου.*

*Απόδειξη.* $\Psi(L) = \{\Psi(\sigma) | \sigma \in L\}$, δηλαδή αποτελείται από όλα τα $(n_1, \dots, n_k)$ τ.ώ. $\exists \sigma \in L$ όπου το $n_i$ εκφράζει τον αριθμό εμφανίσεων του $\sigma_i$ στην $\sigma$. Επεκτείνουμε το $\Psi(L)$ στο κατηγόρημα $\Psi(L) : \mathbb{N}^k \to \{0, 1\}$, όπου $\Psi(L)(n_1, \dots, n_k) = 1$ ανν $(n_1, \dots, n_k) \in \Psi(L)$. Αν το $\mathcal{A}$ υπολογίζει σταθερά το $\Psi(L)$ υπό την παραδοχή καταμέτρησης συμβόλων εισόδου δίνει ως έξοδο την τιμή 1 ανν η ανάθεση εισόδου $x$ αναπαριστά κάποιο $(n_1, \dots, n_k) \in \Psi(L)$ (αν $E_I$ είναι η παραδοχή καταμέτρησης συμβόλων εισόδου, $E_I(x) = (n_1, \dots, n_k)$). Όμως, το $x$ σύμφωνα με την παραδοχή συμβολοσειράς εισόδου αναπαριστά και κάποια συμβολοσειρά $\sigma_x = \sigma_1 \cdots \sigma_n$ και ισχύει ότι $E_I(x) = \Psi(\sigma_1, \dots, \sigma_n)$, αφού $\Psi(\sigma_1, \dots, \sigma_n) = (n_1, \dots, n_k)$ (η $E_I$ απλώς μετράει τις εμφανίσεις κάθε συμβόλου στην ανάθεση εισόδου $x$ ενώ η $\Psi$ μετράει τις εμφανίσεις κάθε συμβόλου στην συμβολοσειρά που αναπαριστά η $x$ και ως εκ τούτου προκύπτει το ίδιο $k$-διάνυσμα φυσικών).

Με βάση τα όσα είπαμε, παρατηρούμε ότι: "Το $\mathcal{A}$ υπολογίζει σταθερά το $\Psi(L)$ υπό την παραδοχή καταμέτρησης συμβόλων εισόδου" $\Leftrightarrow$ "για κάθε $x \in \mathcal{X}$ δίνει ως έξοδο 1 ανν $E_I(x) \in \Psi(L)$" $\Leftrightarrow$ "για κάθε $x \in \mathcal{X}$ δίνει ως έξοδο 1 ανν $\Psi(\sigma_x) \in \Psi(L)$" $\Leftrightarrow$ "για κάθε $x \in \mathcal{X}$ δίνει ως έξοδο 1 ανν $\sigma_x \in L$" $\Leftrightarrow$ "αποδέχεται την $L$". □

### 2.5.1 Σταθερά Υπολογίσιμα Κατηγορήματα

Για να μελετήσουμε ποιες συναρτήσεις μπορούν να υπολογιστούν σταθερά απ' το βασικό μοντέλο πρωτοκόλλων πληθυσμών μπορούμε χ.β.τ.γ. να επικεντρώσουμε το ενδιαφέρον μας στη μελέτη κατηγορημάτων (που δεν είναι τίποτα άλλο από συναρτήσεις με σύνολο τιμών το $Y = \{0, 1\}$). Αυτό οφείλεται στο ακόλουθο αποτέλεσμα:

**Θεώρημα 3.** *Έστω μία συμμετρική συνάρτηση $f : X^n \to Y$ και έστω $P_{f,y} : X^n \to \{0, 1\}$ ένα κατηγόρημα που ορίζεται ως $P_{f,y}(x) = 1$ ανν $f(x) = y$ (δηλαδή, $P_{f,y}(x') = 0$ για κάθε $f(x') \neq y$). Τότε, η $f$ είναι (σταθερά) υπολογίσιμη ανν το $P_{f,y}$ είναι υπολογίσιμο για κάθε $y \in Y$.*

*Απόδειξη.* Το "μόνον εάν" μέρος είναι τετριμμένο. Αφού η $f$ είναι σταθερά υπολογίσιμη, για κάθε $x \in X^n$ ο υπολογισμός δίνει ως έξοδο το $f(x)$ και κάθε κατηγόρημα $P_{f,y}$ με $y = f(x)$ δίνει έξοδο 1, ενώ όλα τα υπόλοιπα κατηγορήματα δίνουν έξοδο 0. Για το "εάν" μέρος, αν το $P_{f,y}$ είναι υπολογίσιμο για κάθε $y \in Y$, τότε τρέχουμε παράλληλα τα αντίστοιχα πρωτόκολλά τους χρησιμοποιώντας μία ξεχωριστή συνιστώσα στην κατάσταση κάθε πράκτορα για κάθε $y$. Η από κοινού συνάρτηση μετάβασης προκύπτει από τη σύνθεση των συναρτήσεων μετάβασης όλων των πρωτοκόλλων. Το $Y$ είναι εξ' ορισμού πεπερασμένο, άρα και οι νέες καταστάσεις είναι πεπερασμένες. Σε κάθε υπολογισμό των $P_{f,y}$ για κάποια είσοδο $x$, ένα μόνο εξ' αυτών αποδέχεται (όλοι οι πράκτορές του δίνουν έξοδο 1), καθώς αν αποδέχονταν τα $P_{f,y_1}$ και $P_{f,y_2}$, τότε θα ίσχυε $P_{f,y_1}(x) = P_{f,y_2}(x) = 1$ το οποίο συνεπάγεται ότι $y_1 = y_2 = f(x)$. Επομένως, το μοναδικό κατηγόρημα $P_{f,y}$ που αποδέχεται κάθε φορά με είσοδο $x$ δίνει την τιμή της συνάρτησης για είσοδο $x$, αφού $f(x) = y$. □

#### Ιδιότητες Κλειστότητας

Ας εξετάσουμε αρχικά ποιες οικογένειες Boolean συναρτήσεων είναι σταθερά υπολογίσιμες.

**Λήμμα 4.** *Έστω ότι $\{f_n\}$ και $\{g_n\}$ είναι οικογένειες Boolean συναρτήσεων τ.ώ. $f_n, g_n : \{0, 1\}^n \to \{0, 1\}$, για κάθε $n \geq 1$. Εάν οι $\{f_n\}$ και $\{g_n\}$ είναι σταθερά υπολογίσιμες, τότε το ίδιο ισχύει και για τις $\{\neg f_n\}$, $\{f_n \wedge g_n\}$, και $\{f_n \vee g_n\}$.*

*Απόδειξη.* Έστω $\mathcal{A}$ και $\mathcal{B}$ τα πρωτόκολλα που υπολογίζουν τις $\{f_n\}$ και $\{g_n\}$, αντίστοιχα. Αφού το $\mathcal{A}$ υπολογίζει σταθερά την $\{f_n\}$, για κάθε γράφο $G_n$ στον οποίο τρέχει υπολογίζει σταθερά την $f_n$. Δηλαδή, για κάθε $x \in \{0,1\}^n$ τ.ώ. $f_n(x) = 1$ όλοι οι πράκτορες συμφωνούν τελικά στην έξοδο 1, αλλιώς όλοι οι πράκτορες συμφωνούν στην έξοδο 0. Η $\neg f_n$ ορίζεται ως $\neg f_n(x) = 1 - f_n(x)$. Άρα, αν θεωρήσουμε το πρωτόκολλο $\mathcal{A}'$ που είναι ίδιο με το $\mathcal{A}$ μόνο που η συνάρτηση εξόδου του ορίζεται ως $O_{\mathcal{A}'}(q) = 1 - O_{\mathcal{A}}(q)$ για κάθε $q \in Q_{\mathcal{A}} = Q_{\mathcal{A}'}$, τότε το $\mathcal{A}'$ απαντάει πάντα το αντίθετο απ᾽ το $\mathcal{A}$ και ως εκ τούτου υπολογίζει σταθερά την $\neg f_n$ και αφού αυτό ισχύει για κάθε $n$ υπολογίζει σταθερά την $\{\neg f_n\}$. Τρέχοντας τα $\mathcal{A}$ και $\mathcal{B}$ παράλληλα στην ίδια είσοδο (το ένα αγνοεί την ύπαρξη του άλλου), οι καταστάσεις των πρακτόρων σπάνε σε δύο συνιστώσες όπου χ.β.τ.γ. η πρώτη ανήκει στο $\mathcal{A}$ και η δεύτερη στο $\mathcal{B}$. Έστω $\mathcal{C}$ το από κοινού πρωτόκολλο. Αν $O_{\mathcal{C}}((q_{\mathcal{A}}, q_{\mathcal{B}})) = 1$ ανν $O_{\mathcal{A}}(q_{\mathcal{A}}) = 1$ και $O_{\mathcal{B}}(q_{\mathcal{B}}) = 1$ για κάθε $(q_{\mathcal{A}}, q_{\mathcal{B}}) \in Q_{\mathcal{A}} \times Q_{\mathcal{B}}$, τότε το $\mathcal{C}$ υπολογίζει την $\{f_n \wedge g_n\}$. Ομοίως, αν $O_{\mathcal{C}}((q_{\mathcal{A}}, q_{\mathcal{B}})) = 1$ ανν $O_{\mathcal{A}}(q_{\mathcal{A}}) = 1$ ή $O_{\mathcal{B}}(q_{\mathcal{B}}) = 1$ για κάθε $(q_{\mathcal{A}}, q_{\mathcal{B}}) \in Q_{\mathcal{A}} \times Q_{\mathcal{B}}$, τότε το $\mathcal{C}$ υπολογίζει την $\{f_n \vee g_n\}$. □

Το Λήμμα 4 δείχνει ότι δεδομένου ενός πρωτοκόλλου που υπολογίζει σταθερά το κατηγόρημα "τουλάχιστον 100 ψάρια μολυσμένα" μπορούμε άμεσα να έχουμε και ένα πρωτόκολλο για το "λιγότερα από 100 ψάρια μολυσμένα", "τουλάχιστον 100 ψάρια υγειή", "το πολύ 100 ψάρια υγειή" (π.χ. ως "λιγότερα από 101 ψάρια υγειή"), "ακριβώς 100 ψάρια υγειή" (ως "το πολύ και τουλάχιστον 100 ψάρια υγειή"), "ακριβώς 100, 200 ή 300 ψάρια υγειή" κ.ο.κ.

Με άλλα λόγια

**Πόρισμα 3.** *Η κλάση των σταθερά υπολογίσιμων οικογενειών Boolean συναρτήσεων από το βασικό μοντέλο είναι κλειστή ως προς το συμπλήρωμα την τομή και την ένωση.*

### Ισοτιμία

Έστω τώρα ότι θέλουμε να κατασκευάσουμε ένα πρωτόκολλο που να δίνει έξοδο 1 αν υπάρχει περιττό πλήθος από 1 στην είσοδο και 0 αν υπάρχει άρτιο πλήθος από 1 στην είσοδο, δηλαδή τη συνάρτηση (κατηγόρημα) ισοτιμίας.

Οι καταστάσεις των πρακτόρων αποτελούνται από δύο συνιστώσες. Η πρώτη είναι το δυαδικό *ψηφίο δεδομένων* και η δεύτερη το δυαδικό *ψηφίο επαγρύπνησης*. Αρχικά, η είσοδος κάθε πράκτορα καταγράφεται στο ψηφίο δεδομένων της κατάστασής του, ενώ τα ψηφία επαγρύπνησης όλων των πρακτόρων έχουν την τιμή 1. Θα λέμε ότι ένας πράκτορας που έχει ψηφίο επαγρύπνησης 1 είναι *άγρυπνος*, ενώ ένας πράκτορας που έχει ψηφίο επαγρύπνησης 0 *κοιμάται* (ή είναι στην *κατάσταση ύπνου*). Όταν δύο άγρυπνοι

πράκτορες αλληλεπιδρούν, ο ένας απ' αυτούς περνάει στην κατάσταση ύπνου ενώ ο άλλος θέτει το ψηφίο δεδομένων του στο mod $2$ άθροισμα των ψηφίων δεδομένων τους (επομένως, αν ο ένας έχει $0$ και ο άλλος $1$ καταγράφει $1$, αλλιώς καταγράφει $0$). Παρατηρούμε ότι το mod $2$ άθροισμα των αρχικών ψηφίων δεδομένων (εισόδων) είναι 0 ανν η είσοδος περιέχει άρτιο πλήθος από $1$, αλλιώς είναι $1$. Απ' την στιγμή που ένας πράκτορας περάσει στην κατάσταση ύπνου το μόνο που κάνει είναι να αντιγράφει το ψηφίο δεδομένων των άγρυπνων πρακτόρων με τους οποίους αλληλεπιδρά. Παρατηρούμε ότι τελικά στον πληθυσμό θα παραμείνει μόνο ένας άγρυπνος πράκτορας και όλοι οι υπόλοιποι θα είναι στην κατάσταση ύπνου, αφού σε κάθε αλληλεπίδραση δύο άγρυπνων πρακτόρων ένας απ' αυτούς περνάει στην κατάσταση ύπνου. Όλοι οι πράκτορες τελικά θα αποκτήσουν το ψηφίο δεδομένων του μοναδικού άγρυπνου πράκτορα. Η τιμή εξόδου ενός πράκτορα είναι το ψηφίο δεδομένων του και ως εκ τούτου αφού όλοι θα έχουν τελικά το ίδιο ψηφίο δεδομένων, όλοι θα συμφωνούν στην ίδια έξοδο και η παραδοχή εξόδου κατηγορημάτων ικανοποιείται. Για να πειστούμε ότι η κοινή αυτή έξοδος είναι πάντοτε σωστή, αρκεί να παρατηρήσουμε ότι σε κάθε βήμα το mod $2$ άθροισμα των ψηφίων δεδομένων των άγρυπνων πρακτόρων παραμένει αμετάβλητο και ίσο με το αρχικό mod $2$ άθροισμα των ψηφίων εισόδου. Άρα, πάντοτε ο τελικός μοναδικός άγρυπνος πράκτορας θα έχει το σωστό ψηφίο δεδομένων που θα διαδοθεί σε όλο τον πληθυσμό.

Γενικά, αν γενικεύσουμε την ιδέα του ψηφίου επαγρύπνησης αποδεικνύεται ότι κάθε συμμετρική κανονική γλώσσα είναι αποδεκτή από το βασικό μοντέλο, π.χ. το πρόβλημα της απόφασης του εάν το πλήθος των $1$ στην είσοδο είναι $i$ modulo $m$ για σταθερές $i$ και $m$.

### Πλειοψηφία

Η συνάρτηση (κατηγόρημα) πλειοψηφίας παίρνει την τιμή $1$ αν υπάρχουν περισσότερα $1$ απ' ότι $0$ στην είσοδο, αλλιώς παίρνει την τιμή $0$. Θα περιγράψουμε ένα πρωτόκολλο που υπολογίζει σταθερά τη συνάρτηση πλειοψηφίας.

Το πρωτόκολλο αυτό βασίζεται και πάλι στην πολύ έξυπνη ιδέα του ψηφίου επαγρύπνησης. Οι καταστάσεις των πρακτόρων αποτελούνται από δύο συνιστώσες όπου η πρώτη είναι το ψηφίο-μετρητής και η δεύτερη το ψηφίο επαγρύπνησης. Αρχικά, όποιος πράκτορας διαβάσει είσοδο $0$ θέτει το μετρητή στο $-1$ και όποιος διαβάσει $1$ θέτει το μετρητή στο $1$, ενώ το ψηφίο επαγρύπνησης όλων των πρακτόρων είναι στο $1$. Παρατηρούμε ότι στην αρχική διαμόρφωση αν το άθροισμα των μετρητών είναι θετικό, τότε υπάρχουν περισσότερα $1$ από $0$ στην είσοδο, αλλιώς το πλήθος των $0$ είναι τουλάχιστον ίσο με το πλήθος των $1$. Όταν δύο άγρυπνοι πράκτορες αλληλεπιδράσουν, αν το άθροισμα των μετρητών τους ανήκει στο $\{-1, 0, 1\}$, τότε και οι δύο θέτουν τους

μετρητές τους στην τιμή του αθροίσματος και ο ένας εκ των δύο περνάει στην κατάσταση ύπνου, αλλιώς δεν κάνουν τίποτα. Συνεπώς, οι αλληλεπιδράσεις που δεν κάνουν τίποτα είναι αυτές που συμβαίνουν μεταξύ άγρυπνων πρακτόρων που έχουν και οι δύο μετρητή $1$ ή και οι δύο μετρητή $-1$. Όπως και πριν, απ' τη στιγμή που ένας πράκτορας θα περάσει στην κατάσταση ύπνου απλώς αντιγράφει το μετρητή κάθε άγρυπνου πράκτορα με τον οποίο αλληλεπιδρά. Παρατηρούμε ότι οι αλληλεπιδράσεις άγρυπνων πρακτόρων με μετρητές $1$ και $-1$ εξαλείφουν τις τιμές αυτές, αφού ο ένας πράκτορας παραμένει άγρυπνος κρατώντας την τιμή $0$ ενώ ο άλλος περνάει στην κατάσταση ύπνου. Επίσης, όταν ένα $0$ αλληλεπιδράσει με $1$ ή $-1$, το άθροισμα είναι $1$ ή $-1$, το παίρνουν και οι δύο πράκτορες και ένας εξ' αυτών περνάει στην κατάσταση ύπνου, άρα το $0$ εξαλείφεται απ' το άγρυπνο υποσύνολο του πληθυσμού. Τελικά, θα απομείνει ένα τελικό σύνολο άγρυπνων πρακτόρων που δεν θα μπορούν να μεταβάλλουν τους μετρητές τους αφού το άθροισμα των μετρητών τους θα είναι πάντοτε εκτός του $\{-1, 0, 1\}$ και σε αυτή την κατάσταση ισορροπίας είναι προφανές ότι ή όλοι οι πράκτορες θα έχουν μετρητή $1$ ή όλοι μετρητή $-1$ όλοι μετρητή $0$ (ακόμα και αυτοί που είναι στην κατάσταση ύπνου καθώς θα τον έχουν αντιγράψει από τους άγρυπνους πράκτορες). Έτσι, αν η συνάρτηση εξόδου ορίζεται ως $O(1) = 1$ και $O(-1) = O(0) = 0$, τότε το πρωτόκολλο αυτό υπολογίζει σταθερά τη συνάρτηση πλειοψηφίας.

Η παρατήρηση κλειδί είναι ότι, σε κάθε βήμα, το άθροισμα των μετρητών των άγρυπνων πρακτόρων παραμένει σταθερό και ίσο με με το πλήθος των $1$ μείον το πλήθος των $0$ της εισόδου. Συνεχώς διαγράφονται μετρητές που το άθροισμά τους ισούται με το μηδέν και ή θα παραμείνουν μόνο άγρυπνα $1$ που δεν έχουν με τί να διαγραφούν (τα $1$ ήταν περισσότερα στην είσοδο) ή μόνο άγρυπνα $-1$ που δεν έχουν με τί να διαγραφούν (τα $0$ ήταν περισσότερα στην είσοδο) ή μόνο ένα άγρυπνο $0$ που δεν έχει άλλο άγρυπνο πράκτορα για να αλληλεπιδράσει (τα $0$ και $1$ είχαν ίσους πληθάριθμους στην είσοδο). Σε κάθε περίπτωση, όλοι οι πράκτορες αποκτούν τη σωστή τιμή μετρητή και η συνάρτηση εξόδου δίνει την σωστή απάντηση ικανοποιώντας την παραδοχή εξόδου κατηγορημάτων.

Το παραπάνω πρωτόκολλο εφαρμόζει μία γενικότερη ιδέα υπολογισμού κατηγορημάτων της μορφής $k \cdot N_1 - l \cdot N_0 \geq 0$, όπου $N_1$ είναι το πλήθος των $1$ στην είσοδο, $N_0$ το πλήθος των $0$ στην είσοδο (δηλαδή $N_0 + N_1 = n$ για $X = \{0, 1\}$) και τα $k$, $l$ είναι θετικοί ακέραιοι (σταθεροί και ανεξάρτητοι του $n$). Το κατηγόρημα $p$ που περιγράφεται ως ($k \cdot N_1 - l \cdot N_0 \geq 0$) ορίζεται ως $p(x) = 1$ αν το $x$ ικανοποιεί την ανισότητα και $p(x) = 0$ αλλιώς. Οι καταστάσεις των πρακτόρων αποτελούνται και πάλι από έναν μετρητή και ένα ψηφίο επαγρύπνησης. Ο μετρητής μπορεί να πάρει όλες τις ακέραιες τιμές από $-l$ μέχρι $k$ (συμπεριλαμβανομένων των $-l$ και $k$). Αρχικά όλοι οι πράκτορες είναι άγρυπνοι και όσοι πράκτορες παίρνουν είσοδο $1$ θέτουν το

μετρητή τους στην τιμή $k$ ενώ όσοι πάρουν $0$ θέτουν το μετρητή τους στην τιμή $-l$. Παρατηρούμε ότι στην αρχική διαμόρφωση το άθροισμα των μετρητών όλων των πρακτόρων ισούται με $k \cdot N_1 - l \cdot N_0$. Όταν δύο άγρυπνοι πράκτορες αλληλεπιδράσουν, αν το άθροισμα των μετρητών τους ανήκει στο $\{-l, \ldots, 0, \ldots, k\}$, τότε και οι δύο θέτουν τους μετρητές τους στην τιμή του αθροίσματος και ο ένας εκ των δύο περνάει στην κατάσταση ύπνου, αλλιώς δεν κάνουν τίποτα. Κάθε πράκτορας που βρίσκεται στην κατάσταση ύπνου απλώς αντιγράφει το μετρητή κάθε άγρυπνου πράκτορα με τον οποίο αλληλεπιδρά. Με τον τρόπο αυτό το άθροισμα των μετρητών των άγρυπνων πρακτόρων είναι πάντοτε (σε κάθε βήμα) αμετάβλητο και ίσο με $k \cdot N_1 - l \cdot N_0$. Κάποια στιγμή οποιαδήποτε αλληλεπίδραση άγρυπνων πρακτόρων δεν θα κάνει τίποτα και αυτό θα σημαίνει ότι ή όλοι (μπορεί να είναι ένας ή περισσότεροι) οι άγρυπνοι πράκτορες έχουν θετικούς μετρητές ή όλοι έχουν αρνητικούς μετρητές ή υπάρχει μόνο ένας άγρυπνος πράκτορας του οποίου ο μετρητής είναι $0$. Λόγω του ότι οι πράκτορες στην κατάσταση ύπνου αντιγράφουν τους μετρητές των άγρυπνων πρακτόρων, στην πρώτη περίπτωση όλος ο πληθυσμός θα έχει θετικό μετρητή, ενώ στις άλλες δύο μη θετικό (αρνητικό ή μηδέν) μετρητή. Η έξοδος κάθε πράκτορα είναι $1$ αν ο μετρητής του είναι θετικός ή $0$ και $0$ αλλιώς (αν αντί για $\geq$ θέλουμε να υπολογίσουμε $>$, τότε η έξοδος είναι 1 αν ο μετρητής είναι αυστηρά θετικός). Μετά τη συζήτηση αυτή πρέπει να είναι προφανές ότι το πρωτόκολλο που περιγράψαμε υπολογίζει σταθερά το κατηγόρημα ($k \cdot N_1 - l \cdot N_0 \geq 0$) στον $G_n$ για κάθε $n \geq 2$ (το $n = 1$ δεν έχει ιδαίτερο νόημα αφού με ένα μόνο πράκτορα το $E_n$ είναι το κενό σύνολο και δεν μπορεί να γίνει καμία αλληλεπίδραση).

Παρατηρούμε τώρα ότι:

$$\begin{aligned} k \cdot N_1 - l \cdot N_0 \geq 0 \Leftrightarrow \\ k \cdot N_1 \geq l \cdot N_0 \Leftrightarrow \\ k \cdot N_1 + l \cdot N_1 \geq l(N_0 + N_1) \Leftrightarrow \\ N_1 \geq \frac{l}{k+l} n \end{aligned}$$

Επομένως, το κατηγόρημα $p$ είναι ισοδύναμο με το κατηγόρημα που είναι $1$ αν τουλάχιστον $l/(k+l)$ των εισόδων είναι $1$ και $0$ αλλιώς. Επομένως, με βάση το πρωτόκολλο που παρουσιάσαμε, για οποιοδήποτε ποσοστό των πρακτόρων που μπορεί να γραφτεί ως $l/(k+l)$ για αυστηρά θετικούς ακέραιους $k$ και $l$ (σταθερούς και ανεξάρτητους του $n$) το αντίστοιχο κατηγόρημα, που είναι $1$ αν τουλάχιστον $100l/(k+l)\%$ των εισόδων είναι $1$ και $0$ αλλιώς, είναι σταθερά υπολογίσιμο από το βασικό μοντέλο πρωτοκόλλων πληθυσμών.

Έτσι, είναι εύκολο πλέον να διαπιστώσουμε ότι υπάρχει ένα πρωτόκολλο το οποίο υπολογίζει σταθερά αν τουλάχιστον $5\%$ των ψαριών του ιχθυοτροφεί-

ου έχουν μολυνθεί, αφού $l/(k+l) = 5/100 = 1/20 = 1/(19+1)$ (απλοποιούμε το $5/100$ στο ανάγωγο $1/20$, διαιρώντας αριθμητή και παρονομαστή με τον ΜΚΔ$(5, 100)$, έτσι ώστε να χρησιμοποιήσουμε τους μικρότερους δυνατούς μετρητές), δηλαδή, $k = 19$ και $l = 1$ και, επομένως, είναι το πρωτόκολλο που υπολογίζει σταθερά το κατηγόρημα $(19N_1 - N_0 \geq 0)$, το οποίο δείξαμε ότι υπάρχει.

### Αριθμητικές Συναρτήσεις

Στην Ενότητα 2.4.3 μελετήσαμε την κατανεμημένη αναπαράσταση $\mathcal{O}(1)$ ακεραίων απόλυτης τιμής φραγμένης εκ των άνω από $\mathcal{O}(n)$. Μπορεί να αποδειχθεί ότι, με βάση τα όσα είπαμε εκεί, υπάρχουν πρωτόκολλα πληθυσμών του βασικού μοντέλο που υπολογίζουν το άθροισμα δύο ακεραίων, το γινόμενο ενός ακεραίου και μίας σταθεράς, το ακέραιο πηλίκο της διαίρεσης ενός ακεραίου με μία σταθερά, την ακέραιο υπόλοιπο της δαίρεσης ενός ακεραίου με μία σταθερά, καθώς και μία σταθερή συνάρτηση (π.χ. $f(x) = k$ για κάθε $x \in X^n$, όπου $k$ μία σταθερά). Αν αυτά τα πρωτόκολλα έχουν *σταθερές εισόδους* (δηλαδή οι είσοδοί τους δεν μεταβάλλονται χρονικά) τότε αυτά τα πρωτόκολλα σταθεροποιούνται ως προς την έξοδό τους και ως εκ τούτου μπορούν να συντεθούν ελεύθερα (αργότερα θα δούμε ότι, ακόμα και αν οι είσοδοι είναι μεταβαλλόμενες, αν κάποια στιγμή σταθεροποιούνται, δηλαδή παύουν να μεταβάλλονται, ισχύουν παρόμοια αποτελέσματα).

### Μία Σταθερά Υπολογίσιμη Γλώσσα Έκφρασης

Με βάση τα αποτελέσματα που έχουμε ήδη παρουσιάσει σε ό, τι αφορά στα σταθερά υπολογίσιμα κατηγορήματα απ' το βασικό μοντέλο, θα επιχειρήσουμε να ορίσουμε μία *γλώσσα έκφρασης* τέτοια ώστε κάθε κατηγόρημα που θα μπορεί να εκφραστεί σε αυτή τη γλώσσα να είναι σταθερά υπολογίσιμο από το βασικό μοντέλο πρωτοκόλλων πληθυσμών. Η γλώσσα έκφρασης που θα παρουσιάσουμε προτάθηκε στο [3] και στην ίδια εργασία αφέθηκε ως ανοικτό πρόβλημα το εάν κάθε σταθερά υπολογίσιμο κατηγόρημα από το βασικό μοντέλο μπορεί να εκφραστεί σε αυτή. Αξίζει κανείς να παρατηρήσει ότι μία τέτοια γλώσσα έκφρασης αποτελεί στην ουσία ένα κάτω φράγμα για την κλάση των υπολογίσιμων κατηγορημάτων, αφού η κλάση θα πρέπει να περιέχει τουλάχιστον τα κατηγορήματα που εκφράζονται στη γλώσσα έκφρασης (ίσως μόνο αυτά ή ίσως και κάποια άλλα που δεν μπορούν να εκφραστούν σε αυτή). Στο επόμενο κεφάλαιο θα δούμε ότι σύμφωνα με το βασικό θεώρημα του [6] (που δημοσιεύτηκε δύο χρόνια μετά την εργασία που όρισε το μοντέλο [3]) αυτή η γλώσσα έκφρασης αποτελεί ταυτόχρονα και άνω φράγμα, δηλαδή ότι τελικά ένα κατηγόρημα είναι σταθερά υπολογίσιμο από το βασικό μοντέ-

λο εάν και μόνον εάν μπορεί να εκφραστεί μέσω της γλώσσας που τώρα θα ορίσουμε.

Για κάθε σύμβολο εισόδου $\sigma \in X$, υπάρχει μία μεταβλητή $N_\sigma$ που αναπαριστά το πλήθος των πρακτόρων στους οποίους ανατίθεται το σύμβολο $\sigma$ από την ανάθεση εισόδου. Με άλλα λόγια, αν $x \in X^n$ είναι το πολυσύνολο εισόδου τότε το $N_\sigma$ ισούται με το πλήθος των εμφανίσεων του $\sigma$ στο $x$. Ένας *όρος* είναι μία σταθερά, ή μία μεταβλητή, ή το άθροισμα δύο όρων, ή το γινόμενο μίας σταθεράς και ενός όρου, ή το υπόλοιπο της ακέραιας διαίρεσης (modulo) ενός όρου με μία μη-μηδενική σταθερά. Μία *ατομική έκφραση* σχηματίζεται από δύο όρους και ένα από τα κατηγορήματα: $=$, $\leq$, $<$, $\geq$, $>$. Τώρα είμαστε σε θέση να ορίσουμε αναδρομικά τις *εκφράσεις*. Κάθε ατομική έκφραση είναι μία *έκφραση*. Αν $\phi$ και $\psi$ είναι εκφράσεις, τότε το ίδιο είναι και οι $\neg\phi$ (άρνηση μίας έκφρασης), $(\phi \wedge \psi)$ (η σύζευξη δύο εκφράσεων) και $(\phi \vee \psi)$ (η διάζευξη δύο εκφράσεων). Κάθε έκφραση, δεδομένης μίας ανάθεσης εισόδου, είναι είτε *αληθής* είτε *ψευδής*. Καλούμε την γλώσσα αυτή, *γλώσσα έκφρασης κατηγορημάτων του βασικού μοντέλου*.

Για παράδειγμα το αν τουλάχιστον $100$ ψάρια έχουν μολυνθεί μπορεί να εκφραστεί ως $(N_1 \geq 100)$, η οποία είναι μία έκφραση που αποτελείται από μία ατομική έκφραση η οποία με τη σειρά της αποτελείται από το κατηγόρημα $\geq$ και δύο όρους, τη μεταβλητή $N_1$ και τη σταθερά $100$. Αντίστοιχα, το πρόβλημα ισοτιμίας μπορεί να εκφραστεί ως $((N_1 \bmod 2) = 1)$ που είναι αληθής έκφραση αν το $N_1$ είναι περιττός και το πρόβλημα της πλειοψηφίας μπορεί να εκφραστεί, όπως είδαμε, ως $(N_1 > N_0)$. Το ερώτημα του εάν τουλάχιστον $5\%$ των ψαριών έχουν μολυνθεί μπορεί να εκφραστεί ως $(19N_1 \geq N_0)$ και γενικότερα το ερώτημα του εάν το ποσοστό των $1$ στην είσοδο είναι μεταξύ $100l_1/(k_1 + l_1)\%$ και $100l_2/(k_2 + l_2)\%$ του συνολικού πληθυσμού μπορεί να εκφραστεί ως

$$((k_1 \cdot N_1 \geq l_1 \cdot N_0) \wedge (k_2 \cdot N_1 \leq l_2 \cdot N_0)).$$

Η γλώσσα έκφρασης κατηγορημάτων του βασικού μοντέλου μπορεί επιτυχώς να εκφράσει και κατηγορήματα πάνω σε μη-δυαδικά αλφάβητα εισόδου. Έτσι, αν $X = \{a, b, c\}$, μπορούμε να εκφράσουμε το κατηγόρημα "υπάρχει ίσος αριθμός από $a$, $b$ και $c$ στην είσοδο" μέσω της έκφρασης $((N_a = N_b) \wedge (N_b = N_c))$. Στο επόμενο κεφάλαιο, όπου και θα επανεξετάσουμε εκτενώς το θέμα της υπολογιστικής ισχύς του βασικού μοντέλου, θα προσπαθήσουμε να πείσουμε τον αναγνώστη ότι κάθε κατηγόρημα που μπορεί να εκφραστεί στη γλώσσα έκφρασης κατηγορημάτων του βασικού μοντέλου είναι σταθερά υπολογίσιμο από το βασικό μοντέλο πρωτοκόλλων πληθυσμών.

# Κεφάλαιο 3

# Υπολογιστική Ισχύς του Βασικού Μοντέλου

*"Everything should be made as simple as possible, but not simpler".*

*Albert Einstein*

## 3.1 Εισαγωγή

Στο κεφάλαιο αυτό θα δείξουμε αρχικά ότι κάθε κατηγόρημα που είτε ορίζεται στην γλώσσα έκφρασης κατηγορημάτων του βασικού μοντέλου, είτε σε ένα είδος αριθμητικής που καλείται Presburger αριθμητική, ή είναι ημιγραμμικό είναι σταθερά υπολογίσιμο από το βασικό μοντέλο πρωτοκόλλων πληθυσμών, δηλαδή υπάρχει κάποιο πρωτόκολλο πληθυσμού το οποίο σε κάθε πλήρη γράφο επικοινωνίας με $n$ κόμβους υπολογίζει σταθερά την υποπερίπτωση του κατηγορήματος που αφορά σε όλες τις εισόδους μεγέθους $n$. Τα αποτελέσματα αυτά εμφανίζονται στα [3], [4] και [9]. Εν συνεχεία θα δούμε ότι η κλάση των ημιγραμμικών κατηγορημάτων είναι ακριβώς ό, τι μπορεί να υπολογίσει το βασικό μοντέλο, δηλαδή, όπως είπαμε, όλα τα ημιγραμμικά κατηγορήματα είναι σταθερά υπολογίσιμα, ενώ δεν υπάρχει ούτε ένα μη-ημιγραμμικό κατηγόρημα που να είναι σταθερά υπολογίσιμο από το βασικό μοντέλο. Το αποτέλεσμα του ακριβούς χαρακτηρισμού της κλάσης των σταθερά υπολογίσιμων κατηγορημάτων εμφανίζονται στο [6], αλλά εμείς θα περιοριστούμε σε απλή αναφορά του βασικού αποτελέσματος.

## 3.2 Ένα Κάτω Φράγμα για τα Υπολογίσιμα Κατηγορήματα

### 3.2.1 Κατηγορήματα της Presburger Αριθμητικής

Η Presburger αριθμητική είναι η πρώτης-τάξης θεωρία ακεραίων που περιλαμβάνει την πρόσθεση και το $<$. Είναι μία πλούσια και αποφασίσιμη θεωρία που επιτρέπει τον ορισμό κατηγορημάτων όπως αυτά της ισοτιμίας και της πλειοψηφίας που παρουσιάσαμε προηγουμένως. Θα ξεκινήσουμε ανακεφαλαιώνοντας τις ιδιότητες της Presburger αριθμητικής και των στενά σχετιζόμενων με αυτή ημιγραμμικών συνόλων. Εν συνεχεία θα δείξουμε ότι κάθε κατηγόρημα που ορίζεται στην Presburger αριθμητική είναι σταθερά υπολογίσιμο από το βασικό μοντέλο των πρωτοκόλλων πληθυσμών (και δείχνοντας ότι η γλώσσα έκφρασης κατηγορημάτων του βασικού μοντέλου είναι ισοδύναμη με τα ημιγραμμικά σύνολα θα αποδείξουμε ότι κάθε κατηγόρημα που μπορεί να εκφραστεί στη γλώσσα αυτή είναι σταθερά υπολογίσιμο).

Ο συνήθης ορισμός της Presburger αριθμητικής θεωρεί μία γλώσσα λογικής πρώτης-τάξης που περιλαμβάνει ένα μόνο συναρτησιακό σύμβολο, το "+", τις σταθερές "0" και "1", τα κατηγορήματα "$=$" και "$<$", τους συνήθεις λογικούς τελεστές "$\wedge$", "$\vee$" και "$\neg$", μεταβλητές $x_1, x_2, \ldots$ και τους ποσοδείκτες "$\forall$" (καθολικός) και "$\exists$" (υπαρξιακός). Το υπονοούμενο σύνολο πάνω στο οποίο εκτείνονται οι ποσοδείκτες είναι το σύνολο των ακεραίων $\mathbb{Z}$ (π.χ. ο τύπος $\exists x(x = 5)$ είναι αληθής αφού υπάρχει ακέραιος που να ισούται με $5$, ενώ ο τύπος $\forall x(x = 5)$ είναι ψευδής αφού δεν είναι όλοι οι ακέραιοι ίσοι με $5$). Η πράξη "+" είναι η συνήθης πρόσθεση ακεραίων. Οι σταθερές "0" και "1" έχουν το σύνηθες νόημά τους ως ακέραιοι. Τα "$=$" και "$<$" ερμηνεύονται ως οι συνήθεις σχέσεις επί του συνόλου των ακεραίων της ισότητας και του μικρότερο από, αντίστοιχα.

Ένας τύπος της Presburger αριθμητικής $\phi(x_1, \ldots, x_k)$ με ελεύθερες μεταβλητές (που δεν εξαρτώνται από κάποιον ποσοδείκτη) $x_1, \ldots, x_k$ *ορίζει* ένα κατηγόρημα $F_\phi : \mathbb{Z}^k \to \{0, 1\}$ ως εξής: Για κάθε $k$-διάνυσμα ακέραιων $(u_1, \ldots, u_k) \in \mathbb{Z}^k$, ισχύει $F_\phi(u_1, \ldots, u_k) = 1$ αν ο τύπος $\phi(x_1, \ldots, x_k)$ είναι αληθής όταν οι μεταβλητές $x_1, \ldots, x_k$ δεσμεύονται στις τιμές $u_1, \ldots, u_k$, αντίστοιχα, ενώ $F_\phi(u_1, \ldots, u_k) = 0$ αλλιώς. Ένα υποσύνολο $S$ του $\mathbb{Z}^k$ είναι *καθορίσιμο* εάν υπάρχει λογικός τύπος $\phi(x_1, \ldots, x_k)$ με ελεύθερες μεταβλητές $x_1, \ldots, x_k$ τ.ώ.

$$S = \{(u_1, u_2, \ldots, u_k) | (u_1, u_2, \ldots, u_k) \in \mathbb{Z}^k \text{ και η } \phi(u_1, u_2, \ldots, u_k) \text{ είναι αληθής}\}.$$

Είδαμε ότι κάθε Presburger τύπος $\phi$ ορίζει ένα κατηγόρημα $F_\phi$. Αξίζει

να παρατηρήσουμε ότι το υποσύνολο του $\mathbb{Z}^k$ που αποτελείται από όλα τα $(u_1, u_2, \ldots, u_k)$ για τα οποία $F_\phi(u_1, u_2, \ldots, u_k) = 1$ είναι καθορίσιμο. Το ίδιο ισχύει και για τα καθορίσιμα υποσύνολα του $\mathbb{N}^k$, τα οποία είναι απλώς εκείνα τα καθορίσιμα υποσύνολα του $\mathbb{Z}^k$ που περιλαμβάνονται στον $\mathbb{N}^k$.

Τα κατηγορήματα που μπορούν να οριστούν με τον παραπάνω τρόπο στην Presburger αριθμητική σχετίζονται στενά με τα ημιγραμμικά σύνολα. Ένα σύνολο $L \subseteq \mathbb{N}^k$ είναι *γραμμικό* εάν υπάρχουν διανύσματα $\nu_0, \nu_1, \ldots, \nu_m \in \mathbb{N}^k$ ($k$-διανύσματα φυσικών) τ.ώ.

$$\begin{aligned} L &= \{\nu_0 + \kappa_1\nu_1 + \ldots + \kappa_m\nu_m | \kappa_1, \ldots, \kappa_m \in \mathbb{N}\} \\ &= \nu_0 + \{\nu_1, \ldots, \nu_m\}^*. \end{aligned}$$

Με απλά λόγια, ένα γραμμικό υποσύνολο του $\mathbb{N}^k$ μπορεί να κατασκευαστεί ξεκινώντας από ένα οποιοδήποτε $k$-διάνυσμα $\nu_0 \in \mathbb{N}^k$ και προσθέτοντας σε αυτό $k$-διανύσματα από ένα πεπερασμένο σύνολο αυθαίρετο αριθμό φορών, π.χ. 1 φορά το $\nu_1$ και 0 φορές τα υπόλοιπα, 2 φορές το $\nu_1$ και 0 φορές τα υπόλοιπα,. . ., 1 φορά το $\nu_1$, 1 φορά το $\nu_2$ και 0 φορές τα υπόλοιπα κ.ο.κ.

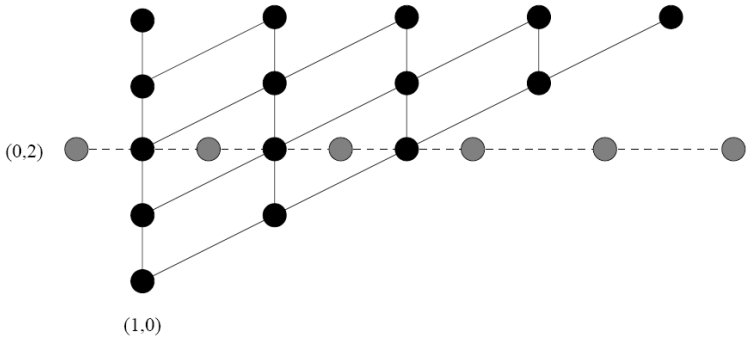
Ένα σύνολο είναι *ημιγραμμικό υποσύνολο* του $\mathbb{N}^k$ αν αποτελεί την ένωση πεπερασμένου αριθμού γραμμικών υποσυνόλων του $\mathbb{N}^k$.

Έστω για παράδειγμα τα σύνολα

$$\begin{aligned} L_1 &= (1,2) + \{(3,5),(7,11)\}^* \\ L_2 &= (1,1) + \{(2,3),(5,7)\}^* \\ L &= L_1 \cup L_2. \end{aligned}$$

Τα $L_1$ και $L_2$ είναι γραμμικά υποσύνολα του $\mathbb{N}^2$ και ως εκ τούτου το $L$ είναι (εξ' ορισμού) ημιγραμμικό υποσύνολο του $\mathbb{N}^2$.

Ας δούμε ένα ακόμα παράδειγμα για να γίνουν πιο κατανοητοί οι ορισμοί. Έστω το γραμμικό υποσύνολο του $\mathbb{N}^2$ που ορίζεται ως $L_3 = \{(1,0) + \alpha_1(1,0) + \alpha_2(0,2)\}$. Το γραμμικό αυτό σύνολο αποτελείται από το *σημείο βάσης* $(1,0)$, το σημείο $(2,0)$ που προκύπτει για $\alpha_1 = 1$ και $\alpha_2 = 0$, γενικότερα τα σημεία $(k+1,0)$ που προκύπτουν από $\alpha_1 = k$ και $\alpha_2 = 0$ για κάθε φυσικό αριθμό $k \geq 0$, και γενικότερα όλα τα σημεία $(k+1, 2l)$ που προκύπτουν από $\alpha_1 = k$ και $\alpha_2 = l$ για όλους τους φυσικούς $k \geq 0$ και $l \geq 0$. Έστω, επίσης το γραμμικό υποσύνολο του $\mathbb{N}^2$ που ορίζεται ως $L_4 = \{(0,2) + \alpha_3(2,0)\}$. Εδώ μπορούμε ακόμα πιο εύκολα να δούμε ότι το $L_4$ αποτελείται απ' τα σημεία $(0,2)$, $(2,2)$,. . . ,$(2k,2)$ για κάθε φυσικό $k \geq 0$. Στο Σχήμα 3.1 φαίνεται με μαύρους κύκλους μέρος των σημείων του γραμμικού συνόλου $L_3$ ενώ με γκρι κύκλους μέρος των σημείων του γραμμικού συνόλου $L_4$. Είναι προφανές ότι το σύνολο $S = L_3 \cup \Sigma_4$ είναι ένα ημιγραμμικό σύνολο που αποτελείται από όλα τα σημεία των $L_3$ και $L_4$ (τα μαύρα και τα γκρι στο Σχήμα 3.1).




Σχήμα 3.1: Ένα ημιγραμμικό σύνολο $S$ (όλοι οι κύκλοι), που είναι ίσο με την ένωση του γραμμικού συνόλου $L_3 = \{(1,0) + \alpha_1(1,0) + \alpha_2(0,2)\}$ (μαύροι κύκλοι) με το γραμμικό σύνολο $L_4 = \{(0,2) + \alpha_3(2,0)\}$ (γκρι κύκλοι).

**Θεώρημα 4 (Ginsburg και Spanier).** *Ένα υποσύνολο του $\mathbb{N}^k$ είναι ημιγραμμικό αν είναι καθορίσιμο στην Presburger αριθμητική.*

*Απόδειξη.* Αποδείχτηκε αρχικά από τους Ginsburg και Spanier [13]. Ο Kracht έδωσε πρόσφατα μία απλούστερη απόδειξη [17]. □

Το θεώρημα αυτό καταδεικνύει την πολύ στενή σχέση της Presburger αριθμητικής με τα ημιγραμμικά υποσύνολα του $\mathbb{N}^k$. Λόγω αυτού του αποτελέσματος μπορούμε αμέσως να αποφανθούμε ότι

**Πόρισμα 4.** *Τα ημιγραμμικά σύνολα είναι κλειστά ως προς το συμπλήρωμα, την πεπερασμένη τομή και την πεπερασμένη ένωση.*

Έστω ένα κατηγόρημα $p : \mathbb{N}^k \to \{0,1\}$. Το *στήριγμα* του $p$ είναι το $p^{-1}(1)$, δηλαδή το σύνολο όλων των $k$-διανυσμάτων του $\mathbb{N}^k$ που το $p$ αντιστοιχίζει στο στην τιμή $1$.

**Ορισμός 12.** *Θα λέμε ότι ένα κατηγόρημα $p : \mathbb{N}^k \to \{0,1\}$ είναι ημιγραμμικό αν το στήριγμά του, $p^{-1}(1)$, είναι ημιγραμμικό υποσύνολο του $\mathbb{N}^k$.*

Αξίζει να παρατηρήσει κανείς ότι λόγω της κλειστότητας των ημιγραμμικών συνόλων ως προς το συμπλήρωμα αυτό είναι ισοδύναμο με το να ζητήσουμε να είναι το $p^{-1}(0)$ ημιγραμμικό υποσύνολο του $\mathbb{N}^k$.

Παρότι η Presburger αριθμητική φαίνεται να περιλαμβάνει μόνο την πράξη της πρόσθεσης, η κατάλληλη χρήση των ποσοδεικτών επιτρέπει και τον ορισμό κατηγορημάτων (μέσω ενός λογικού τύπου που ορίζει το κατηγόρημα) που περιλαμβάνουν πολλαπλασιασμό ή/και διαίρεση. Έστω $m$ μία σταθερά και $\equiv_m$ το κατηγόρημα 2 θέσεων τ.ώ. το $x \equiv_m y$ είναι ισοδύναμο με $x \equiv y$

$(\mathrm{mod}\ m)$, δηλαδή το $x \equiv_m y$ είναι αληθές ανν το $x - y$ είναι ακέραιο πολλαπλάσιο του $m$ (για μη-αρνητικά $x$ και $y$ και θετικό $m$ είναι ισοδύναμο με το οι ακέραιες διαιρέσεις των $x$ και $y$ με το $m$ αφήνουν το ίδιο υπόλοιπο). Το κατηγόρημα αυτό μπορεί να οριστεί από ένα τύπο $\xi_m(x, y)$ ως εξής: Για κάθε μεταβλητή ή σταθερά $q$, έστω $\underline{m}q$ η έκφραση που προσθέτει μεταξύ τους $m$ αντίγραφα του $q$, δηλαδή,

$$\underline{m}q = \underbrace{q + q + q + \ldots + q}_{m \text{ φορές}}$$

Τότε

$$\xi_m(x, y) \stackrel{\text{df}}{=} \exists z \exists q((y + z = x) \wedge \underline{m}q = z).$$

Παρατηρούμε ότι η $\xi_m(x, y)$ ικανοποιείται ανν το $z = x - y$ είναι, για κάποιον ακέραιο $q$, ακέραιο πολλαπλάσιο του $m$ (δηλαδή, $z = x - y$ και $q = (x - y)/m$), δηλαδή, ανν ικανοποιείται η $x \equiv_m y$. Ομοίως, θα μπορούσαμε να έχουμε ορίσει $x + z = y$, και η $\xi_m(x, y)$ να ικανοποιείται ανν $y \equiv_m x$, το οποίο όμως είναι το ίδιο για $m$ φυσικό αριθμό, αφού τότε η $\equiv_m$ είναι σχέση ισοδυναμίας.

Μία *επέκταση* μίας διερμηνευόμενης θεωρίας πρώτης-τάξης προκύπτει ως αποτέλεσμα της προσαύξησης της θεωρίας με νέα κατηγορήματα και νέα σύμβολα για το συμβολισμό των κατηγορηματων αυτών. Μία επέκταση που δεν αλλάζει την κλάση των καθορίσιμων κατηγορημάτων καλείται *συντηρητική*. Θα καλούμε *επεκταθείσα Presburger αριθμητική* την αριθμητική που προκύπτει αν εισαγάγουμε στην Presburger αριθμητική τα σχεσιακά σύμβολα $\equiv_m$ που υποδηλώνουν ισοδυναμία modulo $m$, για κάθε ακέραιο $m \geq 2$.

**Λήμμα 5.** *Η επεκταθείσα Presburger αριθμητική είναι μία συντηρητική επέκταση της Presburger αριθμητικής.*

*Απόδειξη.* Είδαμε ότι ο τύπος $\xi_m(x, y)$ ορίζει το κατηγόρημα $\equiv_m$ για κάθε $m \geq 2$. Άρα, η επεκταθείσα Presburger αριθμητική είναι ίδια με την Presburger αριθμητική ως προς την κλάση των κατηγορημάτων που μπορούν να οριστούν, καθώς η μόνη προσαύξηση που έγινε είναι η ανάθεση του συμβόλου $\equiv_m$ στον τύπο της Presburger αριθμητικής $\exists z \exists q((y + z = x) \wedge \underline{m}q = z)$ για κάθε $m \geq 2$. □

Φαίνεται αναπόφευκτο, ότι για τον ορισμό του τύπου $\xi_m(x, y)$ είναι απαραίτητη η χρήση ποσοδεικτών (εδώ χρησιμοποιήσαμε δύο φορές τον υπαρξιακό ποσοδείκτη). Είναι πολύ ενδιαφέρον το γεγονός ότι μόλις προσαυξήσουμε την Presburger αριθμητική με τα $\equiv_m$, δεν υπάρχει πλέον καμία ανάγκη για την ύπαρξη των ποσοδεικτών (δεν προσφέρουν καμία επιπλέον εκφραστική δύναμη). Η διαίσθηση λέει ότι γίνεται πλήρης χρήση τους μέσω των νέων συμβόλων $\equiv_m$, καθώς αυτά εμπεριέχουν δύο φορές τον υπαρξιακό ποσοδείκτη.

**Θεώρημα 5.** *Κάθε καθορίσιμο κατηγόρημα της Presburger αριθμητικής μπορεί να οριστεί στην επεκταδείσα Presburger αριθμητική από κάποιον τύπο χωρίς ποσοδείκτες.*

*Απόδειξη.* Το 1929 ο Presburger [19] έδειξε την αποκρισιμότητα κλειστών τύπων της Presburger αριθμητικής χωρίς τον τελεστή "$<$". Η αποδεικτική του μέθοδος συνίσταται στην μετατροπή κάθε κλειστού τύπου (δηλαδή, κάθε τύπου που δεν έχει ελεύθερες μεταβλητές) σε μία εύκολα αποκρίσιμη κανονική μορφή στην οποία οι μόνοι ποσοδείκτες εμφανίζονται σε υπο-τύπους που εκφράζουν τη σχέση $\equiv_m$. Η μέθοδος αυτή εύκολα επεκτείνεται και στην παρούσα περίπτωση που εμείς εξετάζουμε. □

## 3.3 Υπολογισμός Presburger Κατηγορημάτων

Στην ενότητα αυτή θα δείξουμε ότι κάθε Presburger-καθορίσιμο κατηγόρημα είναι σταθερά υπολογίσιμο από ένα πρωτόκολλου πληθυσμού που χρησιμοποιεί την παραδοχή κωδικοποίησης ακέραιας εισόδου $\rho^X$ που ορίσαμε στην Ενότητα 2.4.3. Για να το δείξουμε αυτό θα ορίσουμε πρώτα μία ακόμα παραδοχή για την περίπτωση ακέραιας συνάρτησης, την παραδοχή καταμέτρησης συμβόλων εισόδου, εν συνεχεία θα δείξουμε ότι όλα τα Presburger κατηγορήματα είναι σταθερά υπολογίσιμα υπό τη νέα παραδοχή και τέλος θα χρησιμοποιήσουμε τα παραπάνω για να δείξουμε ότι όλα τα Presburger κατηγορήματα είναι σταθερά υπολογίσιμα και υπό την παραδοχή κωδικοποίησης ακέραιας εισόδου.

Η *παραδοχή καταμέτρησης συμβόλων εισόδου* υποθέτει ένα αυθαίρετο αλφάβητο εισόδου $X = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ και μία παραδοχή κωδικοποίησης εισόδου της μορφής $E_I : \mathcal{X} \to \mathbb{N}^k$. Η ιδέα είναι αρκετά απλή: Κάθε ανάθεση εισόδου $x \in \mathcal{X}$ αναπαριστά το $k$-διάνυσμα φυσικών του οποίου η $i$-στή συνιστώσα περιέχει το πλήθος των πρακτόρων στους οποίους η $x$ αναθέτει το σύμβολο $\sigma_i$. Για παράδειγμα αν $|V| = 30$, $X = \{\sigma_1, \sigma_2, \ldots, \sigma_7\}$ και $u = (1, 4, 0, 8, 4, 3, 10) \in \mathbb{N}^7$ τότε το $u$ αναπαρίσταται από κάθε ανάθεση εισόδου $x$ για την οποία ισχύει $|x^{-1}(\sigma_1)| = 1$ (δηλαδή, ο πληθάριθμος του υποσυνόλου των πρακτόρων στους οποίους η $x$ αναθέτει το σύμβολο $\sigma_1$ να είναι 1), $|x^{-1}(\sigma_2)| = 4$, $|x^{-1}(\sigma_3)| = 0$, $|x^{-1}(\sigma_4)| = 8$, $|x^{-1}(\sigma_5)| = 4$, $|x^{-1}(\sigma_6)| = 3$ και $|x^{-1}(\sigma_7)| = 10$. Αξίζει να παρατηρήσει κανείς ότι για κάθε πληθυσμό $V$ το υποσύνολο του $\mathbb{N}^k$ των διανυσμάτων που αναπαρίστανται από τουλάχιστον μία ανάθεση εισόδου ορίζεται ως $\{u | u \in \mathbb{N}^k \text{ και } \sum_{i=1}^{k}(u_i) = |V|\}$, καθώς καμία ανάθεση εισόδου δεν μπορεί να αναπαραστήσει ένα διάνυσμα το οποίο υπονοεί βάσει της παραδοχής καταμέτρησης συμβόλων εισόδου κάποιο πλήθος πρακτόρων διαφορετικό του $|V|$. Με αντίστοιχο τρόπο, δηλαδή, αναπαριστών-

τας με κάθε ανάθεση εξόδου $y$ ένα διάνυσμα $t \in \mathbb{N}^l$ (όπου $Y = \{\tau_1, \ldots, \tau_l\}$), έτσι ώστε $t_i = |y^{-1}(\tau_i)|$, ορίζεται η *παραδοχή καταμέτρησης συμβόλων εξόδου*.

**Λήμμα 6.** *Έστω $X = \{\sigma_1, \ldots, \sigma_k\}$ ένα αυθαίρετο αλφάβητο εισόδου με $k$ σύμβολα. Έστω $a_i$, $c$ και $m$ ακέραιες σταθερές με $m \geq 2$. Τότε τα ακόλουθα κατηγορήματα πάνω στους μη-αρνητικούς ακεραίους $x_1, \ldots, x_k$ (όπου ο $x_i$ εκφράζει του πληθάριθμο του $\sigma_i$ στο πολυσύνολο της εισόδου και για τους οποίους πρέπει λόγω της παραδοχής καταμέτρησης συμβόλων εισόδου να ισχύει $\sum_{i=1}^{k} x_i = |V|$) είναι σταθερά υπολογίσιμα από το βασικό μουτέλο υπό την παραδοχή καταμέτρησης συμβόλων εισόδου:*

1. $\sum_{i=1}^{k} a_i x_i < c$
2. $\sum_{i=1}^{k} a_i x_i \equiv c \pmod{m}$.

*Απόδειξη.* Θα αποδείξουμε το ζητούμενο παρουσιάζοντας πρωτόκολλα που θα αποδείξουμε ότι υπολογίζουν σταθερά τα κατηγορήματα αυτά. Έστω $s = \max(|c| + 1, m, \max_i |a_i|)$, όπου στην περίπτωση του πρώτου κατηγορήματος το $m$ δεν μας χρειάζεται και θεωρούμε ότι είναι $0$. Και στα δύο πρωτόκολλα το σύνολο καταστάσεων είναι το σύνολο $\{0,1\} \times \{0,1\} \times \{u \mid u \in \mathbb{Z} \text{ και } -s \leq u \leq s\}$. Επομένως, κάθε κατάσταση αποτελείται από δύο πεδία δυαδικών ψηφίων και ένα πεδίο ακεραίων τιμών. Το πρώτο ψηφίο είναι ένα ψηφίο επαγρύπνησης. Ένας πράκτορας με ψηφίο επαγρύπνησης $1$ είναι άγρυπνος, ενώ ένας πράκτορας που έχει ψηφίο επαγρύπνησης $0$ κοιμάται (ή είναι στην κατάσταση ύπνου). Ο αναγνώστης αξίζει να ανατρέξει στις Ενότητες 2.5.1 και 2.5.1, καθώς τα πρωτόκολλα που θα παρουσιάσουμε αποτελούν γενίκευση των ιδεών που παρουσιάζονται εκεί. Το δεύτερο ψηφίο καθορίζει την τιμή εξόδου κάθε πράκτορα (κάθε πράκτορας στην κατάσταση ύπνου αντιγράφει σε αυτό το πεδίο την τιμή εξόδου κάθε άγρυπνου πράκτορα με τον οποίο αλληλεπιδρά). Το τρίτο πεδίο είναι ένας ακέραιος μετρητής. Αρχικά, όλοι οι πράκτορες είναι άγρυπνοι, το ψηφίο εξόδου τους είναι $0$ και κάθε πράκτορας που παίρνει ως είσοδο το σύμβολο $\sigma_i$ ξεκινάει με τον μετρητή του στην τιμή $a_i$, που είναι ο συντελεστής του $x_i$ στον γραμμικό συνδυασμό και όπου το $x_i$, σύμφωνα με την παραδοχή καταμέτρησης συμβόλων εισόδου, αντιστοιχεί στον πληθάριθμο του συμβόλου $\sigma_i$ στο πολυσύνολο εισόδου. Η συνάρτηση εισόδου $I$, επομένως, ορίζεται ως $I(\sigma_i) = (1, 0, a_i)$. Αν με $u_j(C)$ συμβολίσουμε την τιμή του μετρητή του πράκτορα $j$ στην διαμόρφωση $C$ και με $C_0$ την αρχική διαμόρφωση, παρατηρούμε ότι αρχικά

$$\sum_{j \in V} u_j(C_0) = \sum_{i=1}^{k} a_i x_i$$

καθώς το σύμβολο $\sigma_i$ ανατίθεται σε $x_i$ πράκτορες και συνεπώς $x_i$ πράκτορες έχουν αρχικά το μετρητή τους στην τιμή $a_i$, για κάθε $i \in \{1, \ldots, k\}$. Η συνάρτηση εξόδου $O$ απλώς αντιστοιχίζει το $(\cdot, b, \cdot)$ στην τιμή $b$ (το αλφάβητο εξόδου είναι, προφανώς, $Y = \{0, 1\}$).

Θα ξεκινήσουμε παρουσιάζοντας την συνάρτηση μετάβασης του πρωτοκόλλου που υπολογίζει σταθερά το κατηγόρημα $\sum_{i=1}^{k} a_i x_i < c$ και το οποίο θα καλούμε *πρωτόκολλο κατωφλίου*. Για κάθε ακεραίους $u$, $u'$ με $-s \leq u, u' \leq s$, ορίζουμε

$$q(u, u') = \max(-s, \min(s, u + u'))$$

και

$$r(u, u') = u + u' - q(u, u')$$

Παρατηρούμε ότι αν το άθροισμα $u + u'$ είναι $-s$, ή $s$, ή μεταξύ των $-s$ και $s$ τότε $q(u, u') = u + u'$, ενώ αν $u + u' < -s$ είναι $q(u, u') = -s$ και αν $u + u' > s$ είναι $q(u, u') = s$. Διαισθητικά το $q(u, u')$ αποθηκεύει όσο περισσότερο γίνεται από το άθροισμα των $u$ και $u'$ χωρίς να φύγει έξω από τα όρια αποθήκευσης $-s$ και $s$. Αν είναι να υπερβεί το κάτω όριο σταματάει στο $-s$ ενώ αν είναι να υπερβεί το πάνω όριο σταματάει στο $s$. Τώρα σε ό, τι αφορά στο $r(u, u')$, επειδή από τη δεύτερη εξίσωση $r(u, u') + q(u, u') = u + u'$, αν το $q(u, u')$ κατάφερε να αποθηκεύσει όλο το άθροισμα, το $r(u, u')$ είναι $0$, ενώ αν το $q(u, u')$ δεν κατάφερε να αποθηκεύσει όλο το άθροισμα τότε το $r(u, u')$ αποθηκεύει το μέρος εκείνο του αθροίσματος των $u$ και $u'$ που το $q(u, u')$ δεν κατάφερε να αποθηκεύσει. Αξίζει να παρατηρήσει κανείς ότι και το $r(u, u')$ είναι πάντοτε μεταξύ $-s$ και $s$ (συμπεριλαμβανομένων), καθώς $|u + u'| \leq 2s$ και συνεπώς στην χειρότερη περίπτωση το $q(u, u')$ θα μεταθέσει για αποθήκευση στο $r(u, u')$ το πολύ $|s|$. Έστω, τέλος

$$b(u, u') = \begin{cases} 1, & \text{αν } q(u, u') < c \\ 0, & \text{αλλιώς.} \end{cases}$$

Οι κανόνες μετάβασης δίδονται από τον τύπο

$$(l, \cdot, u), (l', \cdot, u') \to (1, b(u, u'), q(u, u')), (0, b(u, u'), r(u, u'))$$

εάν τουλάχιστον ένα εκ των $l$ και $l'$ είναι $1$ (δηλαδή τουλάχιστον ένας άγρυπνος πράκτορας στην αλληλεπίδραση). Εάν και οι δύο πράκτορες είναι στην κατάσταση ύπνου, δηλαδή $l = l' = 0$, τότε η αλληλεπίδραση δεν κάνει τίποτα.

*Το πρωτόκολλο συγκλίνει σε έναν μόνο άγρυπνο πράκτορα.* Έστω $\Lambda(C)$ το σύνολο των άγρυπνων πρακτόρων κατά στη διαμόρφωση $C$. $|\Lambda(C_0)| = n$, αφού αρχικά όλοι είναι άγρυπνοι. Κάθε αλληλεπίδραση μεταξύ δύο άγρυπνων πρακτόρων μειώνει το $|\Lambda(C)|$ κατά ένα και καμία αλληλεπίδραση δεν μπορεί

να αυξήσει το $|\Lambda(C)|$. Λόγω της συνθήκης δικαιοσύνης, εάν υπάρχουν δύο άγρυπνοι πράκτορες, τελικά θα συναντηθούν. Επομένως, σε πεπερασμένο αριθμό βημάτων ο υπολογισμός θα φτάσει σε μία διαμόρφωση $C$ κατά την οποία $|\Lambda(C)| = 1$.

*Ο μετρητής του μοναδικού άγρυπνου πράκτορα συγκλίνει στην τιμή* $\max(-s, \min(s, \sum_{i=1}^{k} a_i x_i))$. Με άλλα λόγια, θέλουμε να δείξουμε ότι αν το $\sum_{i=1}^{k} a_i x_i$ τυχαίνει να είναι μεταξύ $-s$ και $s$ (συμπεριλαμβανομένων) τότε ο μοναδικός άγρυπνος πράκτορας θα έχει τον γραμμικό συνδυασμό στο μετρητή του, ενώ αν $\sum_{i=1}^{k} a_i x_i < -s$ θα έχει $-s$ και αν $\sum_{i=1}^{k} a_i x_i > s$ θα έχει $s$ (και αυτή η τιμή δεν πρόκειται να αλλάξει σε μελλοντικές αληλεπιδράσεις, είναι δηλαδή η τελική τιμή μετρητή του μοναδικού άγρυπνου πράκτορα).

Σε κάθε περίπτωση, αξίζει να αναφέρουμε ότι, αν το δείξουμε αυτό, τότε το πρωτόκολλο θα είναι ορθό ως εξής: Στην περίπτωση που ο μετρητής του μοναδικού πράκτορα είναι τελικά ο γραμμικός συνδυασμός, τότε όλοι οι άλλοι πράκτορες έχουν μηδενικούς μετρητές και σε κάθε αλληλεπίδραση του άγρυπνου πράκτορα με έναν πράκτορα που είναι στην κατάσταση ύπνου, ο νέος άγρυπνος πράκτορας (όποιος απ' τους δύο ήταν ο μυητής) παίρνει το γραμμικό συνδυασμό και οι δύο θέτουν το ψηφίο εξόδου τους στην τιμή $1$ αν $\sum_{i=1}^{k} a_i x_i < s$, αλλιώς στην τιμή $0$ και λόγω διακαιοσύνης όλοι θα συναντηθούν τελικά με τον μοναδικό άγρυπνο πράκτορα (αντίστοιχα, ο καθένας θα γίνει κάποια στιγμή ο μοναδικός άγρυπνος πράκτορας, αφού αν ο άγρυπνος είναι ο αποκρινόμενος οι ρόλοι εναλλάσσονται). Αντίστοιχα, αν η τελική τιμή του άγρυπνου πράκτορα είναι $s$, τότε ο γραμμικός συνδυασμός είναι μεγαλύτερος του $s$ και ως εκ τούτου είναι μεγαλύτερος του $c$, αφού $-s \leq c \leq s$ και αφού η σύγκριση που θα γίνεται πάντοτε για το ψηφίο εξόδου θα είναι $s \geq c$ που δίνει $0$ και είναι πάντοτε αληθής, όλοι οι πράκτορες τελικά δίνουν ορθά ως έξοδο το $0$. Η περίπτωση του $-s$ είναι ανάλογη με αυτή του $s$.

Είδαμε ότι στην αρχική διαμόρφωση το άθροισμα όλων των μετρητών ισούται με τον γραμμικό συνδυασμό $\sum_{i=1}^{k} a_i x_i$. Είδαμε, επίσης, ότι σε καμία αλληλεπίδραση δεν χάνεται άθροισμα, αφού πάντοτε το άθροισμα των μετρητών μετά την αλληλεπίδραση ισούται με το άθροισμά τους πριν την αλληλεπίσραση. Άρα, σε κάθε διαμόρφωση $C$ ισχύει ότι το $\sum_{j \in V} u_j(C)$ είναι ίσο με $\sum_{i=1}^{k} a_i x_i$. Με άλλα λόγια, σε κάθε βήμα του υπολογισμού το άθροισμα των μετρητών όλων των πρακτόρων ισούται με το γραμμικό συνδυασμό $\sum_{i=1}^{k} a_i x_i$ που θέλουμε να συγκρίνουμε με το $c$.

Ορίζουμε $p(C) = \sum_{j \notin \Lambda(C)} |u_j(C)|$. Το $p(C)$ εκφράζει το άθροισμα των μετρητών όλων των πρακτόρων που κοιμούνται στην διαμόρφωση $C$. Για ευκολία, όταν το νόημα είναι ξεκάθαρο, θα γράφουμε $p$ αντί για $p(C)$ και $u_j$ αντί για $u_j(C)$. Καλούμε μία διαμόρφωση *σταθερή* εάν υπάρχει ένας μοναδικός άγρυπνος πράκτορας $l$ σε αυτή και επιπλέον ισχύει μία απ' τις

ακόλουθες συνθήκες:

1. $p = 0$.

2. $u_l = s$, και $u_j \geq 0$ για κάθε $j \neq l$.

3. $u_l = -s$, και $u_j \leq 0$ για κάθε $j \neq l$.

Εξετάζοντας τις τρεις περιπτώσεις είναι εύκολο να δει κανείς ότι σε μία σταθερή διαμόρφωση ο μετρητής του άγρυπνου πράκτορα $l$ είναι ίσος με $\max(-s, \min(s, \sum_{i=1}^{k} a_i x_i))$. Στην πρώτη, ο $l$ έχει το γραμμικό συνδυασμό και αφού μπορεί και τον αποθηκεύει προφανώς $-s \leq \sum_{i=1}^{k} a_i x_i \leq s$. Στην δεύτερη έχει $s$ και αφού όλοι οι υπόλοιποι έχουν μη-αρνητικούς μετρητές $\sum_{i=1}^{k} a_i x_i \geq s$. Στην τρίτη έχει $-s$ και αφού όλοι οι υπόλοιποι έχουν μη-θετικούς μετρητές $\sum_{i=1}^{k} a_i x_i \leq -s$.

Θα δείξουμε τώρα ότι το πρωτόκολλο κατωφλίου πάντοτε συγκλίνει σε μία σταθερή διαμόρφωση. Αυτό είναι και το τελευταίο βήμα της απόδειξης, κάθως εύκολα παρατηρεί κανείς ότι αν ο υπολογισμός φτάσει σε μία σταθερή διαμόρφωση τότε όλες οι μετέπειτα διαμορφώσεις θα είναι σταθερές και ο μοναδικός άγρυπνος πράκτορας σε όλες αυτές, εξ' ορισμού των σταθερών διαμορφώσεων, θα έχει στο μετρητή του το $\max(-s, \min(s, \sum_{i=1}^{k} a_i x_i))$. Για να αποδείξουμε ότι ο υπολογισμός πάντοτε φτάνει σε μία σταθερή διαμόρφωση θα δείξουμε ότι σε κάθε μη-σταθερή διαμόρφωση με ένα μοναδικό άγρυπνο πράκτορα, υπάρχει κάποια μετάβαση που μειώνει το $p$ και δεν υπάρχει καμία μετάβαση που να αυξάνει το $p$. Θα συνεχίσουμε να συμβολίζουμε με $l$ την ταυτότητα του μοναδικού άγρυπνου πράκτορα.

Σε κάθε μη σταθερή διαμόρφωση με έναν μόνο άγρυπνο πράκτορα

1. υπάρχει μία αλληλεπίδραση που μειώνει το $p$:

   (α') Έστω ότι $u_l = s$ και υπάρχει κάποιος $j \neq l$ για τον οποίο ισχύει $u_j < 0$ (αν ήταν $u_j \geq 0$ για κάθε $j \neq l$ τότε η διαμόρφωση θα ήταν σταθερή). Στην περίπτωση αυτή, μία συνάντηση μεταξύ των $l$ και $j$ θέτει τον μετρητή του μυητή (που γίνεται ο νέος μοναδικός άγρυπνος πράκτορας) στην τιμή $s + u_j$ και θέτει το μετρητή του αποκρινόμενου στο $0$. Άρα, το $p$ μειώνεται κατά $-u_j > 0$.

   (β') Έστω ότι $u_l = -s$ και υπάρχει κάποιος $j \neq l$ για τον οποίο ισχύει $u_j > 0$. Στην περίπτωση αυτή, μία συνάντηση μεταξύ των $l$ και $j$ θέτει τον μετρητή του μυητή (που γίνεται ο νέος μοναδικός άγρυπνος πράκτορας) στην τιμή $-s + u_j$ και θέτει το μετρητή του αποκρινόμενου στο $0$. Άρα, το $p$ μειώνεται και πάλι κατά $u_j > 0$.

(γ') Έστω ότι $-s < u_l < s$ και υπάρχει κάποιος $j \neq l$ για τον οποίο ισχύει $u_j \neq 0$ (αν για κάθε $j \neq l$ ίσχυε $u_j = 0$, τότε θα ίσχυε $p = 0$ και η διαμόρφωση θα ήταν σταθερή). Σε μία συνάντηση μεταξύ των $l$ και $j$, αν (ι) $u_j > 0$, ο μετρητής του μυητή γίνεται $\min(u_l+u_j, s) = u_l+\min(u_j, s-u_l)$ και ως εκ τούτου το $p$ μειώνεται κατά $\min(u_j, s - u_l) > 0$, ενώ, αν (ιι) $u_j < 0$, η περίπτωση είναι συμμετρική και το $p$ μειώνεται κατά $\min(-u_j, s + u_j) > 0$.

Επομένως σε κάθε μη-σταθερή διαμόρφωση με έναν μόνο άγρυπνο πράκτορα υπάρχει μία αλληλεπίδραση που μειώνει το $p$ και λόγω της συνθήκης δικαιοσύνης τελικά θα συμβεί.

2. δεν υπάρχει καμία αλληλεπίδραση που να αυξάνει το $p$.Οι υπόλοιπες πιθανές μεταβάσεις είναι:

   (α') Αυτές μεταξύ δύο πρακτόρων που είναι στην κατάσταση ύπνου. Αυτού του είδους οι αλληλεπιδράσεις δεν κάνουν τίποτα και συνεπώς δεν αυξάνουν το $p$.

   (β') Αυτές στις οποίες ο άγρυπνος πράκτορας έχει $u_l = s$ και ο πράκτορας που είναι στην κατάσταση ύπνου έχει $u_j \geq 0$. Σε αυτές και πάλι το $p$ δεν αλλάζει καθώς ο νέος άγρυπνος θα θέσει το μετρητή του στην τιμή $s$ και ο αποκρυνόμενος στην $u_j$.

   (γ') Αυτές στις οποίες ο άγρυπνος πράκτορας έχει $u_l = -s$ και ο πράκτορας που είναι στην κατάσταση ύπνου έχει $u_j \leq 0$. Σε αυτές και πάλι το $p$ δεν αλλάζει καθώς ο νέος άγρυπνος θα θέσει το μετρητή του στην τιμή $-s$ και ο αποκρυνόμενος στην $u_j$.

   (δ') Ομοίως και γι' αυτές στις οποίες $-s < u_l < -s$ και $u_j = 0$.

Δείξαμε ότι σε κάθε μη-σταθερή διαμόρφωση με ένα μοναδικό άγρυπνο πράκτορα υπάρχει κάποια μετάβαση που μειώνει το $p$ και δεν υπάρχει καμία μετάβαση που να το αυξάνει. Επίσης, δείξαμε ότι σε πεπερασμένο αριθμό βημάτων ο πληθυσμός θα μείνει με ένα μοναδικό άγρυπνο πράκτορα. Απ' τη στιγμή που θα γίνει αυτό, αν ο υπολογισμός είχε μία υποακολουθία άπειρων διαμορφώσεων στις οποίες το $p$ παραμένει σταθερό, τότε, επειδή το πλήθος των διαφορετικών διαμορφώσεων είναι πεπερασμένο, τουλάχιστον μία απ' αυτές, έστω η $C$, θα έπρεπε να εμφανίζεται άπειρο αριθμό φορών στην υποακολουθία. Όμως, υπάρχει μία διαμόρφωση $C'$ που προκύπτει από την $C$ μέσω κάποιας μετάβασης που μειώνει το $p$ η οποία δεν εμφανίζεται καμία φορά στην άπειρη υποακολουθία, αφού το $p$ παραμένει σταθερό, και σε αυτή την περίπτωση ο δρομολογητής δεν είναι δίκαιος. Άρα, λόγω της συνθήκης

δικαιοσύνης, απ' τη στιγμή που ο πληθυσμός θα μείνει με ένα μοναδικό άγρυπνο πράκτορα, το $p$ θα μειώνεται ανά πεπερασμένο πλήθος βημάτων και θα μειωθεί το πολύ $\sum_{i=1}^{k} |a_i| x_i$ φορές μέχρι να γίνει $0$. Άρα, σε πεπερασμένο πλήθος βημάτων το $p$ τελικά θα γίνει ίσο με $0$ εκτός και αν προηγουμένως ικανοποιηθεί μία εκ των συνθηκών σταθερών διαμορφώσεων $2$ και $3$. Και στις τρεις περιπτώσεις ο υπολογισμός θα φτάσει και θα εγκλωβιστεί τελικά σε μία άπειρη ακολουθία σταθερών διαμορφώσεων. Ως εκ τούτου, το πρωτόκολλο κατωφλίου υπολογίζει σταθερά το κατηγόρημα $\sum_{i=1}^{k} a_i x_i < c$.

Ας επιστρέψουμε τώρα στο $\sum_{i=1}^{k} a_i x_i \equiv c \pmod{m}$ και ας ονομάσουμε το αντίστοιχο πρωτόκολλο, πρωτόκολλο υπολοίπου. Εδώ οι κανόνες μετάβασης δίδονται από τον τύπο

$$(l, \cdot, u), (l', \cdot, u') \to (1, b'(u, u'), (u + u') \bmod m), (0, b'(u, u'), 0),$$

εάν τουλάχιστον ένα εκ των $l$, $l'$ είναι ίσο με $1$. Εάν και οι δύο πράκτορες είναι στην κατάσταση ύπνου, δηλαδή $l = l' = 0$, τότε η αλληλεπίδραση δεν κάνει τίποτα. Η συνάρτηση $b'$ ορίζεται ως:

$$b'(u, u') = \begin{cases} 1, & \text{αν } u + u' \equiv c \pmod{m} \\ 0, & \text{αλλιώς.} \end{cases}$$

Λόγω της ομοιότητας με το πρωτόκολλο κατωφλίου, είναι προφανές ότι και το πρωτόκολλο υπολοίπου πάντοτε διαθέτει τελικά ένα μόνο άγρυπνο πράκτορα. Αρχικά ισχύει προφανώς $(\sum_{i=1}^{k} a_i x_i) \bmod m = (\sum_{j \in V} u_j(C_0)) \bmod m$. Θα δείξουμε τώρα ότι για κάθε $C$, ισχύει $(\sum_{i=1}^{k} a_i x_i) \bmod m = (\sum_{j \in V} u_j(C)) \bmod m$, δηλαδή ότι το υπόλοιπο της διαίρεσης του αρχικού γραμμικού συνδυασμού με το $m$ διατηρείται κατά τον υπολογισμό και είναι πάντοτε ίσο με το υπόλοιπο της διαίρεσης του αθροίσματος των μετρητών (σε μία διαμόρφωση $C$) με το $m$.

Το πρωτόκολλο παίρνει συνεχώς δύο αθροιστέους $t_1$ και $t_2$ του συνολικού αθροίσματος και τους αντικαθιστά με το $(t_1 + t_2) \bmod m$ (το καταγράφει ο μυητής και ο αποκρινόμενος γίνεται $0$). Επομένως, αρκεί να δ.ό.[1] για κάθε άθροισμα ακεραίων $t_1 + t_2 + \ldots + t_r$ ισχύει

$$(t_1 + t_2 + \ldots + t_r) \bmod m = [(t_1 + t_2 + \ldots + t_r - t_i - t_j) + (t_i + t_j) \bmod m] \bmod m.$$

[1] δείξουμε ότι

Πράγματι

$$\begin{aligned}(t_1{+}t_2 + \ldots + t_r) \bmod m &= [(t_1 + t_2 + \ldots + t_r - t_i - t_j) + (t_i + t_j) \bmod m] \\ &\quad \bmod m \\ &= [(t_1 + t_2 + \ldots + t_r - t_i - t_j) + (t_i + t_j) - \left\lfloor \frac{t_i + t_j}{m} \right\rfloor m] \bmod m \\ &= (t_1 + t_2 + \ldots + t_r) - \left\lfloor \frac{t_i + t_j}{m} \right\rfloor m - \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r) - \left\lfloor \frac{t_i+t_j}{m} \right\rfloor m}{m} \right\rfloor m \\ &= (t_1 + t_2 + \ldots + t_r) - z \cdot m\end{aligned}$$

Μένει να δ.ό.

$$z = \left\lfloor \frac{t_i + t_j}{m} \right\rfloor + \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r)}{m} - \left\lfloor \frac{t_i + t_j}{m} \right\rfloor \right\rfloor = \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r)}{m} \right\rfloor,$$

καθώς τότε θα ισχύει

$$(t_1 + t_2 + \ldots + t_r) \bmod m = (t_1 + t_2 + \ldots + t_r) - \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r)}{m} \right\rfloor \cdot m$$

το οποίο εξ' ορισμού του mod είναι αληθές. Πράγματι, επειδή το $\left\lfloor \frac{t_i+t_j}{m} \right\rfloor$ είναι ακέραιος, ισχύει

$$\begin{aligned}z &= \left\lfloor \frac{t_i + t_j}{m} \right\rfloor + \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r)}{m} - \left\lfloor \frac{t_i + t_j}{m} \right\rfloor \right\rfloor \\ &= \left\lfloor \frac{t_i + t_j}{m} \right\rfloor + \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r)}{m} \right\rfloor - \left\lfloor \frac{t_i + t_j}{m} \right\rfloor \\ &= \left\lfloor \frac{(t_1 + t_2 + \ldots + t_r)}{m} \right\rfloor,\end{aligned}$$

*ὅπερ ἔδει δεῖξαι.*

Επομένως, δείξαμε ότι όταν μείνει ένας μόνο άγρυπνος πράκτορας, αφού όλοι οι υπόλοιποι θα έχουν μετρητή ίσο με το $0$, ο πράκτορας αυτός θα πρέπει να έχει μετρητή ίσο με $(\sum_{i=1}^{k} a_i x_i) \bmod m$. Αυτό μπορούμε να το δούμε εύκολα αν σκεφτούμε ότι αναπόφευκτα κάποια στιγμή θα έχουν μείνει μόνο δύο άγρυπνοι πράκτορες οι οποίοι μόλις αλληλεπιδράσουν αφήνουν τον πληθυσμό με έναν άγρυπνο πράκτορα. Έστω $u$ και $u'$ οι μετρητές τους. Είδαμε ότι $(\sum_{i=1}^{k} a_i x_i) \bmod m = (u + u') \bmod m$ (αφού όλοι οι άλλοι πράκτορες είναι στην κατάσταση ύπνου και έχουν μετρητή ίσο με το $0$) και μόλις

αλληλεπιδράσουν ο μυητής θέτει το μετρητή του στην τιμή $(u + u') \bmod m$ και πλέον είναι ο μοναδικός άγρυπνος πράκτορας του πληθυσμού. Τέλος, $b'(u, u') = 1$ αν $(\sum_{i=1}^{k} a_i x_i) \bmod m \equiv c \pmod m$ και 0 αλλιώς. Μένει να δείξουμε ότι $(\sum_{i=1}^{k} a_i x_i) \bmod m \equiv c \pmod m$ ανν $\sum_{i=1}^{k} a_i x_i \equiv c \pmod m$. Έστω $t = \sum_{i=1}^{k} a_i x_i$. Τότε

$$\begin{aligned} t \pmod m &\equiv c \pmod m \Leftrightarrow \\ t \pmod m - c &= k \cdot m, \text{ για κάποιον ακέραιο } k, \Leftrightarrow \\ t - \left\lfloor \frac{t}{m} \right\rfloor m - c &= k \cdot m \Leftrightarrow \\ t - c &= (k + \left\lfloor \frac{t}{m} \right\rfloor) m \Leftrightarrow \\ t &\equiv c \pmod m \end{aligned}$$

Άρα, απ' τη στιγμή που ο πληθυσμός θα μείνει με ένα μόνο άγρυπνο πράκτορα, όλοι οι πράκτορες τελικά (λόγω της συνθήκης δικαιοσύνης) θα αποκτήσουν την ορθή τιμή εξόδου. □

**Θεώρημα 6.** *Κάθε Presburger-καθορίσιμο κατηγόρημα πάνω στους μη-αρνητικούς ακεραίους είναι σταθερά υπολογίσιμο από το βασικό μοντέλο πρωτοκόλλων πληθυσμών υπό την παραδοχή καταμέτρησης συμβόλων εισόδου.*

*Απόδειξη.* Δοθέντος ενός Presburger τύπου $\Phi$, εφαρμόζουμε το Θεώρημα 5 για να την μετατρέψουμε σε ένα τύπο χωρίς ποσοδείκτες $\Phi'$ πάνω στην επεκταθείσα Presburger αριθμητική (που περιλαμβάνει τα σύμβολα $\equiv_m$). Ο $\Phi'$ θα είναι ένας Boolean τύπος πάνω στα κατηγορήματα που μπορούν να γραφούν σε μία απ' τις ακόλουθες τρεις μορφές:

$$\sum a_i x_i + c_1 < \sum b_i x_i + c_2 \tag{3.1}$$

$$\sum a_i x_i + c_1 = \sum b_i x_i + c_2 \tag{3.2}$$

$$\sum a_i x_i + c_1 \equiv_m b_i x_i + c_2 \tag{3.3}$$

Εάν μπορέσουμε να δείξουμε ότι κάθε τέτοιο κατηγόρημα είναι σταθερά υπολογίσιμο, τότε η $\Phi'$ θα είναι σταθερά υπολογίσιμη, αφού κάθε Boolean τύπος σταθερά υπολογίσιμων κατηγορημάτων με ένα κοινό αλφάβητο εισόδου $X$ είναι σταθερά υπολογίσιμος.

Αλλάζοντας τη σειρά των όρων, τα κατηγορήματα της μορφής (3.1) μπορούν να γραφτούν ως

$$\sum d_i x_i < c$$

όπου $d_i = a_i - b_i$ για κάθε $i$ και $c = c_2 - c_1$. Τα κατηγορήματα αυτού του τύπου, όπως είδαμε, υπολογίζονται σταθερά από το πρωτόκολλο κατωφλίου του Λήμματος 6.

Τα κατηγορήματα της μορφής (3.2) μπορούν να αντικατασταθούν από τη σύζευξη ενός ζεύγους κατηγορημάτων:

$$\sum a_i x_i + c_1 < \sum b_i x_i + c_2 + 1$$

$$\sum a_i x_i + c_1 > \sum b_i x_i + c_2 - 1$$

Τα κατηγορήματα αυτά υπολογίζονται σταθερά από το πρωτόκολλο κατωφλίου και, όπως έχουμε ήδη δει, η σύζευξη σταθερά υπολογίσιμων κατηγορημάτων είναι σταθερά υπολογίσιμη.

Τα κατηγορήματα της μορφής (3.3) μπορούν, ομοίως, να γραφτούν ως

$$\sum d_i x_i \equiv_m c.$$

Τέτοια κατηγορήματα, όπως είδαμε, υπολογίζονται σταθερά από το πρωτόκολλο υπολοίπου του Λήμματος 6. □

**Πόρισμα 5.** *Κάθε Presburger-καθορίσιμο κατηγόρημα πάνω στο $\mathbb{Z}^k$ είναι σταθερά υπολογίσιμο στον από το βασικό μοντέλο πρωτοκόλλων πληθυσμών με την παραδοχή κωδικοποίησης ακέραιας εισόδου.*

*Απόδειξη.* Ο αναγνώστης καλείται να ανατρέξει στο [4] για την απόδειξη. □

**Πόρισμα 6.** *Εάν η εικόνα μίας συμμετρικής γλώσσας $L \subseteq X^*$ σύμφωνα με την αντιστοιχία Parikh είναι ένα ημιγραμμικό σύνολο τότε η $L$ είναι αποδεκτή από το βασικό μοντέλο πρωτοκόλλων πληθυσμών (υπάρχει κάποιο βασικό πρωτόκολλο που την αποδέχεται).*

*Απόδειξη.* Αφού το σύνολο $\Psi(L)$ είναι ημιγραμμικό, σύμφωνα με το Θεώρημα 4 είναι καθορίσιμο στην Presburger αριθμητική. Σύμφωνα με το Θεώρημα 6, υπάρχει κάποιο πρωτόκολλο $\mathcal{A}$ που υπολογίζει σταθερά το Presburger κατηγόρημα που ορίζει το ημιγραμμικό σύνολο $\Psi(L)$ υπό την παραδοχή καταμέτρησης συμβόλων εισόδου. Σύμφωνα με το Λήμμα 3, το $\mathcal{A}$ αποδέχεται την $L$. □

**Πόρισμα 7.** *Η κλάση των σταθερά υπολογίσιμων κατηγορημάτων του βασικού μοντέλου πρωτοκόλλων πληθυσμών είναι υπερσύνολο της κλάσης των ημιγραμμικών κατηγορημάτων.*

*Απόδειξη.* Κάθε ημιγραμμικό κατηγόρημα είναι σταθερά υπολογίσιμο από το βασικό μοντέλο. □

## 3.4 Τα Υπολογίσιμα Κατηγορήματα είναι Ημιγραμμικά

Στην ενότητα αυτή θα δώσουμε έναν πλήρη χαρακτηρισμό της κλάσης των σταθερά υπολογίσιμων κατηγορημάτων (πάντα για το βασικό μοντέλο). Συγκεκριμένα, θα αναφέρουμε χωρίς να αποδείξουμε (λόγω της έκτασης της συγκεκριμένης απόδειξης) ότι η κλάση των ημιγραμμικών κατηγορημάτων εκτός από κάτω είναι άνω φράγμα της και ως εκ τούτου το τελικό συμπέρασμα θα είναι ότι ένα κατηγόρημα είναι σταθερά υπολογίσιμο εάν και μόνον εάν είναι ημιγραμμικό. Να σημειώσουμε ότι η εργασία των Angluin, Aspnes, και Eisenstat [6] στην οποία αποδείχτηκε το άνω φράγμα, έκλεισε στην ουσία το πιο σημαντικό ανοικτό πρόβλημα που έχει παρουσιαστεί μέχρι σήμερα στο πεδίο των Πρωτοκόλλων Πληθυσμών.

### 3.4.1 Βασικό Αποτέλεσμα

**Θεώρημα 7.** *Κάθε σταθερά υπολογίσιμο κατηγόρημα είναι ημιγραμμικό.*

*Απόδειξη.* Η απόδειξη είναι ουσιαστικά όλο το [6] και ως εκ τούτου ο αναγνώστης παραπέμπεται σε αυτό. □

**Πόρισμα 8.** *Τα κατηγορήματα που είναι σταθερά υπολογίσιμα απ' τα πρωτόκολλα πληθυσμών είναι ακριβώς τα ημιγραμμικά κατηγορήματα.*

*Απόδειξη.* Γνωρίζουμε απ' το Πόρισμα 7 ότι κάθε ημιγραμμικό κατηγόρημα είναι σταθερά υπολογίσιμο από το βασικό μοντέλο ενώ απ' το Θεώρημα 7 ότι κάθε σταθερά υπολογίσιμο κατηγόρημα είναι ημιγραμμικό. Άρα, ένα κατηγόρημα είναι σταθερά υπολογίσιμο ανν είναι ημιγραμμικό. □

# Κεφάλαιο 4

# Το Μοντέλο των Πρωτοκόλλων Πληθυσμών με Διαμεσολαβητή

*"Ἓν οἶδα ὅτι οὐδὲν οἶδα".*

*Σωκράτης*

## 4.1 Εισαγωγή-Ο Διαμεσολαβητής

Στο κεφάλαιο αυτό παρουσιάζονται τα βασικά αποτελέσματα της έρευνας που διεξήχθη στα πλαίσια της παρούσας Διπλωματικής Εργασίας. Στη σχετική βιβλιογραφία, μετά την εργασία που πρότεινε το μοντέλο των πρωτοκόλλων πληθυσμών [3] παρουσιάστηκαν κάποιες εργασίες που προσπάθησαν να χαλαρώσουν τους πολύ ισχυρούς περιορισμούς που αυτό έθετε, ούτως ώστε να προκύψουν πιο ισχυρά υπολογιστικά μοντέλα. Για παράδειγμα, στο [14] επετράπει στους πράκτορες να έχουν μοναδικούς προσδιοριστές ενώ στο [10] εξετάζεται ένα πιο ετερογεννές σύστημα στο οποίο ορισμένοι πράκτορες έχουν μεγαλύτερη υπολογιστική ισχύ. Γενικά, η τάση είναι αυτή η από κάτω προς τα πάνω προσέγγιση, όπου έχοντας το βασικό αποτέλεσμα σχετικά με την υπολογιστική ισχύ του βασικού μοντέλου των πρωτοκόλλων (βλέπε Πόρισμα **;;**) πληθυσμών προσπαθούμε να ορίσουμε πιο ισχυρά μοντέλα χωρίς να χρησιμοποιούμε για το σκοπό αυτό πολύ ισχυρές υποθέσεις (πράγμα που θα έκανε τα νέα μοντέλα να μην έχουν πρακτική αξία).

Στην παρούσα εργασία προτείνουμε τα *Πρωτόκολλα Πληθυσμών με Διαμεσολαβητή*. Η βασική ιδέα είναι ότι επιτρέπουμε την ύπαρξη ενός *διαμεσολαβητή* ο οποίος είναι υπεύθυνος για τον έλεγχο των επικοινωνιών. Συγκεκριμένα, για να επικοινωνήσουν δύο πράκτορες πρέπει να πάρουν την άδεια του διαμεσολαβητή. Υποθέτουμε ότι κάθε πράκτορας έχει ένα μοναδικό (ερ-

γοστασιακό) αναγνωριστή τον οποίο δεν μπορεί να χρησιμοποιεί το πρωτόκολλο, καθώς η μνήμη κάθε πράκτορα έχει και πάλι μέγεθος $\mathcal{O}(1)$, δηλαδή, τα πρωτόκολλα είναι και πάλι ομοιόμορφα και ανώνυμα. Οι αναγνωριστές δύο πρακτόρων που πρόκειται να αλληλεπιδράσουν, απλώς αποστέλλονται στον διαμεσολαβητή ούτως ώστε αυτός να ελέγξει εάν θα πρέπει να επιτρέψει στους συγκεκριμένους πράκτορες να αλληλεπιδράσουν.

Ο διαμεσολαβητής, όπως τον περιγράψαμε μέχρι τώρα, δείχνει απλώς να επιλύει κάποια ανοικτά θέματα σχετικά με την ασφάλεια των επικοινωνιών στα πρωτόκολλα πληθυσμών. Και παρότι το θέμα της ασφάλειας των συστημάτων αυτών δεν έχει εξεταστεί σχεδόν καθόλου στη σχετική βιβλιογραφία, εμείς θα επικεντρωθούμε σε μία άλλη πολύ σημαντική συνεισφορά του, που έχει να κάνει με την αύξηση της υπολογιστικής ισχύος των πρωτοκόλλων πληθυσμών ως αποτέλεσμα μίας πολύ φτηνής (και φυσικής) επιπλέον υπόθεσης.

Υποθέτουμε ότι ο διαμεσολαβητής αποθηκεύει ζεύγη ταυτοτήτων πρακτόρων σε κλάσεις επικοινωνίας. Κάθε κλάση αντιστοιχεί σε μία κατάσταση και κάθε διατεταγμένο ζεύγος πρακτόρων μπορεί να ανήκει το πολύ σε μία κλάση κάθε στιγμή. Υπάρχει μία ένα-προς-ένα αντιστοιχία μεταξύ των ζευγών της βάσης δεδομένων του διαμεσολαβητή και των επιτρεπόμενων αλληλεπιδράσεων του γράφου επικοινωνίας. Συγκεκριμένα, το ζεύγος $(u, v)$ υπάρχει σε μία κλάση της βάσης δεδομένων του διαμεσολαβητή ανν επιτρέπεται η επικοινωνία μεταξύ των πρακτόρων $u$ και $v$ στην οποία ο $u$ είναι ο μυητής και $v$ ο αποκρινόμενος. Όταν το ζεύγος $(u, v)$ είναι έτοιμο να αλληλεπιδράσει, οι πράκτορες αποστέλλουν τους προσδιοριστές τους στον διαμεσολαβητή ο οποίος αναζητά το ζεύγος $(u, v)$ στη βάση δεδομένων του. Αν το εντοπίσει σε κάποια κλάση, τότε η κατάσταση που αντιστοιχεί στην κλάση αυτή αποστέλλεται στους $u$ και $v$ και τους επιτρέπεται να αλληλεπιδράσουν, διαφορετικά ο διαμεσολαβητής ενημερώνει τους πράκτορες ότι θα πρέπει να ματαιώσουν την αλληλεπίδραση.

Παρατηρούμε επομένως ότι ο διαμεσολαβητής αποθηκεύει πλήρως τον γράφο επικοινωνίας, αφού κρατάει μία διαμέριση του συνόλου των ακμών σε κλάσεις επικοινωνίας. Δύο ακμές ανήκουν σε κάποιο βήμα στην ίδια κλάση ανν στο βήμα αυτό είναι και οι δύο στην κατάσταση της κλάσης. Άρα, είναι σα να επιτρέπουμε στις ακμές του γράφου επικοινωνίας να έχουν μνήμη και να κρατάνε καταστάσεις. Φυσικά, θα πρέπει να είμαστε πολύ προσεκτικοί. Το πλήθος των κλάσεων επικοινωνίας θα πρέπει να είναι σταθερό και ανεξάρτητο του μεγέθους του πληθυσμού ούτως ώστε οι περιγραφές των πρωτοκόλλων του νέου μοντέλου να είναι και πάλι σταθερές. Κατ' αναλογία, αν θεωρήσουμε ακμές με μνήμη αντί για τον διαμεσολαβητή που τις αποθηκεύει, κάθε ακμή του γράφου θα πρέπει να έχει μία μνήμη συνολικής χωρητικότητας $\mathcal{O}(1)$. Με άλλα λόγια υπάρχουν δύο ισοδύναμοι τρόποι να δούμε το νέο μοντέλο:

1. Ένας κλασικός γράφος επικοινωνίας που επικοινωνεί συνεχώς με έναν διαμεσολαβητή.

2. Ένας νέου τύπου γράφος επικοινωνίας, όπου τα κανάλια επικοινωνίας έχουν σταθερή μνήμη, ακριβώς όπως και οι πράκτορες.

Για την τυπική περιγραφή του νέου μοντέλου θα ακολουθήσουμε την δεύτερη ερμηνεία του, καθώς μας επιτρέπει να μην χρειαστεί να λάβουμε υπ' όψιν μας λεπτομέρειες υλοποίησης του διαμεσολαβητή. Ο λόγος δεν είναι ότι η αρχιτεκτονική του διαμεσολαβητή είναι λιγότερο σημαντική, αλλά ότι στην εργασία αυτή βασικός μας στόχος είναι να μελετήσουμε ορισμένες πτυχές της υπολογιστικής ισχύος του νέου μοντέλου, ελπίζοντας ότι το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή είναι ισχυρότερο απ' το μοντέλο των πρωτοκόλλων πληθυσμών.

Έτσι, μοντελοποιούμε τον διαμεσολαβητή μέσω καναλιών επικοινωνίας που ικανοποιούν τις ακόλουθες ιδιότητες:

1. Κάθε ακμή $e \in E$ είναι εφοδιασμένη με έναν *buffer* $\mathcal{O}(1)$ συνολικής αποθηκευτικής χωρητικότητας.

2. Πριν από κάθε αλληλεπίδραση $e = (u, v)$, το ζεύγος που πρόκειται να αλληλεπιδράσει διαβάζει τα περιεχόμενα του αντίστοιχου buffer, δηλαδή την κατάσταση της $e$, για να την δώσει ως όρισμα στην συνάρτηση μετάβασης.

3. Μετά από κάθε αλληλεπίδραση $e = (u, v)$, το ζεύγος που έχει μόλις αλληλεπιδράσει ανανεώνει τα περιεχόμενα του αντίστοιχου buffer, γράφοντας σε αυτόν τη νέα κατάσταση της $e$ που επεστράφη από τη συνάρτηση μετάβασης.

Έστω, για παράδειγμα, οποιοσδήποτε κατευθυνόμενος γράφος $G = (V, E)$, όπου $|V| = n$, και ένας διαμεσολαβητής που αποτελείται από δύο κλάσεις. Η μία, $Cl_0$, αντιστοιχεί στην κατάσταση $0$ και η άλλη, $Cl_1$, στην κατάσταση $1$. Έστω ότι αρχικά $E = Cl_0$, δηλαδή, κάθε ακμή είναι στην κατάσταση $0$. Ισχύει πάντα ότι $Cl_0 \cup Cl_1 = E$, δηλαδή, ο διαμεσολαβητής περιέχει πάντοτε την πλήρη αναπαράσταση του γράφου επικοινωνίας. Επομένως, επειδή επιπλέον $Cl_0 \cap Cl_1 = \emptyset$ (αποθηκεύεται ένα μόνο αντίγραφο κάθε ακμής), εδώ ισχύει αρχικά $Cl_1 = E - Cl_0 = \emptyset$, αφού καμία ακμή δεν είναι αρχικά στην κατάσταση $1$. Γενικά, αν ο διαμεσολαβητής αποτελείται από $l$ κλάσεις επικοινωνίας $Cl_1, Cl_2, \ldots, Cl_l$, τότε ισχύει πάντοτε:

$$E = \bigcup_{i=1}^{l} Cl_i$$

και για κάθε $1 \leq i < j \leq l$ ισχύει ότι $Cl_i \cap Cl_j = \emptyset$. Αυτό σημαίνει ότι ο διαμεσολαβητής αποθηκεύει πάντοτε μία διαμέριση του $E$ σε κλάσεις επικοινωνίας. Όταν το ζεύγος $e = (u, v)$ πρόκειται να αλληλεπιδράσει, αν $e \in Cl_0 \cup Cl_1$, έστω π.χ. ότι ανήκει στην $Cl_0$, τότε η κατάσταση $0$ αποστέλλεται από τον διαμεσολαβητή στους $u$ και $v$, αυτοί αλληλεπιδρούν και στέλνουν στο διαμεσολαβητή τη νέα κατάσταση της $e$, έστω $1$. Ο διαμεσολαβητής τότε απλώς μεταφέρει την $e$ στην κλάση $Cl_1$ (διαγράφοντάς την από την $Cl_0$). Αν $e \notin Cl_0 \cup Cl_1$, τότε ο διαμεσολαβητής στέλνει κάποιο ειδικό σύμβολο (ή σήμα) στους $u$ και $v$ που τους ενημερώνει ότι η αλληλεπίδραση θα πρέπει να ματαιωθεί.

Αντίστοιχα, στη μοντελοποίηση χωρίς διαμεσολαβητή, ο γράφος επικοινωνίας περιέχει μόνο τις επιτρεπόμενες αλληλεπιδράσεις και έτσι απλώς δεν λαμβάνουμε υπ' όψιν οποιεσδήποτε άλλες ενδεχόμενες μη-επιτρεπτές αλληλεπιδράσεις (θεωρούμε ότι τέτοιες δεν μπορούν να υπάρξουν, σα να υπάρχει κάποιος διαμεσολαβητής που τις ματαιώνει). Κάθε ακμή (που αναπαριστά μία επιτρεπόμενη αλληλεπίδραση) έχει έναν buffer που αρχικά περιέχει μία εκ των καταστάσεων $0$ και $1$. Στο συγκεκριμένο παράδειγμα υποθέτουμε ότι αρχικά όλοι οι buffers περιέχουν το σύμβολο $0$, δηλαδή, ισοδύναμα, όλες οι ακμές του $E$ είναι στην κατάσταση $0$, ισοδύναμα, όλες θα ανήκαν στην κλάση $Cl_0$ του διαμεσολαβητή, εάν αυτός υπήρχε. Όταν το ζεύγος $e = (u, v)$ πρόκειται να αλληλεπιδράσει, τότε η συνάρτηση μετάβασης λαμβάνει υπ' όψιν τόσο τις καταστάσεις των πρακτόρων $u$ και $v$, όσο και την κατάσταση της ακμής $e$. Το αποτέλεσμα της αλληλεπίδρασης είναι η ανανέωση των καταστάσεων των πρακτόρων και της κατάστασης της ακμής, σύμφωνα με τις τιμές που επέστρεψε η συνάρτηση μετάβασης. Είναι προφανές ότι τα δύο μοντέλα είναι ισοδύναμα.

Αξίζει, τέλος, να παρατηρήσουμε ότι εάν για κάποιο πρόβλημα πρέπει να θεωρήσουμε ένα μη-κατευθυνόμενο γράφο $G$, τότε απλώς απαιτούμε η σχέση $E$ (κάθε σύνολο ακμών είναι μία μη-ανακλαστική δυαδική σχέση επί του $V$) να είναι συμμετρική (δηλαδή, για κάθε $(u, v) \in E$ ισχύει επίσης ότι $(v, u) \in E$) και ότι κάθε ζεύγος αντιπαράλληλων ακμών $(u, v), (v, u) \in E$ αποθηκεύεται σε ένα μόνο μη-κατευθυνόμενο αντίγραφο στον διαμεσολαβητή. Τόσο η αλληλεπίδραση $(u, v)$, όσο και η $(v, u)$ επιτρέπονται (αν $(u, v), (v, u) \in E$) και αντιστοιχίζονται στο ένα και μοναδικό αντίγραφο $\{u, v\}$ του διαμεσολαβητή. Ισοδύναμα, στην περίπτωση που δεν υπάρχει διαμεσολαβητής, μοντελοποιούμε αυτή την υπόθεση συσχετίζοντας κάθε κάθε δικατευθυνόμενη ακμή του γράφου επικοινωνίας μέ έναν μοναδικό buffer. Επιπρόσθετα, επειδή στο νέο μοντέλο διατηρούμε την υπόθεση μυητή-αποκρινόμενου (για λόγους συνέπειας με τα πρωτόκολλα πληθυσμών) εάν εφαρμοσθεί ο κανόνας $(a, b, s) \to (a', b', s')$, τότε $a$ και $a'$ είναι, αντίστοιχα, η παλιά και νέα κατάσταση του μυητή, $b$ και $b'$ του αποκρινόμενου και $s$ και $s'$ της μη-κατευθυνόμενης

ακμής που τους συνδέει. Στην μη-κατευθυνόμενη περίπτωση υποθέτουμε την ύπαρξη και του αντίστροφου (ως προς τους ρόλους των πρακτόρων) κανόνα $(b, a, s) \rightarrow (b', a', s')$ ο οποίος επιφέρει ακριβώς το ίδιο αποτέλεσμα. Εάν είναι προφανές, επομένως, ότι αναφερόμαστε σε μη-κατευθυνόμενο γράφο θα παρουσιάζουμε έναν μόνο εκ των δύο ισοδύναμων κανόνων.

## 4.2 Το Νέο Μοντέλο

### 4.2.1 Πρωτόκολλα Πληθυσμών με Διαμεσολαβητή

Ένα *πρωτόκολλο πληθυσμού με διαμεσολαβητή* $\mathcal{A}$ αποτελείται από πεπερασμένα *αλφάβητα εισόδου* και *εξόδου* $X$ και $Y$, ένα πεπερασμένο *καταστάσεων πρακτόρων* $Q$, μία *συνάρτηση εισόδου πρακτόρων* $I : X \rightarrow Q$ που αντιστοιχίζει εισόδους σε καταστάσεις πρακτόρων, μία *συνάρτηση εξόδου πρακτόρων* $O : Q \rightarrow Y$ που αντιστοιχίζει καταστάσεις πρακτόρων σε εξόδους, ένα πεπερασμένο σύνολο *καταστάσεων ακμών* $S$, μία *συνάρτηση εισόδου ακμών* $\iota : X \rightarrow S$ που αντιστοιχίζει εισόδους σε κατατάσεις ακμών, μία *συνάρτηση εξόδου ακμών* $\omega : S \rightarrow Y$ που αντιστοιχίζει καταστάσεις ακμών σε εξόδους, μία *οδηγία εξόδου* $r$, ένα πεπερασμένο ολικά διατεταγμένο *σύνολο από κόστη* $K$, μία *συνάρτηση κόστους* $c : E \rightarrow K$ που αναθέτει ένα κόστος σε κάθε ακμή του γράφου επικοινωνίας και μία συνάρτηση μετάβασης $\delta : Q \times Q \times K \times S \rightarrow Q \times Q \times K \times S$ (από εδώ και στο εξής θα υποθέτουμε πάντοτε ότι το κόστος παραμένει το ίδιο μετά την εφαρμογή της $\delta$ και για το λόγο αυτό δεν θα καθορίζουμε επιστρεφόμενο κόστος από τη $\delta$). Εάν $\delta(q_i, q_j, x, s) = (q_i', q_j', s')$ (το οποίο, σύμφωνα με την υπόθεση που κάναμε, είναι ισοδύναμο με το $\delta(q_i, q_j, x, s) = (q_i', q_j', x, s')$) καλούμε το $(q_i, q_j, x, s) \rightarrow (q_i', q_j', s')$ *μετάβαση* και ορίζουμε $\delta_1(q_i, q_j, x, s) = q_i'$, $\delta_2(q_i, q_j, x, s) = q_j'$ και $\delta_3(q_i, q_j, x, s) = s'$. Θα καλούμε την $\delta_1$ *απόκτημα του μυητή*, την $\delta_2$ *απόκτημα του αποκρινόμενου* και την $\delta_3$ *απόκτημα της ακμής* μετά την αντίστοιχη αλληλεπίδραση.

Στις περισσότερες των περιπτώσεων θα υποθέτουμε ότι $K \subset \mathbb{Z}^+$ και ότι $c_{max} = \max_{w \in K}\{w\} = \mathcal{O}(1)$. Γενικά, αν $c_{max} = \max_{w \in K}\{|w|\} = \mathcal{O}(1)$ τότε κάθε πράκτορας μπορεί να αποθηκεύει το πολύ $k$ αθροιστικά κόστη (το πολύ την τιμή $kc_{max}$), για κάποιο $k = \mathcal{O}(1)$ και λέμε ότι η συνάρτηση κόστους είναι *χρήσιμη* (αξίζει να παρατηρήσει κανείς ότι αν το $K$ εξαρτιόταν από το μέγεθος του πληθυσμού τότε οι πράκτορες και οι ακμές δεν θα μπορούσαν να συγκρατήσουν ούτε ένα κόστος και τότε θα ήταν αδύνατη οποιασδήποτε μορφής βελτιστοποίηση).

Ένα πρωτόκολλο πληθυσμού με διαμεσολαβητή τρέχει σε ένα γράφο επικοινωνίας $G = (V, E)$, όπου το $V$ είναι ένας πληθυσμός $|V| = n$ πρακτόρων

και $E$ είναι μία μη-ανακλαστική δυαδική σχέση επί του $V$, της οποίας ο πληθάριθμος συμβολίζεται ως $m$. Στην περίπτωση ενός μη-κατευθυνόμενου γράφου απλώς απαιτούμε η $E$ να είναι επίσης συμμετρική και για κάθε $(u,v),(v,u) \in E$, οι $(u,v)$ και $(v,u)$ να μοιράζονται τον ίδιο buffer (επίσης, στην μη-κατευθυνόμενη περίπτωση υποθέτουμε ότι αν $\delta(q_i,q_j,x,s) = (q_i',q_j',s')$ τότε $\delta(q_j,q_i,x,s) = (q_j',q_i',s')$), για κάθε $(q_i,q_j,x,s) \in Q \times Q \times K \times S$). Τόσο στην κατευθυνόμενη όσο και στην μη-κατευθυνόμενη περίπτωση, μία $(u,v) \in E$ σημαίνει ότι η αλληλεπίδραση $(u,v)$ επιτρέπεται στην οποία ο $u$ είναι ο *μυητής* και ο $v$ ο *αποκρινόμενος*.

Μία *διαμόρφωση δικτύου* είναι μία αντιστοιχία $C : V \cup E \to Q \cup S$ που καθορίζει την κατάσταση πράκτορα για κάθε πράκτορα του πληθυσμού και την κατάσταση ακμής για κάθε ακμή του γράφου επικοινωνίας. Αν θέλουμε να επικεντρώσουμε το ενδιαφέρον μας μόνο στις καταστάσεις των πρακτόρων, μπορούμε να χρησιμοποιούμε την αντιστοιχία $C_V : V \to Q$ η οποία καλείται *διαμόρφωση πληθυσμού*, ενώ αν θέλουμε να επικεντρωθούμε μόνο στις καταστάσεις των ακμών μπορούμε να χρησιμοποιούμε την *διαμόρφωση ακμών* $C_E : E \to S$. Έστω $C$ και $C'$ δύο διαμορφώσεις δικτύου και έστω $u$ και $v$ δύο διαφορετικοί πράκτορες του πληθυσμού. Λέμε ότι η $C$ πηγαίνει στην $C'$ μέσω της *συνάντησης* $e = (u,v)$ και συμβολίζουμε $C \xrightarrow{e} C'$, εάν

$$
\begin{aligned}
&C'(u) = \delta_1(C(u),C(v),x,C(e)),\\
&C'(v) = \delta_2(C(u),C(v),x,C(e)),\\
&C'(e) = \delta_3(C(u),C(v),x,C(e)),\ \text{και}\\
&C'(z) = C(z),\ \text{για κάθε } z \in (V - \{u,v\}) \cup (E - e).
\end{aligned}
$$

Λέμε ότι η $C$ μπορεί να πάει στην $C'$ σε ένα βήμα και συμβολίζουμε με $C \to C'$, αν $C \xrightarrow{e} C'$ για κάποια συνάντηση $e \in E$. Η σχέση "μπορεί να πάει στην" (σε ένα ή περισσότερα βήματα) ορίζεται και πάλι ως η μεταβατική θήκη της "μπορεί να πάει σε ένα βήμα στην". Τυπικά, γράφουμε $C \xrightarrow{*} C'$, αν υπάρχει μία ακολουθία διαμορφώσεων δικτύου $C = C_0, C_1, \ldots, C_t = C'$, τέτοια ώστε $C_i \to C_{i+1}$ για κάθε $i$, όπου $0 \leq i < t$, και στην περίπτωση αυτή λέμε ότι η $C'$ είναι *προσβάσιμη* απ' την $C$.

Μία *εκτέλεση* είναι μία πεπερασμένη ή άπειρη ακολουθία διαμορφώσεων δικτύου $C_0, C_1, C_2, \ldots$ τέτοια ώστε για κάθε $i$, $C_i \to C_{i+1}$. Μία άπειρη εκτέλεση είναι *δίκαιη*, εάν για κάθε ζεύγος διαμορφώσεων πληθυσμού $C$ και $C'$, τέτοιων ώστε $C \to C'$, αν η $C$ εμφανίζεται άπειρο αριθμό φορών στην εκτέλεση, τότε και η $C'$ εμφανίζεται άπειρο αριθμό φορών στην εκτέλεση. Ένας *υπολογισμός* είναι μία (άπειρη) δίκαιη εκτέλεση. Ισοδύναμα, λέμε ότι ο εχθρικός δρομολογητής είναι δίκαιος αν η ακολουθία αλληλεπιδράσεων που επιλέγει οδηγεί πάντοτε σε δίκαιη εκτέλεση.

Αξίζει να παρατηρήσει κανείς ότι ο *κώδικας* ενός πρωτοκόλλου πληθυσμού με διαμεσολαβητή έχει *σταθερό μέγεθος* (ανεξάρτητο του μεγέθους του πληθυσμού) και, επομένως, μπορεί να αποθηκευτεί σε κάθε πράκτορα του πληθυσμού. Ως εκ τούτου, διατηρείται η ιδιότητα *ομοιομορφίας* και επιπλέον τόσο οι πράκτορες όσο και οι ακμές έχουν σταθερή μνήμη, άρα, διατηρείται και η ιδιότητα *ανωνυμίας*.

### 4.2.2 Ο Υπολογισμός στο Νέο Μοντέλο

Λέμε ότι μία διαμόρφωση δικτύου $C$ είναι *σταθερής-εξόδου πρακτόρων*, αν $O(C'(u)) = O(C(u))$ για κάθε $u \in V$ και για κάθε $C'$ τ.ώ. $C \xrightarrow{*} C'$. Επιπλέον, αν επεκτείνουμε την $O$ σε μία συνάρτηση $O : \mathcal{C}_V \to \mathcal{Y}_V$, όπου $\mathcal{C}_V = Q^V$ και $\mathcal{Y}_V = Y^V$, τότε μπορούμε να γράφουμε $O(C'_V) = O(C'_V)$ για κάθε $C'$ τ.ώ. $C \xrightarrow{*} C'$ και θα εννοούμε και πάλι ότι η $C$ είναι σταθερής-εξόδου πρακτόρων. Λέμε ότι μία διαμόρφωση δικτύου $C$ είναι *σταθερής-εξόδου ακμών*, αν $\omega(C'(e)) = \omega(C(e))$ για κάθε $e \in E$ και για κάθε $C'$ τ.ώ. $C \xrightarrow{*} C'$ (γράφουμε και $\omega(C'_E) = \omega(C_E)$ αν επεκτείνουμε την $\omega$ σε $\omega : \mathcal{C}_E \to \mathcal{Y}_E$, όπου $\mathcal{C}_E = S^E$ και $\mathcal{Y}_E = Y^E$). Τέλος, μία διαμόρφωση θα λέγεται *καθολικής σταθερής-εξόδου*, εάν είναι σταθερής-εξόδου πρακτόρων και σταθερής-εξόδου ακμών. Αν η $C$ είναι σταθερής εξόδου πρακτόρων, τότε σε όλες τις διαμορφώσεις που είναι προσβάσιμες απ' την $C$ η καθολική ανάθεση εξόδου $y : V \cup E \to Y$ παραμένει η ίδια. Αυτό ισχύει γιατί κάθε διαμόρφωση σχετίζεται με μία τέτοια ανάθεση εξόδου αφού, αν $y$ είναι η καθολική ανάθεση εξόδου κατά μία διαμόρφωση $C$ και έχουμε συναρτήσεις εξόδου $O$ και $\omega$, τότε η $y$ ορίζεται ως $y(u) = O(C(u))$, αν $u \in V$ και $y(e) = \omega(C(e))$, αν $e \in E$, άρα $y = O \circ C$, αν η είσοδος ανήκει στο $V$ και $y = \omega \circ C$, αν η είσοδος ανήκει στο $E$.

Ας δούμε τώρα τί είναι η οδηγία $r$ που έχουμε εισαγάγει στον ορισμό του μοντέλου. Η οδηγία αυτή απλώς ενημερώνει τον διαχειριστή ή τον χρήστη του συστήματος σχετικά με το πώς να λάβει και να ερμηνεύσει την έξοδο του υπολογισμού. Ο λόγος που εισάγουμε την οδηγία αυτή είναι απλός: Ένα πρωτόκολλο με διαμεσολαβητή μπορεί να υπολογίζει μία συνάρτηση (ίσως και με τη βοήθεια των ακμών) και να δίνει την έξοδό του ως μία νάθεση εξόδου των πρακτόρων, ακριβώς όπως και τα πρωτόκολλα πληθυσμών, όμως επιπλέον μπορεί να μαρκάρει κάποιον υπογράφο αν τέτοιο ήταν το πρόβλημα για το οποίο σχεδιάστηκε. Για παράδειγμα, εάν ένα πρωτόκολλο υπολογίζει ένα κατηγόρημα πάνω στις αναθέσεις εισόδου πρακτόρων, τότε μία κατάλληλη οδηγία $r$ θα ήταν: *"Συνέλλεξε οποιοδήποτε $u \in V$ και δες την έξοδό του"*. Στην περίπτωση αυτή θα ονομάζουμε μία διαμόρφωση σταθερής-εξόδου πρακτόρων, $r$-σταθερή διαμόρφωση. Ας θεωρήσουμε τώρα το πρόβλημα:

**Πρόβλημα 1 (Ακμές ελαχίστου κόστους).** *Δοθέντος ενός μη-κατευθυνόμενου*

*συνεκτικού γράφου επικοινωνίας $G = (V, E)$ και μίας χρήσιμης συνάρτησης οικογένειακόστους $c : E \to K$ πάνω στο σύνολο των ακμών, όπου $K \subset \mathbb{Z}^+$, να σχεδιαστεί ένα πρωτόκολλο με διαμεσολαβητή που να βρίσκει τις ακμές ελαχίστου κόστους του $E$.*

Ένα πρωτόκολλο για το πρόβλημα αυτό θα πρέπει με κάποιο τρόπο να μαρκάρει τις ακμές ελαχίστου κόστους. Μία κατάλληλη οδηγία $r$ για την περίπτωση αυτή θα ενημέρωνε απλώς τον χρήστη ότι μόνο οι ακμές που τελικά ανήκουν στην κλάση 1 πρέπει να συλλεχθούν, δηλαδή, $r$: *"Συνέλλεξε κάθε $e \in E$ για την οποία ισχύει $\omega(s_e) = 1$"*, όπου με $s_e$ συμβολίζουμε την κατάσταση της $e$, π.χ. αν ο χρήστης εφαρμόσει την οδηγία $r$ κατά την διαμόρφωση $C$, τότε $s_e = C(e)$. Παρατηρούμε ότι στην περίπτωση αυτή μία $r$-σταθερή διαμόρφωση $C$ θα μπορούσε απλώς να είναι μία διαμόρφωση σταθερής-εξόδου ακμών ή μία διαμόρφωση όπου για κάθε $C'$ που είναι προσβάσιμη απ' την $C$ το υποσύνολο του $E$ που δίνει έξοδο $1$ δεν αλλάζει.

Επιπρόσθετα, μία οδηγία $r$ θα μπορούσε να είναι ένα κατηγόρημα πάνω στις (καθολικές) αναθέσεις εξόδου. Για παράδειγμα, μία οδηγία τέτοιου τύπου είναι η "Εάν υπάρχει τουλάχιστον ένας πράκτορας με έξοδο $0$, απέρριψε, αλλιώς, αποδέξου". Με μια πρώτη ματιά θα έλεγε κανείς ότι για να παρθεί μία τέτοια απόφαση, θα πρέπει κάποια καθολική μηχανή Turing να εκτελέσει έναν υπολογισμό πάνω στην έξοδο, όμως, όπως θα δούμε, αυτό μπορεί να επιτευχθεί μέσω ενός νέου τρόπου "σύνθεσης" δύο πρωτοκόλλων όπου το ένα εκ των δύο υλοποιεί την $r$.

Γενικεύοντας τα παραπάνω, μία διαμόρφωση $C$ θα λέγεται $r$-σταθερή εάν ικανοποιεί μία απ' τις ακόλουθες δύο συνθήκες:

- Εάν το πρόβλημα αφορά σε έναν υπογράφο που πρέπει να βρεθεί, τότε η $C$ σταθεροποιεί έναν υπογράφο που δεν πρέπει να τροποποιείται σε καμία $C'$ που είναι προσβάσιμη απ' την $C$.
- Εάν το πρόβλημα αφορά σε μία συνάρτηση που πρέπει να υπολογιστεί από τους πράκτορες, τότε η $C$ πρέπει να είναι σταθερής-εξόδου πρακτόρων.

**Ορισμός 13.** *Θα λέμε ότι ένα πρωτόκολλο $\mathcal{A}$* ***επιλύει σταθερά*** *ένα πρόβλημα $\Pi$, εάν για κάθε στιγμιότυπο $I$ του $\Pi$ και κάθε υπολογισμό (δίκαιη εκτέλεση) του $\mathcal{A}$ στο $I$, το δίκτυο φτάνει σε μία $r$-σταθερή διαμόρφωση $C$ που δίνει την σωστή λύση για $I$ εάν ερμηνευθεί σύμφωνα με την οδηγία εξόδου $r$. Στην ειδική περίπτωση που το $\Pi$ είναι μία προς υπολογισμό συνάρτηση $f$, θα λέμε ότι το $\mathcal{A}$* ***υπολογίζει σταθερά*** *την $f$.*

**Ορισμός 14.** *Στην ειδική περίπτωση που το $\Pi$ είναι ένα πρόβλημα βελτιστοποίησης (όπως το Πρόβλημα 1), ένα πρωτόκολλο που επιλύει σταθερά το $\Pi$ θα καλείται* ***πρωτόκολλο βελτιστοποίησης*** *για το πρόβλημα $\Pi$.*

**Ορισμός 15.** *Θα λέμε ότι ένα πρόβλημα* ***επιδέχεται διαμεσολαβητή*** *εάν υπάρχει πρωτόκολλο πληθυσμού με διαμεσολαβητή που το επιλύει σταθερά.*

### 4.2.3 Μερικά Πρωτόκολλα Γράφων

Μία αξιοσημείωτη δυνατότητα του νέου μοντέλου είναι ότι μπορεί να επιλύει σταθερά ορισμένα σημαντικά γραφοθεωρητικά προβλήματα που αφορούν π.χ. σε εύρεση υπογράφων του γράφου επικοινωνίας. Βέβαια, παρότι έχουμε καταφέρει ήδη να κατασκευάσουμε πρωτόκολλα για ορισμένα αντιπροσωπευτικά προβλήματα αυτής της κατηγορίας, δεν είμαστε ακόμα σε θέση να γνωρίζουμε περισσότερα πράγματα σχετικά με την κλάση των προβλημάτων που επιλύει σταθερά το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή.

#### Μεγιστοτικό Ταίριασμα

Αρχικά, θα παρουσιάσουμε ένα πρωτόκολλο πληθυσμού με διαμεσολαβητή (MPP, απ' το Mediated Population Protocol) το οποίο επιλύει σταθερά το ευρέως διαδεδομένο πρόβλημα, στην Επιστήμη των Υπολογιστών, του μεγιστοτικού ταιριάσματος:

**Πρόβλημα 2 (Μεγιστοτικό Ταίριασμα).** *Δοθέντος ενός μη-κατευθυνόμενου γράφου επικοινωνίας $G = (V, E)$, να βρεθεί ένα μεγιστοτικό ταίριασμα, δηλαδή, ένα σύνολο $E' \subseteq E$ τ.ώ. να μην υπάρχουν δύο στοιχεία του $E'$ με κοινό άκρο στο $V$ και, επιπρόσθετα, δεν υπάρχει $e \in E - E'$ τ.ώ. η $e$ να μην έχει κοινό άκρο με κάθε στοιχείο του $E'$.*

Με απλά λόγια, ένα υποσύνολο των ακμών είναι μεγιστοτικό ταίριασμα, αν οι ακμές αυτές ανά δύο δεν έχουν κοινό άκρο και δεν υπάρχει καμία ακμή εκτός του υποσυνόλου αυτού που να μην έχει κοινό άκρο με καμία ακμή του υποσυνόλου (για τον τελευταίο λόγο ένα μεγιστοτικό ταίριασμα δεν μπορεί να αυξηθεί εισάγοντας του κάποια ακμή, αφού δεν υπάρχει καμία επιπλέον ακμή που να μπορεί να εισαχθεί στο μεγιστοτικό ταίριασμα χωρίς να καταστρέψει την ιδιότητα του ταιριάσματος). Ας δούμε ένα πρωτόκολλο, ονόματι $MaximalMatching$, για το πρόβλημα αυτό:

**MaximalMatching**

- $X = \{0\}$, $Y = \{0, 1\}$,
- $Q = \{q_0, q_1\}$, $S = \{0, 1\}$,
- $I(0) = q_0$,

- $\iota(0) = 0$, $\omega(0) = 0$, $\omega(1) = 1$,
- $r$: *"Συνέλλεξε κάθε* $e \in E$ *για την οποία ισχύει* $\omega(s_e) = 1$",
- $\delta$:

$$(q_0, q_0, 0) \to (q_1, q_1, 1)$$

Στο σημείο αυτό θα πρέπει να αναφέρουμε ορισμένες σημαντικές διευκρινήσεις. Πρώτα απ' όλα, επειδή το πρόβλημα δεν έχει να κάνει με κόστη, θεωρούμε ότι η $\delta$ είναι της ειδικότερης μορφής $\delta : Q \times Q \times S \to Q \times Q \times S$. Επιπρόσθετα, επειδή ο γράφος είναι μη-κατευθυνόμενος, αν λόγου χάρην είχαμε κάποια μετάβαση $(q_i, q_j, s) \to (q'_i, q'_j, s')$, τότε θα υποθέταμε, χωρίς να την παρουσιάζουμε, την ύπαρξη της συμμετρικής μετάβασης $(q_j, q_i, s) \to (q'_j, q'_i, s')$. Στο συγκεκριμένο πρωτόκολλο δεν υπάρχει τέτοια ανάγκη, αφού ο συμμετρικός κανόνας του μοναδικού κανόνα του πρωτοκόλλου είναι ο ίδιος κανόνας. Οποιαδήποτε άλλη μετάβαση δεν εμφανίζεται στα πρωτόκολλα που σχεδιάζουμε (πέραν των συμμετρικών μεταβάσεων) υποθέτουμε ότι υπάρχει αλλά είναι ταυτοτική μετάβαση, δηλαδή δεν τροποποιεί κανένα από τα τρία στοιχεία που δέχεται ως είσοδο (χάρην απλότητας), π.χ. στο πρωτόκολλο $MaximalMatching$ μερικοί απ' τους μη-εμφανιζόμενους ταυτοτικούς κανόνες των οποίων υποθέτουμε την ύπαρξη είναι οι $(q_0, q_1, 0) \to (q_0, q_1, 0)$ και $(q_1, q_1, 1) \to (q_1, q_1, 1)$. Τέλος, να πούμε ότι δεν καθορίζουμε μία συνάρτηση εξόδου πρακτόρων, καθώς θα διαβάσουμε την έξοδο μόνο απ' τις εξόδους των ακμών. ΣΥνήθως, αν κάποιο στοιχείο του ορισμού δεν είναι απαραίτητο για την ορθότητα του πρωτοκόλλου θα αποφεύγουμε τον ορισμό του.

**Θεώρημα 8.** *Το πρωτόκολλο* $MaximalMatching$ *επιλύει σταθερά το πρόβλημα του μεγιστοτικού ταιριάσματος.*

*Απόδειξη.* Έστω $M(C)$ το υποσύνολο των ακμών που βρίσκονται στην κατάσταση 1 κατά τη διαμόρφωση $C$. Έστω ότι κατά τη διαμόρφωση $C$ συμβαίνει η αλληλεπίδραση $e = (u, v)$ και έστω $C \xrightarrow{e} C'$ και $e \notin M(C)$. Σύμφωνα με το μοναδικό κανόνα της $\delta$, για να ισχύει $e \in M(C')$ θα πρέπει $C(u) = C(v) = q_0$. Εάν αυτό ισχύει τότε έχουμε $e \in M(C')$, δηλαδή $C'(e) = 1$ και $C'(u) = C'(v) = q_1$, δηλαδή η $e$ περνάει στην κατάσταση 1 ενώ οι $u$ και $v$ περνούν στην $q_1$ για να υποδεικνύουν ότι εφάπτονται με κάποια ακμή που ανήκει στο τρέχον σύνολο $M(C')$. Από εδώ και πέρα, καμία ακμή που συμπίπτει με την $e$ (έχει κοινό άκρο) δεν μπορεί να μπει στο σύνολο, απλούστατα διότι ο κόμβος στον οποίο συμπίπτει με την $e$ είναι στην

κατάσταση $q_1$. Ακόμα και να επιτρέπαμε στο δρομολογητή να επιλέγει πολλαπλά ζεύγη προς αλληλεπίδραση, είναι προφανές ότι κανένας κόμβος δεν θα μπορούσε να συμμετέχει σε περισσότερα από ένα ζεύγη. Τα παραπάνω αποδεικνύουν ότι το $M(C)$ είναι ταίριασμα για κάθε $C$ οποιουδήποτε υπολογισμού. Επισπρόσθετα, δεν μπορεί να υπάρχει ακμή που δεν συγκρούεται με το τελικό ταίριασμα που να μην μπει τελικά στο ταίριασμα, αφού το ότι δεν συγκρούεται αποδεικνύει ότι και τα δύο άκρα της είναι στην $q_0$ και ο μόνος τρόπος να πάψουν να είναι στην $q_0$, είναι να την επιλέξει ο δρομολογητής, το οποίο λόγω της συνθήκης δικαιοσύνης τελικά θα συμβεί. Το τελευταίο αποδεικνύει ότι το ταίριασμα που τελικά κατασκευάζει το πρωτόκολλο είναι πάντοτε μεγιστοτικό. □

### Μεταβατική Θήκη με τη Βοήθεια ενός Αρχηγού

Ας υποθέσουμε ότι $G = (V, E)$ είναι ένας γράφος που ανήκει στην οικογένεια $\mathcal{G}^d_{All}$, δηλαδή, στην όλων-των-ζευγών οικογένεια κατευθυνόμενων γράφων επικοινωνίας και ότι ένα πρωτόκολλο (ή οποιαδήποτε άλλη προεπεξεργαστική διαδικασία) έχει ήδη υπολογίσει έναν υπογράφο του $G$, $G' = (V', E')$, θέτοντας κάθε $e \in E'$ στην κατάσταση $1$ και κάθε $e \in E - E'$ (δηλαδή, όλες τις υπόλοιπες ακμές) στην κατάσταση $0$. Προφανώς, το $V'$ απλώς περιλαμβάνει κάθε κόμβο που αποτελεί άκρο τουλάχιστον μίας ακμής του $E'$. Θέλουμε να κατασκευάσουμε ένα MPP που να επιλύει σταθερά το ακόλουθο πρόβλημα:

**Πρόβλημα 3 (Μεταβατική Θήκη).** *Δοθέντος ενός γράφου επικοινωνίας $G = (V, E)$ από την $\mathcal{G}^d_{All}$ με έναν εκ των προτέρων υπολογισθέντα υπογράφο $G' = (V', E')$ σύμφωνα με τα παραπάνω, να βρεθεί η μεταβατική θήκη του $G'$, δηλαδή, να βρεθεί ένα νέο σύνολο ακμών $E^*$ το οποίο θα περιλαμβάνει μία κατευθυνόμενη ακμή $(u, v)$ για κάθε $u, v \in V'$ για τους οποίους υπάρχει μηκενό μονοπάτι από τον $u$ στον $v$ στον $G'$ (αξίζει να παρατηρήσουμε ότι πάντοτε $E' \subseteq E^*$).*

Υποθέτουμε μία *ελεγχόμενη ανάθεση εισόδου* $W : E \to X$ που μοντελοποιεί την έξοδο της προεπεξεργαστικής διεργασίας-πρωτοκόλλου, δηλαδή, $f(e) = 1$ ανν $e \in E'$. Επιπλέον, υποθέτουμε ότι αρχικά όλοι οι πράκτορες είναι στην κατάσταση $q_0$ εκτός από έναν μοναδικό εκλεγμένο (από οποιοδήποτε πρωτόκολλο εκλογής αρχηγού) *αρχηγό* που είναι στην κατάσταση $l$. Η υπόθεση σχετικά με τον αρχηγό και η ιδέα ότι η ύπαρξή του βοηθάει τα πρωτόκολλα πρωτοεμφανίστηκε στο [3] και μελετήθηκε εκτενώς στο [5]. Ακολουθεί ο ορισμός του MPP, $TranClos$ που επιλύει σταθερά το Πρόβλημα 3:

**TranClos**

- $X = Y = \{0, 1\}$,

- $Q = \{l, q_0, q_1, q_1', q_2, q_2', q_3\}$, $S = \{0, 1\}$,
- *ελεγχόμενη ανάθεση εισόδου*: "$W(e') = 1$, *για κάθε* $e' \in E'$, *και* $W(e) = 0$, *για κάθε* $e \in E - E'$",
- $\iota(x) = x$, για κάθε $x \in X$, $\omega(s) = s$, για κάθε $s \in S$,
- $r$: "*Συνέλλεξε κάθε* $e \in E$ *για την οποία ισχύει* $\omega(s_e) = 1$",
- $\delta$:

$$\begin{array}{rcl@{\qquad}rcl} (l, q_0, 0) & \to & (q_0, l, 0) & (q_2, q_0, 1) & \to & (q_2', q_3, 1) \\ (l, q_0, 1) & \to & (q_1, q_2, 1) & (q_1, q_3, x) & \to & (q_1', q_0, 1), \text{ για } x \in \{0, 1\} \\ (q_1, q_2, 1) & \to & (q_0, l, 1) & (q_1', q_2', 1) & \to & (q_0, l, 1) \end{array}$$

**Θεώρημα 9.** *Το πρωτόκολλο* $TranClos$ *επιλύει σταθερά το πρόβλημα της μεταβατικής θήκης.*

*Απόδειξη.* Έστω $E'$ το υποσύνολο των ακμών που βρίσκονται αρχικά στην κατάσταση 1 (όλες οι υπόλοιπες ακμές του πλήρους διγραφήματος $G$ είναι αρχικά στην κατάσταση 0). Το $E'$ είναι μία δυαδική σχέση επί του $V'$. Η μεταβατική θήκη του $E'$ σε συνδυασμό με το $V'$ συνιστούν τη μεταβατική θήκη του $G'$ (που ζητείται να υπολογιστεί), αφού κάθε κόμβος του $V - V'$ δεν είναι προσβάσιμος απ' το $E'$ και συνεπώς δεν μπορεί να είναι προσβάσιμος ούτε από την μεταβατική θήκη του $E'$.

Επιπρόσθετα, δεν υπάρχει κανόνας στην $\delta$ που να μεταρέπει την κατάσταση μίας ακμής από 1 σε 0. Αυτό, σε συνδυασμό με το γεγονός ότι η έξοδος σύμφωνα με την οδηγία $r$ είναι κάθε ακμή που βρίσκεται στην κατάσταση 1, συνεπάγεται ότι το $E'$ είναι πάντοτε υποσύνολο του $E^*$ (όπου $E^*$ το υποσύνολο του $E$ που το πρωτόκολλο δίνει ως έξοδο).

Το πρωτόκολλο πάντα κάνει τα ακόλουθα: Αρχικά, υπάρχει ένας μοναδικός αρχηγός $u$ στην κατάσταση $l$ και όλοι οι υπόλοιποι πράκτορες είναι στην $q_0$. Όταν ο αρχηγός $u$ αλληλεπιδράσει με κάποιον πράκτορα $v$ που είναι στην $q_0$ μέσω της ακμής $(u, v)$ που είναι στην κατάσταση 0, οι πράκτορες ανταλλάσσουν τις καταστάσεις τους, δηλαδή, πλέον ο $v$ είναι ο μοναδικός αρχηγός. Εάν, ανταυτού, η $(u, v)$ είναι στην κατάσταση 1, τότε ο αρχηγός $u$ πηγαίνει στην $q_1$ και ο $v$ στην $q_2$. Μετά από αυτό, όλοι οι πράκτορες είναι στην $q_0$ εκτός απ' τους $u$ και $v$ που είναι στις $q_1$ και $q_2$, αντίστοιχα, η $(u, v)$ είναι στην 1 και μόνο οι κανόνες $(q_1, q_2, 1) \to (q_0, l, 1)$ και $(q_2, q_0, 1) \to (q_2', q_3, 1)$ μπορούν να εφαρμοσθούν (οι υπόλοιποι που μπορούν είναι ταυτοτικοί). Εάν εφαρμοσθεί ο πρώτος, τότε ο πληθυσμός περνάει σε μία διαμόρφωση παρόμοια με την αρχική, στην οποία υπάρχει ένας μοναδικός αρχηγός ενώ όλοι οι υπόλοιποι

πράκτορες είναι στην $q_0$. Ο κανόνας αυτός (παρότι μπορεί να μην είναι προφανές το γιατί) είναι πολύ σημαντικός καθώς εξασφαλίζει ότι εάν ο $v$ που είναι στην $q_2$, δεν έχει κανένα εξερχόμενο γείτονα $w$, τ.ώ. $q_w = q_0$ και $s_{(v,w)} = 1$, τότε το πρωτόκολλο δε θα "κολλήσει". Εάν ο δεύτερος κανόνας εφαρμοσθεί πρώτα, τότε αυτό σημαίνει ότι ο $v$ έχει μόλις αλληλεπιδράσει με έναν πράκτορα $w$ που είναι στην $q_0$ και όπου η $(v, w)$ είναι στην κατάσταση 1. Στην περίπτωση αυτή, ο $v$ μεταβαίνει στην $q_2'$ και ο $w$ στην $q_3$. Μετά από αυτό το βήμα, το πρωτόκολλο έχει σχηματίσει ένα κατευθυνόμενο μονοπάτι $uvw$, με καταστάσεις πρακτόρων $q_1$, $q_2'$, $q_3$, αντιστοίχως, και τις $(u, v)$ και $(v, w)$ (δηλαδή, τις ακμές του μονοπατιού) στην κατάσταση 1. Πλέον μόνο ο κανόνας $(q_1, q_3, x) \to (q_1', q_0, 1)$ μπορεί να εφαρμοσθεί (και τελικά θα εφαρμοσθεί λόγω της συνθήκης δικαιοσύνης), ο οποίος αναθέτει την κατάσταση 1 στην ακμή $(u, w)$. Τελικά, το πρωτόκολλο απομένει και πάλι με έναν μοναδικό αρχηγό, $v$, και όλοι οι υπόλοιποι πράκτορες είναι στην $q_0$, επαναλαμβάνοντας την ίδια γενική λειτουργία που μόλις περιγράψαμε.

Έστω $u$, $v$, $w$ τρις πράκτορες για τους οποίους $(u, v), (v, w) \in E'$ (δηλαδή, αυτές οι ακμές είναι αρχικά στην κατάσταση 1). Όπως είπαμε, το πρωτόκολλο τελικά (λόγω της συνθήκης δικαιοσύνης) θα επιλέξει κάποιο μονοπάτι $uvw$ και θα αναθέσει την κατάσταση 1 στην $(u, w)$. Επίσης, είδαμε ότι το $E'$ διατηρείται, συνεπώς το $TranClos$ τελικά κατασκευάζει ένα σύνολο $E_1$ που περιλαμβάνει το $E'$ και που για κάθε $(u, v), (v, u) \in E'$ ισχύει $(u, w) \in E_1$. Το $E_1$ είναι η *μεταβατική επέκταση* του $E'$. Όμως, το πρωτόκολλο συνεχίζει να λειτουργεί και επιδρά πάνω στο $E_1$ ακριβώς με τον ίδιο τρόπο όπως και στο $E'$, καθώς τελικά η νέα του "είσοδος" είναι το $E_1$, παράγοντας ένα νέο σύνολο $E_2$, που είναι η μεταβατική επέκταση του $E_1$ κ.ο.κ. μέχρι να κατασκευάσει μία σχέση $E^*$ που δεν μπορεί να επεκταθεί περαιτέρω. Όταν συμβεί αυτό το πρωτόκολλο θα έχει φτάσει σε μία διαμόρφωση σταθερής-εξόδου ακμών, αφού από εδώ και στο εξής καμία ακμή δεν μπορεί να αλλάξει την κατάστασή της και συνεπώς ούτε και την τιμή εξόδου της. Προφανώς, η $E^*$, δηλαδή το τελικό σύνολο εξόδου που αποτελείται από όλες τις ακμές στην κατάσταση 1, είναι η μεταβατική θήκη του $E'$ και η απόδειξη έχει ολοκληρωθεί. □

### Ακμές Ελαχίστου Κόστους

Στην Ενότητα 4.2.2 παρουσιάσαμε το Πρόβλημα 1 το οποίο αφορούσε στην κατασκευή ενός πρωτοκόλλου βελτιστοποίησης το οποίο θα βρίσκει τις ακμές ελαχίστου κόστους ενός μη-κατευθυνόμενου γραφήματος. Εδώ ορίζουμε ένα τέτοιο πρωτόκολλο, ονόματι $MinEdges$, και αποδεικνύουμε την ορθότητά του.

**MinEdges**

- $X = Y = \{0, 1\}$,
- $Q = K \cup \{q_0\}$, $S = \{0, 1\}$,
- $I(x) = q_0$, για κάθε $x \in X$,
- $\iota(x) = 0$, για κάθε $x \in X$, $\omega(s) = s$, για κάθε $s \in S$,
- $r$: *"Συνέλλεξε κάθε $e \in E$ για την οποία ισχύει $\omega(s_e) = 1$"*,
- $\delta$:

$$
\begin{aligned}
(q_0, q_0, c, d) &\to (c, c, 1) \\
(c_i, c_j, c, d) &\to (c, c, 1), \text{ εάν } c \leq \min\{c_i, c_j\} \\
&\to (\min\{c_i, c_j\}, \min\{c_i, c_j\}, 0), \text{ εάν } c > \min\{c_i, c_j\} \\
(c_i, q_0, c, d) &\to (c, c, 1), \text{ εάν } c \leq c_i \\
&\to (c_i, c_i, 0), \text{ εάν } c > c_i
\end{aligned}
$$

**Θεώρημα 10.** *Το πρωτόκολλο $MinEdges$ είναι ένα πρωτόκολλο βελτιστοποίησης για το πρόβλημα εύρεσης των ακμών ελαχίστου κόστους.*

*Απόδειξη.* Πρέπει να δείξουμε ότι το σύστημα φτάνει σε μία $r$-σταθερή διαμόρφωση δικτύου $C$, όπου εάν $E_{out}$ είναι το υποσύνολο του $E$ που προσδιορίζεται απ' την οδηγία $r$, τότε έχουμε $e \in E_{out}$ εάν και μόνον εάν $c(e) = c_{opt}$, όπου $c_{opt} = \min_{e \in E}\{c(e)\}$.

Οι κανόνες της $\delta$ σε συνδυασμό με τη συνθήκη διακαιοσύνης εξασφαλίζουν ότι κάθε πράκτορας θα πάρει τελικά το $c_{opt}$ (ένα μικρότερο κόστος πάντοτε αντικαθιστά το τρέχον κόστος ενός πράκτορα). Τη στιγμή αυτή το σύστημα θα έχει περάσει σε μία διαμόρφωση σταθερής-εξόδου πρακτόρων, αφού δεν θα υπάρχει κόστος μικρότερο απ' το $c_{opt}$ ούτως ώστε να να το αντικαταστήσει (το $c_{opt}$ είναι το μικρότερο δυνατό). Από εδώ και στο εξής, μετά από κάθε αλληλεπίδραση $(u, v)$, όπου $e = \{u, v\}$

1. $E_{out} \leftarrow E_{out} \cup \{e\}$, εάν το κόστος κανενός πράκτορα δεν είναι μικρότερο από το $c(e)$ (δηλαδή, αυτό ισχύει στην περίπτωση που $c(e) = c_{opt}$),
2. $E_{out} \leftarrow E_{out} - \{e\}$, διαφορετικά.

Προκύπτει, επομένως, ότι το σύστημα τελικά θα βρεθεί σε κάποια διαμόρφωση $C$, όπου $e \in E_{out}$ θα συνεπάγεται ότι $c(e) = c_{opt}$ ενώ $e \notin E_{out}$ ότι $c(e) > c_{opt}$. Μόλις συμβεί αυτό, καμία ακμή δε θα είναι πλέον σε θέση να μπει

ή να βγει απ' το $E_{out}$, και αφού το $E_{out}$ είναι το σύνολο που προσδιορίζεται απ' την οδηγία $r$, η $C$ θα είναι μία $r$-σταθερή διαμόρφωση. Έτσι, το $MinEdges$ πράγματι είναι ένα πρωτόκολλο βελτιστοποίησης για το Πρόβλημα 1. □

### Συντομότερο Μονοπάτι Ρίζας-Φύλλων

Τώρα θα παρουσιάσουμε ένα πρωτόκολλο βελτιστοποίησης, ονόματι $SRLpath$, για το πρόβλημα της εύρεσης του συντομότερου μονοπατιού που συνδέει τη ρίζα ενός έξω-κατευθυνόμενου δέντρου (κατευθυνόμενο *arborescence*, στο οποίο όλες οι ακμές κατευθύνονται από τον πατέρα στα παιδιά του και ποτέ το αντίστροφο) με κάποιο από τα φύλλα του. Τυπικά, το πρόβλημα ορίζεται ως εξής:

**Πρόβλημα 4.** *Δοθέντος ότι ο γράφος επικοινωνίας $G = (V, E)$ είναι ένα έξω-κατευθυνόμενο δέντρο και δοθείσας μίας χρήσιμης συνάρτηση κόστους $c : E \to K$ πάνω στο σύνολο των ακμών, να σχεδιαστεί ένα πρωτόκολλο που θα βρίσκει το μονοπάτι ελαχίστου κόστους απ' το μη-κενό σύνολο $P = \{p \mid$ το $p$ είναι ένα μονοπάτι από τη ρίζα προς ένα φύλλο και $c(p) = \mathcal{O}(1)\}$, όπου $c(p)$ είναι μία συντομογραφία του $\sum_{e \in p} c(e)$.*

Υποθέτουμε ότι η μέγιστη τιμή που μπορεί να αποθηκεύσει κάθε πράκτορας είναι $kc_{max}$, όπου τόσο το $k$ όσο και το $c_{max} = \max_{e \in E}\{c(e)\}$, είναι σταθερά και ανεξάρτητα του μεγέθους του πληθυσμού ($|V| = n$), δοθείσας μίας συνάρτησης κόστους $c : E \to K$ που παίρνει μη-αρνητικές ακέραιες τιμές.

Εάν υπάρχει τουλάχιστον ένα μονοπάτι $p$ τ.ώ. $c(p) = \sum_{e \in p} c(e) < kc_{max}$, τότε το $SRLpath$ θα σταθεροποιηθεί τελικά επιστρέφοντας το συντομότερο τέτοιο μονοπάτι, διαφορετικά απλώς θα επιστρέψει οποιοδήποτε μονοπάτι (από τη ρίζα ως τα φύλλα), χωρίς να εξασφαλίζει ότι είναι το συντομότερο δυνατό, αλλά στην περίπτωση αυτή η τιμή εξόδου της ρίζας θα είναι $0$ υποδεικνύοντας την αδυναμία του πρωτοκόλλου να βρει το συντομότερο μονοπάτι.

**SRLpath**

- $X = \{0, 1\}$,
- $Y = \{0, 1\} \cup Q$,
- $Q = \{q_0, q_s\} \cup \{(i, j) \mid i \in \{q_1, q_2, q_3, q_s\}$ και $j \in \{0, 1, 2, \ldots, kc_{max}\}$,
- $I(x) = q_0$, για κάθε $x \in X$,
- $O(q_1, kc_{max}) = 0$, $O(q) = q$, για κάθε $q \in Q - \{(q_1, kc_{max})\}$,

- $S = \{0, 1\}$,
- $\iota(x) = 0$, για κάθε $x \in X$,
- $\omega(s) = s$, για κάθε $s \in S$,
- $r$: *"Εάν η ρίζα δώσει ως έξοδο 0, απόρριψε, διαφορετικά ξεκινώντας από τη ρίζα ακολούθησε κάθε ακμή με έξοδο* $1$*, μέχρι να φτάσεις σε κάποιο φύλλο"*,
- $\delta$:

$$
\begin{aligned}
(q_0, q_0, c, 0) &\to ((q_1, c), q_0, 1) \\
(q_0, (q_1, c_1), c, 0) &\to ((q_1, kc_{max}), (q_1, c_1), 1), \text{ εάν } c_1 + c > kc_{max} \\
&\to ((q_1, c_1 + c), (q_1, c_1), 1), \text{ διαφορετικά} \\
((q_1, c_1), (q_1, c_2), c, 1) &\to ((q_1, kc_{max}), (q_1, c_2), 1), \text{ εάν } c_2 + c > kc_{max} \\
&\to ((q_1, c_2 + c), (q_1, c_2), 1), \text{ διαφορετικά} \\
((q_1, c_1), (q_1, c_2), c, 0) &\to ((q_2, c_2 + c), (q_s, c_2), 1), \text{ εάν } c_2 + c < c_1 \\
((q_2, c_1), (q_i, c_2), c, 1) &\to ((q_3, c_1), (q_i, c_2), 0), \text{ για } i \in \{1, 2, 3\} \\
((q_3, c_1), (q_s, c_2), c, 1) &\to ((q_1, c_1), (q_1, c_2), 1) \\
((q_1, c_1), q_0, c, 0) &\to ((q_2, c), q_s, 1), \text{ εάν } c < c_1 \\
((q_2, c_1), q_0, c, 1) &\to ((q_3, c_1), q_0, 0) \\
((q_3, c_1), q_s, c, 1) &\to ((q_1, c_1), q_0, 1)
\end{aligned}
$$

**Θεώρημα 11.** *Εάν υπάρχει τουλάχιστον ένα μονοπάτι* $p$ *από τη ρίζα ως τα φύλλα, όπου* $c(p) < kc_{max}$*, τότε το* $SRLpath$ *είναι ένα πρωτόκολλο βελτιστοποίησης για το Πρόβλημα 4. Διαφορετικά, η ρίζα δίνει ως έξοδο την τιμή* $0$ *υποδεικνύοντας ότι δεν υπάρχει τέτοιο μονοπάτι.*

*Απόδειξη.* Η απόδειξη είναι με επαγωγή στο πλήθος των κόμβων του κατευθυνόμενου arborescence $T$. Έστω $\mathcal{T}_i = \{T \mid \text{το } T \text{ είναι ένα κατευθυνόμενο arborescence με } i \text{ κόμβους}\}$, δηλαδή, η οικογένεια όλων των έξω-κατευθυνόμενων δέντρων που αποτελούνται από $i$ κόμβους. Υπάρχει μόνο ένα δέντρο στην $\mathcal{T}_1$, το ίδιο και στην $\mathcal{T}_2$, όπου το μοναδικό της δέντρο αποτελείται από δύο μόνο κόμβους συνδεδεμένους με μία κατευθυνόμενη ακμή. Προφανώς, το $SRLpath$ πάντα βρίσκει το συντομότερο μονοπάτι ρίζας-φύλλων σε κάθε κατευθυνόμενο arborescence με το πολύ 2 κόμβους, κατά τετριμμένο τρόπο. Έστω ότι για κάθε κατευθυνόμενο arborescence με το πολύ $n$ κόμβους, το

$SRLpath$ πάντοτε βρίσκει το συντομότερο μονοπάτι ρίζας-φύλλων. Έστω $T_{n+1}$ οποιοδήποτε κατευθυνόμενο arborescence με $(n+1)$ κόμβους. Αγνοώντας τη ρίζα του $T_{n+1}$ και τις εξερχόμενες από αυτήν ακμές, παίρνουμε τουλάχιστον ένα ή περισσότερα έξω-κατευθυνόμενα δέντρα με το πολύ $n$ κόμβους. Σε κάθε τέτοιο υποδέντρο γνωρίζουμε λόγω της επαγωγικής υπόθεσης ότι το $SRLpath$ πάντοτε βρίσκει το συντομότερο μονοπάτι ρίζας-φύλλων. Επιπρόσθετα, εύκολα μπορεί να δει κανείς ότι το πρωτόκολλο πάντοτε κρατάει στη ρίζα του δέντρου το κόστος του επιλεγμένου μονοπατιού ρίζας-φύλλων. Έστω $u$ η ρίζα που αφαιρέσαμε και $v_j$, όπου $j = \{1, 2, \ldots, t\}$, τα $t$ παιδιά της. Κάθε παιδί $v_j$ θα έχει τελικά μαρκάρει το συντομότερο μονοπάτι ρίζας-φύλλων στο υποδέντρο του οποίου είναι ρίζα και επομένως τελικά η ρίζα θα περιέχει στην κατάστασή της το κόστος αυτού του μονοπατιού, $c(p_j)$. Συνεπώς, τελικά ο $u$ θα επιλέξει το παιδί του $\arg\min_{v_j}\{c(p_j) + c(u, v_j)\}$ (ή κάποιο απ' αυτά αν είναι πολλά), το οποίο θα είναι το συντομότερο μονοπάτι ρίζας-φύλλων του $T_{n+1}$. Αξίζει να παρατηρήσουμε ότι εάν $\min_{v_j}\{c(p_j) + c(u, v_j)\} < kc_{max}$, τότε τουλάχιστον ένα τέτοιο μονοπάτι μπορεί να επιλεγεί από τη ρίζα (τελικά θα επιλεγεί το συντομότερο) και ως εκ τούτου σε αυτή την περίπτωση δεν πρόκειται να πάρουμε έξοδο $0$ απ' τη ρίζα. Από την άλλη, αν δεν υπάρχει τέτοιο μονοπάτι, τότε $\min_{v_j}\{c(p_j) + c(u, v_j)\} \geq kc_{max}$ και ο $u$ μπορεί να αποθηκεύσει μέχρι την τιμή $kc_{max}$, πράγμα το οποίο τελικά θα κάνει και σε συνδυασμό με την κατάσταση $q_1$ (αφού $O(q_1, kc_{max}) = 0$) θα δίνει πάντοτε έξοδο $0$, υποδεικνύοντας ότι δεν υπάρχει τέτοιο μονοπάτι. □

### 4.2.4 Προσεγγιστικά Πρωτόκολλα

Μία ακόμα ενδιαφέρουσα ιδιότητα του μοντέλου των πρωτοκόλλων πληθυσμών με διαμεσολαβητή είναι ότι μας επιτρέπουν να ορίσουμε αυτά που θα αποκαλούμε προσεγγιστικά πρωτόκολλα. Άτυπα, αυτά είναι πρωτόκολλα που σταθεροποιούνται πάντοτε σε μία αποδεκτή λύση για ένα πρόβλημα βελτιστοποίησης που αφορά κάποια οικογένεια γράφων επικοινωνίας που είναι αποδεδειγμένα "κοντά" στην βέλτιστη λύση, όπου το κοντά αναφέρεται στο συνολικό κόστος (κέρδος) ή τον συνολικό πληθάριθμο της λύσης.

Τυπικά, ένα πρόβλημα βελτιστοποίησης, $\Pi$ αποτελείται από:

- Ένα σύνολο *στιγμιοτύπων*, $D_\Pi$
- Κάθε στιγμιότυπο $I \in D_\Pi$ έχει ένα σύνολο *αποδεκτών λύσεων*, $S_\Pi(I)$. Επιπλέον, υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου που, δοθέντος ενός ζεύγους $(I, s)$, αποφασίζει εάν $s \in S_\Pi(I)$.
- Υπάρχει μία υπολογίσιμη σε πολυωνυμικό χρόνο *αντικειμενική συνάρτηση* $f_\Pi$, η οποία αναθέτει ένα μη-αρνητικό ρητό αριθμό σε κάθε ζεύγος

$(I, s)$, όπου $I$ είναι ένα στιγμιότυπο του $\Pi$ και $s$ είναι μία αποδεκτή λύση για το $I$ (συνήθως η αντικειμενική συνάρτηση έχει ένα αντίστοιχο φυσικό νόημα όπως κόστος, μήκος, κέρδος, βάρος κ.ο.κ.).

- Τέλος, το $\Pi$ είναι είτε ένα *πρόβλημα ελαχιστοποίησης* είτε ένα *πρόβλημα μεγιστοποίησης*.

Στα ακόλουθα εξετάζουμε μόνο την περίπτωση κατά την οποία το $\Pi$ είναι πρόβλημα ελαχιστοποίησης, ενώ οι ορισμοί για προβλήματα μεγιστοποίησης είναι ανάλογοι.ς Μία βέλτιστη λύση για ένα στιγμιότυπο ενός προβλήματος ελαχιστοποίησης είναι μία αποδεκτή λύση που επιτυγχάνει τη μικρότερη δυνατή τιμή για την αντικειμενική συνάρτηση. Θα συμβολίζουμε με OPT($I$) την τιμή αντικειμενικής συνάρτησης μίας βέλτιστης λύσης του στιγμιοτύπου $I$ (συνήθως, και όταν δεν υπάρχει πιθανότητα να προκληθεί σύγχυση, θα γράφουμε εν συντομία OPT)

Έστω $\Pi$ ένα πρόβλημα ελαχιστοποίησης και έστω $\kappa$ ένας θετικός ακέραιος αριθμός, $\kappa \geq 1$. Ένα πρωτόκολλο $\mathcal{A}$ θα λέμε ότι είναι ένα $\kappa$-προσεγγιστικό πρωτόκολλο για το $\Pi$ εάν για κάθε στιγμιότυπο του $\Pi$ και κάθε δίκαιη εκτέλεση του $\mathcal{A}$ στο $I$, το δίκτυο φτάνει τελικά σε μία $r$-σταθερή διαμόρφωση $C$, η οποία εάν ερμηνευτεί σύμφωνα με την οδηγία εξόδου $r$ του $\mathcal{A}$ δίνει μία αποδεκτή λύση $s$ για το $I$ τ.ώ.

$$f_{\Pi}(I, s) \leq \kappa \cdot \text{OPT}(I)$$

Ας θεωρήσουμε το ευρέως διαδεδομένο πρόβλημα του καλύμματος κορυφών ελαχίστου πληθαρίθμου (minimum cardinality vertex cover):

**Πρόβλημα 5 (Ελάχιστο Κάλυμμα Κορυφών).** *Δοθέντος ενός μη-κατευθυνόμενου γράφου επικοινωνίας $G = (V, E)$, να βρεθεί ένα κάλυμμα κορυφών ελαχίστου πληθαρίθμου, δηλαδή, ένα σύνολο $V' \subseteq V$ τ.ώ. κάθε ακμή $e \in E$ έχει τουλάχιστον ένα άκρο στο $V'$.*

Όπως θα δούμε στη συνέχεια, η κλάση των προβλημάτων που επιδέχονται διαμεσολαβητή είναι ακόμα ανοικτή και δεν γνωρίζουμε εάν το παραπάνω πρόβλημα επιδέχεται διαμεσολαβητή, παρότι εικάζουμε ότι δεν επιδέχεται. Αν η υπόθεση αυτή ισχύει τότε το καλύτερο για το οποίο μπορούμε να ελπίζουμε είναι ένα προσεγγιστικό πρωτόκολλο για το πρόβλημα αυτό. Το ευχάριστο είναι ότι υπάρχει ένα προσεγγιστικό πρωτόκολλο το οποίο εγγυάται ότι στην χειρότερη περίπτωση θα επιστρέψει ένα κάλυμμα κορυφών με διπλάσιο πληθάριθμο απ' το βέλτιστο.

Στο Θεώρημα 8 αποδείξαμε ότι το πρωτόκολλο $MaximalMatching$ επιδέχεται διαμεσολαβητή. Ας θεωρήσουμε ένα πρωτόκολλο, ονόματι $VerteCover$ το οποίο συμφωνεί σε όλα με το $MaximalMatching$ εκτός από την οδηγία $r$ η

οποία τώρα είναι $r$: "Συνέλλεξε κάθε $v \in V$ για τον οποίο ισχύει $O(q_v) = 1$", όπου $q_v$ είναι η κατάσταση του πράκτορα $v$. Διαισθητικά, πλέον συλλέγουμε όλους τους πράκτορες που πρόσκεινται σε κάποια ακμή του μεγιστοτικού ταιριάσματος, με άλλα λόγια το πρωτόκολλο δίνει ως έξοδο τους κόμβους των ακμών του ταιριάσματος. Παραθέτουμε το πρωτόκολλο $VertexCover$ για να διευκολύνουμε τη συζήτηση:

**VertexCover**

- $X = \{0\}$, $Y = \{0, 1\}$,
- $Q = \{q_0, q_1\}$, $S = \{0, 1\}$,
- $I(0) = q_0$,
- $\iota(0) = 0$, $\omega(0) = 0$, $\omega(1) = 1$,
- $r$: "*Συνέλλεξε κάθε $v \in V$ για τον οποίο ισχύει $O(q_v) = 1$*",
- $\delta$:

$$(q_0, q_0, 0) \rightarrow (q_1, q_1, 1)$$

**Θεώρημα 12.** *Το πρωτόκολλο $VertexCover$ είναι ένα 2-προσεγγιστικό πρωτόκολλο για το πρόβλημα του καλύμματος κορυφών ελαχίστου πληθαρίθμου.*

*Απόδειξη.* Σύμφωνα με το Θεώρημα 8 οι τελικές ακμές που δίνει ως έξοδο το πρωτόκολλο, έστω $M$ το σύνολό τους, αποτελούν ένα μεγιστοτικό ταίριασμα του $G$. Επομένως, το σύνολο των άκρων τους, έστω $R$, είναι ένα κάλυμμα κορυφών, γιατί εάν υπάρχει έστω και μία ακμή $e$ που δεν καλύπτεται απ' το $R$, τότε η ακμή αυτή θα μπορούσε μπει στο $M$, αφού δεν συγκρούεται με καμία άλλη ακμή του $M$. Όμως τότε το $M$ δεν θα ήταν μεγιστοτικό, αφού θα υπήρχε κάποια ακμή που ενώ μπορούσε να εισαχθεί στο $M$, το πρωτόκολλο δεν την εισήγαγε. Άρα, το $R$ είναι κάλυμμα κορυφών και έστω ALG $= |R|$. Επιπρόσθετα, πάντοτε ισχύει $|M| \leq$ OPT (για κάθε $M$ και για κάθε OPT), αφού οποιοδήποτε κάλυμμα κορυφών θα πρέπει να καλύπτει τουλάχιστον μία φορά κάθε ακμή οποιουδήποτε ταιριάσματος του γραφήματος (αφού καμία ακμή ενός ταιριάσματος δεν έχει κοινό άκρο με καμία άλλη ακμή του ίδιου ταιριάσματος) και ισχύει ALG $= 2|M|$, αφού για κάθε ακμή του $M$ το $VertexCover$ δίνει ως έξοδο δύο κορυφές. Άρα, τελικά ALG $\leq$ 2OPT και συνεπώς το $VertexCover$ είναι ένα 2-προσεγγιστικό πρωτόκολλο για το πρόβλημα του καλύμματος κορυφών ελαχίστου πληθαρίθμου. (Η ανάλυση εδώ είναι απ' το εισαγωγικό κεφάλαιο του [21]). □

# Κεφάλαιο 5

# Υπολογιστική Ισχύς του MPP

*"E pur si muove!"*

*Galileo (legend)*

## 5.1 Εισαγωγή

Στο κεφάλαιο αυτό θα διατυπώσουμε και θα αποδείξουμε το βασικό Θεώρημα της παρούσας εργασίας, το οποίο σε γενικές γραμμές δείχνει ότι το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή είναι ένα ισχυρότερο υπολογιστικό μοντέλο από το μοντέλο των πρωτοκόλλων πληθυσμών. Δυστυχώς, δεν είμαστε ακόμα σε θέση να πούμε πόσο ισχυρότερο είναι το νέο μοντέλο και η ποσοτικοποίηση αυτού του ερωτήματος είναι ο βασικός μελλοντικός ερευνητικός μας στόχος.

Για να δείξουμε το αποτέλεσμα αυτό θα χρειαστούμε μία παραλλαγή του μοντέλου των πρωτοκόλλων πληθυσμών στην οποία οι είσοδοι μπορούν να μεταβάλλονται, αλλά σε πεπερασμένο χρονικό διάστημα πρέπει να σταθεροποιούνται σε κάποια τελική ανάθεση εισόδου. Το μοντέλο αυτό ονομάζεται μοντέλο πρωτοκόλλων πληθυσμών με *σταθεροποιούμενες εισόδους* και προτάθηκε στο [2].

## 5.2 Σταθεροποιούμενες Είσοδοι

Ας υποθέσουμε ότι υπάρχει ένα πεπερασμένο σύνολο συμβόλων εισόδου $X$ (κατά τα γνωστά) και ότι κάθε πράκτορας έχει μία ξεχωριστή θύρα εισόδου στην οποία γίνεται διαθέσιμο το τρέχον σύμβολο εισόδου σε κάθε βήμα του υπολογισμού. Υποθέτουμε ότι μεταξύ δύο υπολογιστικών βημάτων (μεταξύ, δηλαδή, δύο διαδοχικών επιλογών του δρομολογητή) οι είσοδοι οποιουδήποτε

υποσυνόλου των πρακτόρων μπορεί να τροποποιηθούν αυθαίρετα (φυσικά, με νέα σύμβολα απ' το $X$).

Τυπικά, τροποποιούμε τη συνάρτηση μετάβασης, έτσι ώστε να είναι πλέον της μορφής $\delta : (Q \times X) \times (Q \times X) \to Q \times Q$. Δηλαδή, όταν δύο πράκτορες $u$, $v$ επιλεχθούν προς αλληλεπίδραση μέσω της ακμής $(u, v)$, αν $q_u$ είναι η τρέχουσα κατάσταση και $\sigma_u$ το τρέχον σύμβολο εισόδου του $u$ και $q_v$ είναι η τρέχουσα κατάσταση και $\sigma_v$ το τρέχον σύμβολο εισόδου του $v$ και αν $\delta((q_u, \sigma_u), (q_v, \sigma_v)) = (q'_u, q'_v)$, τότε μετά την αλληλεπίδραση ο $u$ μεταβαίνει στην κατάσταση $q'_u$, ο $v$ στην $q'_v$ και τα σύμβολα εισόδου και των δύο παραμένουν αμετάβλητα. Παρ' όλα αυτά, θεωρούμε ότι τα σύμβολα εισόδου παραμένουν αμετάβλητα μόνον λόγω της αλληλεπίδρασης καθώς μπορεί τελικά να μεταβληθούν αρκετές φορές μέχρι την επόμενη επιλογή του δρομολογητή, αλλά για λόγους ανεξάρτητους της λειτουργίας του πρωτοκόλλου (π.χ. γιατί οι πράκτορες παρατηρούν (μέσω των αισθητήρων τους) δεδομένα που μεταβάλλονται χρονικά, αλλά που κάποια στιγμή σταθεροποιούνται). Εδώ μία διαμόρφωση $C$ είναι μία συνάρτηση $C : V \to Q \times X$ που καθορίζει την κατάσταση και την είσοδο κάθε πράκτορα του πληθυσμού, ενώ κατά τα γνωστά, αν $C(u) = (q, \sigma)$, τότε $\pi_1(C(u)) = q$ και $\pi_2(C(u)) = \sigma$ (δεν χρησιμοποιούμε τα $C_1$ και $C_2$ γιατί έτσι δυσχεραίνεται η αρίθμηση των διαμορφώσεων του υπολογισμού). Υποθέτουμε ότι αρχικά κάθε πράκτορας βρίσκεται σε μία αρχική κατάσταση (ίδια για όλους) και οι είσοδοι είναι αυθαίρετες. Η έξοδος μίας διαμόρφωσης $C$ συμβολίζεται ως $y_C$ είναι μία συνάρτηση $y_C : V \to Y$, όπου $y_C(u) = O(\pi_1(C(u)))$, για κάθε $u \in V$, δηλαδή, προκύπτει εφαρμόζοντας την συνάρτηση εξόδου στις συνιστώσες κατάστασης των πρακτόρων κατά τη διαμόρφωση $C$.

Τώρα πρέπει να δώσουμε ένα νέο ορισμό για τη σχέση "μπορεί να πάει σε ένα βήμα στην" πάνω στο σύνολο $\mathcal{C}$ των διαμορφώσεων. Έστω δύο διαμορφώσεις $C$ και $C'$ (όχι απαραίτητα διαφορετικές) και έστω $u, v \in V$ με $u \neq v$. Λέμε ότι η $C$ πηγαίνει στην $C'$ μέσω της *συνάντησης* $e = (u, v)$ και συμβολίζουμε με $C \xrightarrow{e} C'$, εάν

$$\begin{aligned}
&\pi_1(C'(u)) = \delta_1(C(u), C(v)),\\
&\pi_1(C'(v)) = \delta_2(C(u), C(v)), \text{ και}\\
&\pi_1(C'(w)) = \pi_1(C(w)), \text{ για κάθε } w \in V - \{u, v\}.
\end{aligned}$$

Επομένως, οι καταστάσεις των $u$ και $v$ στην $C'$ έχουν ανανεωθεί βάσει της $\delta$ χρησιμοποιώντας τις καταστάσεις και τις εισόδους των $u$ και $v$ στην $C$, ενώ η κατάσταση κάθε άλλου πράκτορα $w$ παραμένει αμετάβλητη από την $C$ στην $C'$. Λέμε ότι η $C$ μπορεί να πάει στην $C'$ σε ένα βήμα και συμβολίζουμε με $C \to C'$, αν $C \xrightarrow{e} C'$ για κάποια συνάντηση $e \in E$.

Οι εκτελέσεις ορίζεται όπως και προηγουμένως, ωστόσο θα πρέπει να δια-

χωρίσουμε με κάποιον τρόπο τις εκτελέσεις εκείνες στις οποίες οι είσοδοι σταθεροποιούνται. Λέμε ότι μία εκτέλεση $C_0, C_1, C_2, \ldots$ έχει *σταθεροποιούμενες εισόδους* εάν υπάρχει κάποιο πεπερασμένο βήμα $k$ μετά το οποίο η είσοδος κάθε πράκτορα παύει να αλλάζει. Επομένως, υπάρχει μία *τελική ανάθεση εισόδου* $x : V \to X$ τ.ώ. $x(u) = \pi_2(C_t(u))$ για κάθε $u \in V$ και κάθε $t \geq k$. Μία εκτέλεση έχει *αμετάβλητες εισόδους* εάν για κάθε $u \in V$ η είσοδος του $u$ δεν αλλάζει ποτέ, δηλαδή, αν $k = 0$ (όλες οι είσοδοι σταθεροποιούνται στο μηδενικό βήμα). Παρατηρούμε, επομένως, ότι οι αμετάβλητες είσοδοι είναι μία ειδική περίπτωση των σταθεροποιούμενων εισόδων.

Μία εκτέλεση με σταθεροποιούμενες εισόδους είναι *δίκαιη* εάν για κάθε διαμόρφωση $C$ που εμφανίζεται άπειρο αριθμό φορών στην εκτέλεση και κάθε διαμόρφωση $C'$ τ.ώ. η ανάθεση εισόδου κατά την $C'$ είναι η ίδια με την ανάθεση εισόδου κατά την $C$ και $C \to C'$, η $C'$ εμφανίζεται επίσης άπειρο αριθμό φορών στην εκτέλεση. Τέλος, ένας *υπολογισμός* είναι (όπως και πριν) μία δίκαιη εκτέλεση.

Επιπρόσθετα, στο [2] ορίζονται οι ιδιότητες γράφων με ταμπέλες. Εδώ θεωρούμε γράφους, στους οποίους οι κόμβοι έχουν το σύμβολο εισόδου τους ως ταμπέλα. Μία *ιδιότητα γράφου με ταμπέλες* $P$ είναι μία αντιστοιχία από ζεύγη $(G, x)$ στο $\{0, 1\}$, όπου $G$ είναι ένας γράφος επικοινωνίας και $x$ είναι μία ανάθεση εισόδου για τον $G$. Ένα πρωτόκολλο $\mathcal{A}$ υπολογίζει σταθερά την ιδιότητα γράφου με ταμπέλα $P$ με σταθεροποιούμενες εισόδους στην οικογένεια γράφων $\mathcal{G}$ εάν για κάθε $G \in \mathcal{G}$ και κάθε ανάθεση εισόδου $x$ στον $G$, κάθε υπολογισμός του $\mathcal{A}$ στον $G$ που ξεκινάει απ' την αρχική διαμόρφωση και έχει εισόδους που σταθεροποιούνται σε μία τελική ανάθεση $x$ σταθεροποιείται στην έξοδο $P(G, x)$ (όλοι οι πράκτορες συμφωνούν τελικά ως προς τη σωστή έξοδο). Από εδώ και στο εξής θα αναφερόμαστε στις ιδιότητες γράφων με ταμπέλες, ως κατηγορήματα. Ένα κατηγόρημα είναι *σταθερά υπολογίσιμο με σταθεροποιούμενες εισόδους* εάν υπάρχει πρωτόκολλο που το υπολογίζει σταθερά με σταθεροποιούμενες εισόδους.

**Ορισμός 16.** *Η **μη-περιορισμένη** οικογένεια γράφων επικοινωνίας περιέχει όλους τους δυνατούς συνεκτικούς κατευθυνόμενους γράφους επικοινωνίας και συμβολίζεται με $\mathcal{G}^d_{Unr}$.*

Ακολουθούν ορισμένα πολύ σημαντικά αποτελέσματα που αφορούν στο μοντέλο των σταθεροποιούμενων εισόδων, τα οποία παραθέτουμε χωρίς απόδειξη (τα τρία πρώτα είναι από το [2] ενώ το τέταρτο από το [6]).

**Θεώρημα 13.** *Κάθε ημιγραμμικό κατηγόρημα (Presburger καθορίσιμο κατηγόρημα) είναι σταθερά υπολογίσιμο με σταθεροποιούμενες εισόδους στην $\mathcal{G}^d_{All}$.*

**Θεώρημα 14.** *Για κάθε πρωτόκολλο $\mathcal{A}$ υπάρχει ένα πρωτόκολλο $\mathcal{B}$ τ.ώ. για κάθε $n$, εάν το $\mathcal{A}$ υπολογίζει σταθερά ένα κατηγόρημα $p$ με σταθεροποιούμενες*

*εισόδους στον $G \in \mathcal{G}^d_{All}$, όπου $|V(G)| = n$ και $G' \in \mathcal{G}^d_{Unr}$ όπου επίσης $|V(G')| = n$, τότε το $\mathcal{B}$ υπολογίζει σταθερά το $p$ με σταθεροποιούμενες εισόδους στον $G'$.*

**Πόρισμα 9.** *Τα ημιγραμμικά κατηγορήματα είναι σταθερά υπολογίσιμα με σταθεροποιούμενες εισόδους στην $\mathcal{G}^d_{Unr}$.*

**Θεώρημα 15.** *Τα κατηγορήματα που είναι σταθερά υπολογίσιμα απ' το μοντέλο των πρωτοκόλλων πληθυσμών με σταθεροποιούμενες εισόδους είναι ακριβώς τα ημιγραμμικά κατηγορήματα.*

Το τελευταίο αποτέλεσμα δείχνει ότι το μοντέλο των σταθεροποιούμενων εισόδων είναι ισοδύναμο με το κλασικό μοντέλο των πρωτοκόλλων πληθυσμών (με αμετάβλητες εισόδους). Και τα δύο μοντέλα μπορούν να υπολογίζουν μόνο ημιγραμμικά κατηγορήματα γεγονός που συνεπάγεται ότι κάθε πρωτόκολλο με αμετάβλητες εισόδους μπορεί να μετατραπεί σε ένα ισοδύναμο πρωτόκολλο με σταθεροποιούμενες εισόδους (αξίζει να σημειώσουμε ότι μια γενική διαδικασία μετατροπής ενός πρωτοκόλλου με αμετάβλητες εισόδους σε ένα ισοδύναμο με σταθεροποιούμενες εισόδους, αν υπάρχει, θα είχε μεγάλη αξία, αλλά μέχρι τώρα δεν έχει προταθεί καμία στη σχετική βιβλιογραφία).

## 5.3 Υπολογισιμότητα στο Μοντέλο MPP

Τώρα είμαστε έτοιμοι να ερευνήσουμε ορισμένες πτυχές της υπολογιστικής ισχύς του μοντέλου των πρωτοκόλλων πληθυσμών με διαμεσολαβητή.

### 5.3.1 Το MPP είναι Ισχυρότερο

Θα ξεκινήσουμε αποδεικνύοντας ένα πολύ σημαντικό αποτέλεσμα σχετικά με το νέο μοντέλο. Το αποτέλεσμα αυτό δείχνει ότι το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή είναι ισχυρότερο από το μοντέλο των πρωτοκόλλων πληθυσμών ως προς την κλάση των κατηγορημάτων που τα δύο μοντέλα υπολογίζουν σταθερά. Η γενική ιδέα είναι η εξής: το μοντέλο των πρωτοκόλλων πληθυσμών είναι ειδική περίπτωση του μοντέλου με διαμεσολαβητή, άρα το νέο μοντέλο είναι τουλάχιστον όσο ισχυρό είναι και το μοντέλο των πρωτοκόλλων πληθυσμών. Υπάρχει ένα κατηγόρημα το οποίο επιδέχεται διαμεσολαβητή αλλά δεν είναι ημιγραμμικό, άρα υπάρχει τουλάχιστον ένα κατηγόρημα το οποίο είναι σταθερά υπολογίσιμο από το νέο μοντέλο αλλά όχι από το μοντέλο των πρωτοκόλλων πληθυσμών.

**Ορισμός 17.** *Το MPP μοντέλο με τον επιπρόσθετο περιορισμό ότι τρέχει στην όλων-των-ζευγών οικογένεια κατευθυνόμενων γράφων επικοινωνίας ($\mathcal{G}^d_{All}$), θα καλείται **βασικό MPP μοντέλο**.*

Θυμίζουμε ότι παρόμοιος είναι ο ορισμός του βασικού μοντέλου των πρωτοκόλλων πληθυσμών.

**Ορισμός 18.** *Λέμε ότι ένα κατηγόρημα* ***επιδέχεται διαμεσολαβητή ισχυρά****, εάν επιδέχεται διαμεσολαβητή και επιπλέον ισχύει η παραδοχή εξόδου κατηγορημάτων, δηλαδή, όλοι οι πράκτορες τελικά συμφωνούν στην ορθή τιμή εξόδου.*

Επομένως, εάν απλώς πούμε ότι ένα κατηγόρημα επιδέχεται διαμεσολαβητή δεν είναι ξεκάθαρο εάν όλοι οι πράκτορες συμφωνούν στην ορθή τιμή εξόδου. Από την άλλη μεριά, όταν λέμε ότι ένα κατηγόρημα είναι σταθερά υπολογίσιμο θα εννοούμε πάντα ότι είναι σταθερά υπολογίσιμο από το μοντέλο των πρωτοκόλλων πληθυσμών με την παραδοχή εξόδου κατηγορημάτων, δηλαδή όλοι οι πράκτορες τελικά συμφωνούν στην ίδια ορθή τιμή.

**Θεώρημα 16.** *Το μοντέλο των πρωτοκόλλων πληθυσμών είναι ειδική περίπτωση του μοντέλου των πρωτοκόλλων πληθυσμών με διαμεσολαβητή.*

*Απόδειξη.* Αγνοώντας όλες τις συναρτήσεις που αφορούν στις ακμές, τις καταστάσεις των ακμών, τα κόστη των ακμών και την οδηγία εξόδου $r$, μετατρέπουμε το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή στο μοντέλο των πρωτοκόλλων πληθυσμών. □

Όλα τα πορίσματα που ακολουθούν είναι άμεσα επακόλουθα του Θεωρήματος 16, αφού το θεώρημα δείχνει ότι το μοντέλο των πρωτοκόλλων πληθυσμών μπορεί να προσωμοιωθεί από το μοντέλο με διαμεσολαβητή. Επομένως, δεν υπάρχει τίποτα που κάνει το μοντέλο των πρωτοκόλλων πληθυσμών και δεν μπορεί να το κάνει το μοντέλο με διαμεσολαβητή.

**Πόρισμα 10.** *Κάθε σταθερά υπολογίσιμο κατηγόρημα επιδέχεται διαμεσολαβητή ισχυρά.*

**Πόρισμα 11.** *Κάθε σταθερά υπολογίσιμο κατηγόρημα στο βασικό μοντέλο των πρωτοκόλλων πληθυσμών επιδέχεται διαμεσολαβητή ισχυρά στο βασικό MPP μοντέλο.*

**Πόρισμα 12.** *Κάθε σταθερά υπολογίσιμο κατηγόρημα στο μοντέλο των πρωτοκόλλων πληθυσμών με σταθεροποιούμενες εισόδους επιδέχεται διαμεσολαβητή ισχυρά στην προφανή επέκταση του μοντέλου των πρωτοκόλλων πληθυσμών με διαμεσολαβητή έτσι ώστε να έχει σταθεροποιούμενες εισόδους.*

Είναι ευρέως γνωστό ότι η Presburger αριθμητική δεν επιτρέπει τον πολλαπλασιασμό μεταβλητών. Επιπλέον, γνωρίζουμε ότι κάθε ημιγραμμικό κατηγόρημα μπορεί να περιγραφεί από λογικούς τύπους πρώτης-τάξης της Presburger αριθμητικής (Θεώρημα 4) και από το Πόρισμα 8 γνωρίζουμε ότι ένα

κατηγόρημα είναι σταθερά υπολογίσιμο στο βασικό μοντέλο των πρωτοκόλλων πληθυσμών ανν είναι ημιγραμμικό. Για να δείξουμε ότι το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή είναι ισχυρότερο από το μοντέλο των πρωτοκόλλων πληθυσμών, θα δείξουμε ότι το βασικό MPP μοντέλο είναι ισχυρότερο από το βασικό μοντέλο των πρωτοκόλλων πληθυσμών και αφού σύμφωνα με το Πόρισμα 11 έχει τουλάχιστον την ίδια υπολογιστική ισχύ με το βασικό μοντέλο των πρωτοκόλλων πληθυσμών αρκεί να δείξουμε ότι υπάρχει τουλάχιστον ένα μη-ημιγραμμικό κατηγόρημα το οποίο επιδέχεται διαμεσολαβητή ισχυρά στο βασικό MPP μοντέλο (γιατί ένα τέτοιο κατηγόρημα είναι γνωστό ότι δεν είναι σταθερά υπολογίσιμο στο βασικό μοντέλο των πρωτοκόλλων πληθυσμών).

Είναι προφανές ότι το κατηγόρημα "το πλήθος των $c$ ισούται με το γινόμενο του πλήθους των $a$ και του πλήθους των $b$" δεν είναι ημιγραμμικό. Επαναλαμβάνουμε, ότι αυτό ισχύει επειδή ο πολλαπλασιασμός μεταβλητών δεν μπορεί να περιγραφεί από λογικούς τύπους πρώτης-τάξης της Presburger αριθμητικής. Έστω $N_q$ η πολλαπλότητα της κατάστασης $q$ στο πολυσύνολο της αρχικής διαμόρφωσης (μπορούμε να χρησιμοποιήσουμε πολυσύνολο χ.β.τ.γ. διότι ο γράφος επικοινωνίας είναι πλήρης). Τότε, $N_c = N_a \cdot N_b$ είναι μία συντομογραφία του προαναφερθέντος κατηγορήματος.

Το πρωτόκολλο πληθυσμού με διαμεσολαβητή $VarProduct$ που θα περιγράψουμε ευθύς αμέσως, υπολογίζει σταθερά το κατηγόρημα $N_c = N_a \cdot N_b$ στην οικογένεια $\mathcal{G}^d_{All}$.

**VarProduct**

- $X = \{a, b, c, 0\}$, $Y = \{0, 1\}$,
- $Q = \{a, \dot{a}, b, c, \bar{c}, 0\}$, $S = \{0, 1\}$,
- $I(x) = x$, για κάθε $x \in X$, $O(a) = O(b) = O(\bar{c}) = O(0) = 1$, και $O(c) = O(\dot{a}) = 0$,
- $\iota(x) = 0$, για κάθε $x \in X$,
- $r$: *"Εάν υπάρχει τουλάχιστον ένας πράκτορας με τιμή εξόδου 0, απόρριψε, διαφορετικά, αποδέξου."*,
- $\delta$:

$$(a, b, 0) \to (\dot{a}, b, 1)$$
$$(c, \dot{a}, 0) \to (\bar{c}, a, 0)$$
$$(\dot{a}, c, 0) \to (a, \bar{c}, 0)$$

**Θεώρημα 17.** *Το πρωτόκολλο $VarProduct$ υπολογίζει σταθερά (σύμφωνα με του πιο χαλαρό ορισμό της σταθερής υπολογισιμότητας βάσει της οδηγίας $r$) το κατηγόρημα $N_c = N_a \cdot N_b$ στην $\mathcal{G}^d_{All}$.*

*Απόδειξη.* Πρώτα απ' όλα, ας παρατηρήσουμε ότι σε κάθε πλήρη κατευθυνόμενο γράφο αλληλεπιδράσεων, το $N_a \cdot N_b$ ισούται με το πλήθος των κατευθυνόμενων ακμών από πράκτορες που είναι αρχικά στην κατάσταση $a$ προς πράκτορες που είναι αρχικά στην κατάσταση $b$. Η βασική ιδέα είναι ότι θα πρέπει να μαρκάρουμε τόσα $c$ όσο είναι το γινόμενο του αριθμού των $a$ και των $b$. Επομένως, για κάθε $a$ πρέπει να μαρκάρουμε τόσα $c$ όσα είναι τα $b$. Στο μοντέλο των πρωτοκόλλων πληθυσμών, η βασική δυσκολία για τον υπολογισμό ενός τέτοιου κατηγορήματος είναι ότι δεν υπάρχει κανένας τρόπος κάποιος πράκτορς, έστω χ.β.τ.γ. στην κατάσταση $a$, να μπορεί να θυμάται εάν έχει ήδη μετρήσει κάποιον συγκεκριμένο πράκτορα που είναι στην κατάσταση $b$ (κάθε πράκτορας στην $a$ θα έπρεπε να αφήνει τον δικό του προσδιοριστή σε κάθε πράκτορα που έχει μετρήσει, αλλά αυτό δεν επιτρέπεται για πληθαρίθμους της τάξεως του $n$). Εάν π.χ. $N_a = N_b = N_c = \mathcal{O}(n)$, τότε είναι αδύνατον χωρίς μοναδικούς προσδιοριστές κάθε $b$ να μπορεί να θυμάται όλα τα $a$ που το έχουν μετρήσει.

Από την άλλη μεριά, στο μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή αυτό μπορεί να γίνει πολύ εύκολα. Είναι εύκολο να παρατηρήσει κανείς ότι όταν τουλάχιστον ένα εκ των $N_a$, $N_b$ και $N_c$ είναι ίσο με το μηδέν, τότε σε όλες αυτές τις περιπτώσεις, εκτός από την περίπτωση που $N_c = 0$, $N_a \neq 0$ και $N_b \neq 0$, δεν μπορεί να συμβεί καμία μετάβαση και η έξοδος είναι πάντοτε σωστή αν ερμηνευτεί βάσει της οδηγίας $r$. Στην μόνη περίπτωση που ξεχωρίσαμε, ο πρώτος κανόνας της $\delta$ εφαρμόζεται τουλάχιστον μία φορά, ενώ οι άλλοι δύο κανόνες δεν μπορούν να εφαρμοσθούν (αφού το $N_c$ παραμένει πάντοτε μηδέν) και ως εκ τούτου τουλάχιστον ένας πράκτορας μεταβαίνει στην $\dot{a}$, η οποία δίνει έξοδο $0$, χωρίς να μπορεί να φύγει από αυτήν. Παρατηρώντας ότι $N_a \cdot N_b \neq 0$ είναι προφανές ότι σε αυτή την περίπτωση το $VarProduct$ απαντάει ορθά "απόρριψη".

Η ενδιαφέρουσα περίπτωση είναι όταν όλα τα $N_a$, $N_b$ και $N_c$ είναι διάφορα του μηδενός (δηλαδή, αυστηρά θετικά, αφού τα $N_q$ είναι εξ' ορισμού

μη-αρνητικά). Όλες οι ακμές είναι αρχικά στην κατάσταση $0$. Το πρωτόκολλο λειτουργεί ως εξής: Όταν ένας πράκτορας στην $a$ αλληλεπιδρά με έναν πράκτορα στην $b$ διαμέσου μίας ακμής που οδηγεί από τον $a$ (τον πράκτορα με κατάσταση $a$) στον $b$, τότε ο πρώτος μεταβαίνει στην $\dot{a}$ και η ακμή στην $1$. Η τροποίηση της κατάστασης της ακμής που καθορίζει αυτό το συγκεκριμένο ζεύγος $(a, b)$ είναι ό, τι χρειάζεται να θυμάται το πρωτόκολλο ούτως ώστε να μην προσμετρήσει το ίδιο ζεύγος ξανά. Όταν ένας πράκτορας στην κατάσταση $c$ αλληλεπιδρά με έναν πράκτορα στην $\dot{a}$, τότε ο $c$ μαρκάρεται μεταβαίνοντας στην $\bar{c}$ και ο $\dot{a}$ επιστρέφει στην αρχική του λειτουργία μεταβαίνοντας στην $a$. Το κρίσιμη παρατήρηση είναι ότι στην ουσία το πρωτόκολλο προσπαθεί να μαρκάρει $N_a \cdot N_b$ πράκτορες κατάστασης $c$. Εάν $N_c = N_a \cdot N_b$, τότε θα τα καταφέρει και τελικά κανείς πράκτορας δεν θα είναι σε κάποια από τις καταστάσεις $\dot{a}$ και $c$ και, επιπρόσθετα, κανείς πράκτορας δεν θα μπορεί να μεταβεί μελλοντικά σε κάποια απ' αυτές τις καταστάσεις. Επομένως, τελικά το πρωτόκολλο απαντάει ορθά "αποδοχή" σε αυτή την περίπτωση. Εάν $N_c < N_a \cdot N_b$ τότε τελικά τουλάχιστον ένας πράκτορας θα παραμείνει για πάντα στην κατάσταση $\dot{a}$, αφού δεν θα υπάρχει κανένας μη-μαρκαρισμένος πράκτορας στην κατάσταση $c$ για να τον επαναφέρει στην $a$ (όλα τα $c$ μαρκάρονται πριν να έχει ολοκληρωθεί το γινόμενο, αφού είναι λιγότερα από αυτό). Επομένως, στην περίπτωση αυτή το πρωτόκολλο απαντάει ορθά "απόρριψη", αφού $O(\dot{a}) = 0$. Τέλος, όταν $N_c > N_a \cdot N_b$ κάποιοι πράκτορες στην $c$ θα παραμείνουν για πάντα αμαρκάριστοι, αφού το γινόμενο θα ολοκληρωθεί πριν να μαρκαριστούν όλα τα $c$, δηλαδή, θα απομένουν κάποια $c$ ενώ δεν θα υπάρχει κανένα μη-χρησιμοποιημένο ζεύγος $(a, b)$ για να μαρκάρει έστω και ένα από αυτά. Προφανώς, και εδώ το $VarProduct$ ορθά απαντάει "απόρριψη". □

Είναι εύκολο να παρατηρήσει κανείς ότι το συγκεκριμένο πρωτόκολλο έχει και ένα επιπρόσθετο χαρακτηριστικό: Σε κάθε υπολογισμό οι καταστάσεις του τελικά παύουν να μεταβάλονται.

**Ορισμός 19.** *Ένα πρωτόκολλο $\mathcal{A}$ λέγεται πρωτόκολλο με* ***σταθεροποιούμενες καταστάσεις****, εάν σε κάθε υπολογισμό το $\mathcal{A}$ φτάνει σε κάποιο πεπερασμένο βήμα $k$ σε μία διαμόρφωση $C_k$ τ.ώ. $C_t = C_k$, για κάθε $t \geq k$.*

Αξίζει να παρατηρήσουμε ότι οι σταθεροποιούμενες καταστάσεις είναι πιο ισχυρό χαρακτηριστικό απ' την απλή σταθεροποίηση αφού κάθε πρωτόκολλο με σταθεροποιούμενες καταστεις πάντοτε σταθεροποιείται (αφού παύουν να αλλάζουν οι καταστάσεις του σίγουρα παύουν να αλλάζουν και οι έξοδοί του).

Όπως έχουμε ήδη δει, ο κλασικός σταθερός υπολογισμός με την παραδοχή εξόδου κατηγορημάτων απαιτεί όλοι οι πράκτορες να συμφωνούν τελικά στην ορθή τιμή εξόδου. Όμως, το $VarProduct$ δεν φαίνεται να πληροί αυτή την προϋπόθεση ή με άλλα λόγια ακόμα δεν έχουμε δείξει ότι το $N_c = N_a \cdot N_b$

επιδέχεται δρομολογητή ισχυρά. Θα δείξουμε τώρα ότι με μία μικρή τροποποίηση η παραδοχή εξόδου κατηγορημάτων ικανοποιείται.

Ας παρατηρήσει ο αναγνώστης ότι η οδηγία $r$ ορίζει ένα ημιγραμμικό κατηγόρημα πάνω στα πολυσύνολα των καταστάσεων (στοιχεία του $Q$). Για να γίνει αυτό εμφανές, αρκεί να γράψουμε τυπικά την οδηγία $r$ ως $(N_c > 0) \vee (N_{\dot{a}} > 0)$. Το γεγονός ότι είναι ημιγραμμικό αρκεί για να γνωρίζουμε ότι υπάρχει ένα πρωτόκολλο πληθυσμού $\mathcal{B}'$ με σταθεροποιούμενες εισόδους από το σύνολο $Q$ των καταστάσεων του $VarProduct$ που το υπολογίζει σταθερά (λόγω του Πορίσματος 9). Επιπρόσθετα, το Πόρισμα 12 συνεπάγεται ότι υπάρχει ένα πρωτόκολλο με διαμεσολαβητή $\mathcal{B}$ με σταθεροποιούμενες εισόδους που είναι ισοδύναμο με το $\mathcal{B}'$ (αυτό που αγνοεί ό, τι αφορά στις ακμές και λειτουργεί ακριβώς όπως και το $\mathcal{B}'$), που, δηλαδή, υπολογίζει σταθερά και ισχυρά (με την παραδοχή εξόδου κατηγορημάτων) το κατηγόρημα που ορίζεται από την $r$. Επιπρόσθετα, το $VarProduct$ έχει σταθεροποιούμενες καταστάσεις, επομένως, η σύνθεσή του με το $\mathcal{B}$ (τα δύο πρωτόκολλα τρέχουν παράλληλα με ζεύγη καταστάσεων που θυμούνται τις καταστάσεις του κάθε πρωτοκόλλου) παρέχει σταθεροποιούμενες εισόδους στο $\mathcal{B}$. Εάν τώρα πάρουμε την απάντηση του απο κοινού πρωτοκόλλου από την έξοδο του $\mathcal{B}$, τότε είναι εύκολο να δείξουμε ότι η σύνθεση υπολογίζει σταθερά και ισχυρά το $N_c = N_a \cdot N_b$.

Θα διατυπώσουμε τώρα ένα θεώρημα σύνθεσης πρωτοκόλλων για να γενικεύσουμε αυτή την παρατήρηση. Το αξιοσημείωτο είναι ότι το θεώρημα αυτό ισχύει για οποιαδήποτε οικογένεια κατευθυνόμενων και συνεκτικών γράφων επικοινωνίας $\mathcal{G}$. Στο θεώρημα αυτό χρησιμοποιούμε το σύμβολο $\mathcal{C}$ για να υποδηλώσουμε ένα πρωτόκολλο και όχι για το σύνολο όλων των δυνατών διαμορφώσεων δικτύου.

**Θεώρημα 18.** *Κάθε πρωτόκολλο πληθυσμού με διαμεσολαβητή $\mathcal{A}$, που υπολογίζει σταθερά ένα κατηγόρημα $p$ με σταθεροποιούμενες καταστάσεις σε κάποια οικογένεια κατευθυνόμενων και συνεκτικών γράφων επικοινωνίας $\mathcal{G}$, και που περιέχει μία οδηγία $r$ που ορίζει ένα ημιγραμμικό κατηγόρημα $t$ πάνω στα πολυσύνολα των καταστάσεων πρακτόρων του $\mathcal{A}$, μπορεί να συντεθεί με ένα αποδεδειγμένα υπάρχον πρωτόκολλο πληθυσμού με διαμεσολαβητή $\mathcal{B}$, το οποίο υπολογίζει σταθερά και ισχυρά (δηλαδή, επιπλέον με την παραδοχή εξόδου κατηγορημάτων) το $t$ με σταθεροποιούμενες εισόδους στην $\mathcal{G}$, για να δώσει ένα νέο πρωτόκολλο πληθυσμού με διαμεσολαβητή $\mathcal{C}$ που ικανοποιεί τις ακόλουθες ιδιότητες:*

- *Το πρωτόκολλο $\mathcal{C}$ σχηματίζεται από τη σύνθεση των $\mathcal{A}$ και $\mathcal{B}$,*
- *η είσοδός του είναι η είσοδος του $\mathcal{A}$,*
- *η έξοδός του είναι η έξοδος του $\mathcal{B}$, και*

- *το $\mathcal{C}$ υπολογίζει σταθερά και ισχυρά το $p$ (δηλαδή, όλοι οι πράκτορες συμφωνούν τελικά στην ορθή έξοδο) στην $\mathcal{G}$.*

*Απόδειξη.* Το πρωτόκολλο $\mathcal{A}$ έχει σταθεροποιούμενες καταστάσεις και μία οδηγία $r$ που ορίζει ένα ημιγραμμικό κατηγόρημα $t$ πάνω στα πολυσύνολα των καταστάσεων πρακτόρων του $\mathcal{A}$. Έστω $X_{\mathcal{A}}$ το αλφάβητο εισόδου του $\mathcal{A}$, $Q_{\mathcal{A}}$ το σύνολο καταστάσεων του $\mathcal{A}$, $\delta_{\mathcal{A}}$ η συνάρτηση μετάβασης του $\mathcal{A}$ και ομοίως για κάθε άλλη συνιστώσα του $\mathcal{A}$. Θα χρησιμοποιούμε τους δείκτες $\mathcal{B}$ και $\mathcal{C}$ για τις αντίστοιχες συνιστώσες των άλλων δύο πρωτοκόλλων.

Αφού το κατηγόρημα $t$ είναι ημιγραμμικό, σύμφωνα με το Πόρισμα 9 υπαχει ένα πρωτόκολλο πληθυσμού $\mathcal{B}'$ που το υπολογίζει σταθερά με σταθεροποιούμενες εισόδους στην μη-περιορισμένη οικογένεια γράφων επικοινωνίας $\mathcal{G}^d_{Unr}$. Για κάθε οικογένεια κατευθυνόμενων και συνεκτικών γράφων $\mathcal{G}$ ισχύει $\mathcal{G} \subseteq \mathcal{G}^d_{Unr}$, και ως εκ τούτου κάθε κατηγόρημα που είναι σταθερά υπολογίσιμο (με ή χωρίς σταθεροποιούμενες εισόδους) στην $\mathcal{G}^d_{Unr}$ θα είναι επίσης και στην $\mathcal{G}$, αφού είναι σταθερά υπολογίσιμο σε κάθε πιθανό γράφο επικοινωνίας. Έτσι, το $\mathcal{B}'$ υπολογίζει σταθερά το $t$ με σταθεροποιούμενες εισόδους στην $\mathcal{G}$. Επιπρόσθετα, σύμφωνα με το Πόρισμα 12, υπάρχει επίσης και ένα πρωτόκολλο πληθυσμού με διαμεσολαβητή $\mathcal{B}$ (αυτό που κάνει τα ίδια με το $\mathcal{B}'$ και απλώς αγνοεί τις επιπρόσθετες συνιστώσες του νέου μοντέλου) που υπολογίζει σταθερά και ισχυρά το $t$ με σταθεροποιούμενες εισόδους στην $\mathcal{G}$. Το αλφάβητο εισόδου του $\mathcal{B}$ είναι $X_{\mathcal{B}}$ και η συνάρτηση μετάβασης είναι της μορφής $\delta_{\mathcal{B}} : (Q_{\mathcal{A}} \times Q_{\mathcal{B}}) \times (Q_{\mathcal{A}} \times Q_{\mathcal{B}}) \to Q_{\mathcal{B}} \times Q_{\mathcal{B}}$, αφού δεν υπάρχει λόγος να καθορίσουμε καταστάσεις ακμών (τυπικά θα έπρεπε, αλλά το πρωτόκολλο ούτως ή άλλως τις αγνοεί). Το $Q_{\mathcal{A}}$ είναι το σύνολο των καταστάσεων πρακτόρων του $\mathcal{A}$ και ταυτόχρονα οι είσοδοι του $\mathcal{B}$ που τελικά σταθεροποιούνται.

Ορίζουμε ένα πρωτόκολλο πληθυσμού με διαμεσολαβητή $\mathcal{C}$ ως εξής: $X_{\mathcal{C}} = X_{\mathcal{A}}$, $Y_{\mathcal{C}} = Y_{\mathcal{B}} = \{0, 1\}$, $Q_{\mathcal{C}} = Q_{\mathcal{A}} \times Q_{\mathcal{B}}$, $I_{\mathcal{C}} : X_{\mathcal{A}} \to Q_{\mathcal{C}}$ που ορίζεται ως $I_{\mathcal{C}}(x) = (I_{\mathcal{A}}(x), i_{\mathcal{B}})$, για κάθε $x \in Q_{\mathcal{C}}$, όπου $i_{\mathcal{B}} \in Q_{\mathcal{B}}$ είναι η αρχική κατάσταση του πρωτοκόλλου $\mathcal{B}$, $S_{\mathcal{C}} = S_{\mathcal{A}}$, $\iota_{\mathcal{C}} : X_C \to S_{\mathcal{C}}$, δηλαδή, $\iota_{\mathcal{C}}(x) = \iota_{\mathcal{A}}(x)$, για κάθε $x \in X_{\mathcal{C}}$, $O_{\mathcal{C}}(a, b) = O_{\mathcal{B}}(b)$, για κάθε $q = (a, b) \in Q_{\mathcal{C}}$, και τέλος η συνάρτηση μετάβασής του $\delta_{\mathcal{C}} : Q_{\mathcal{C}} \times Q_{\mathcal{C}} \times S_{\mathcal{C}} \to Q_{\mathcal{C}} \times Q_{\mathcal{C}} \times S_{\mathcal{C}}$ (φυσικά δεν συμπεριλαμβάνουμε κόστη, αφού δεν μας χρειάζονται καθόλου σε αυτή την περίπτωση) ορίζεται ως

$$\begin{aligned}\delta_{\mathcal{C}}((a, b), (a', b'), s) = ((&\delta_{\mathcal{A}_1}(a, a', s), \delta_{\mathcal{B}_1}((a, b), (a', b'))),\\ &(\delta_{\mathcal{A}_2}(a, a', s), \delta_{\mathcal{B}_2}((a, b), (a', b'))),\\ &\delta_{\mathcal{A}_3}(a, a', s)),\end{aligned}$$

όπου για $\delta_{\mathcal{A}}(x, y, z) = (x', y', z')$ (στην συνάρτηση μετάβασης του $\mathcal{A}$), έχουμε ότι $\delta_{\mathcal{A}_1}(x, y, z) = x'$, $\delta_{\mathcal{A}_2}(x, y, z) = y'$, $\delta_{\mathcal{A}_3}(x, y, z) = z'$, και ομοίως για την $\delta_{\mathcal{B}}$.

Διαισθητικά, το $\mathcal{C}$ αποτελείται από τα $\mathcal{A}$ και $\mathcal{B}$ που τρέχουν παράλληλα. Η κατάσταση κάθε πράκτορα είναι ένα ζεύγος $c = (a, b)$, όπου $a \in Q_{\mathcal{A}}$, $b \in Q_{\mathcal{B}}$ και η κατάσταση κάθε ακμής είναι στοιχείο του $S_{\mathcal{A}}$. Αρχικά, κάθε πράκτορας αισθάνεται (διαβάζει) μία είσοδο $x$ απ' το $X_{\mathcal{A}}$ η οποία μετατρέπεται μέσω της $I_{\mathcal{C}}$ σε ένα τέτοιο ζεύγος, όπου $a = I_{\mathcal{A}}(x)$ και $b$ είναι πάντοτε μία ειδική αρχική κατάσταση του $\mathcal{B}$, $i_{\mathcal{B}} \in Q_{\mathcal{B}}$. Όταν δύο πράκτορες με καταστάσεις $(a, b)$ και $(a', b')$ αλληλεπιδρούν μέσω μίας ακμής στην κατάσταση $s$, τότε το πρωτόκολλο $\mathcal{A}$ ανανεώνει τις πρώτες συνιστώσες των καταστάσεων των πρακτόρων, δηλαδή, τις $a$ και $a'$, και την κατάσταση $s$ της ακμής, σα να μην υπήρχε το πρωτόκολλο $\mathcal{B}$. Από την άλλη μεριά, το $\mathcal{B}$ ανανεώνει τις δεύτερες συνιστώσες λαμβάνοντας υπ' όψιν του τις πρώτε συνιστώσες σαν αυτές να παίζουν το ρόλο των ξεχωριστών θυρών εισόδου στις οποίες το τρέχον σύμβολο εισόδου κάθε πράκτορα είναι διαθέσιμο σε κάθε αλληλεπίδραση (το $\mathcal{B}$ θεωρεί τις καταστάσεις του $\mathcal{A}$ ως σύμβολα εισόδου που μπορούν να μεταβάλλονται αυθαίρετα μεταξύ δύο διαδοχικών υπολογιστικών βημάτων, αλλά η αλήθεια εδώ είναι ότι μεταβάλλονται μόνο λόγω του υπολογισμού του $\mathcal{A}$). Αφού οι πρώτες συνιστώσες των καταστάσεων πρακτόρων του $\mathcal{C}$ τελικά σταθεροποιούνται, λόγω του ότι το $\mathcal{A}$ έχει σταθεροποιούμενες καταστάσεις, το πρωτόκολλο $\mathcal{B}$ αποκτά τελικά σταθερές εισόδους (παύουν να μεταβάλλονται). Έτσι, το $\mathcal{B}$ θα αρχίσει τότε να λειτουργεί ορθά και θα υπολογίσει σταθερά και ισχυρά το $t$ σα να είχε ξεκινήσει τον υπολογισμό με αμετάβλητη είσοδο την τελική διαμόρφωση του $\mathcal{A}$. Όμως, αφού το $t$ παρέχει την ορθή απάντηση για το $p$ εάν εφαρμοσθεί στην τελική (σταθερή) διαμόρφωση του $\mathcal{A}$, είναι προφανές ότι το $\mathcal{C}$ υπολογίζει σταθερά και ισχυρά το $p$ στην $\mathcal{G}$ και με αυτό ολοκληρώνεται η απόδειξη. □

**Ορισμός 20.** *Έστω **SEM** η κλάση των κατηγορημάτων που είναι σταθερά υπολογίσιμα, σύμφωνα με τον κλασικό ορισμό του σταθερού υπολογισμού, από το βασικό μουτέλο των πρωτοκόλλων πληθυσμών (δηλαδή, ακριβώς τα ημιγραμμικά κατηγορήματα), και έστω **MP** η κλάση των αριθμητικών κατηγορημάτων επιδέχονται διαμεσολαβητή ισχυρά στο βασικό MPP μουτέλο.*

Για τον ορισμό των αριθμητικών κατηγορημάτων ο αναγνώστης καλείται να ανατρέξει παρακάτω στον Ορισμό 23.

**Θεώρημα 19.** *Η **SEM** είναι γνήσιο υποσύνολο της **MP**.*

*Απόδειξη.* Το Πόρισμα 11 συνεπάγεται ότι $SEM \subseteq MP$. Το Θεώρημα 17 δείχνει ότι υπάρχει ένα μη-ημιγραμμικό κατηγόρημα, $p : N_c = N_a \cdot N_b$, το οποίο φυσικά γνωρίζουμε ότι δεν ανήκει στην $SEM$, αλλά είναι υπολογίζεται σταθερά από το βασικό MPP μοντέλο (σύμφωνα με τον ορισμό του σταθερού υπολογισμού του νέου μοντέλου). Το πρωτόκολλο με διαμεσολαβητή $VarProduct$ που υπολογίζει σταθερά το $p$ περιέχει μία οδηγία εξόδου

$r$ που ορίζει ένα ημιγραμμικό κατηγόρημα πάνω στα πολυσύνολα των καταστάσεων του $VarProduct$. Συνεπώς, το Θεώρημα 18 μπορεί να εφαρμοσθεί και τελικά το $p$ επιδέχεται διαμεσολαβητή ισχυρά (δηλαδή, όλοι οι πράκτορες συμφωνούν τελικά στην σωστή έξοδο, σύμφωνα με την παραδοχή εξόδου κατηγορημάτων) στο βασικό MPP μοντέλο, με άλλα λόγια το $p$ ανήκει στην $MP$. □

Το Θεώρημα 19 αποδεικνύει, προφανώς, αυτό που είπαμε στην αρχή της παρούσας ενότητας, ότι δηλαδή το μοντέλο των πρωτοκόλλων πληθυσμών με διαμεσολαβητή είναι υπολογιστικά ισχυρότερο από το μοντέλο των πρωτοκόλλων πληθυσμών. Επίτηδες επιλέξαμε να περιορίσουμε και τα δύο μοντέλα σε πλήρεις γράφους επικοινωνίας, γιατί πρώτα απ' όλα για τους γράφους αυτούς είναι που γνωρίζουμε το αποτέλεσμα σχετικά με την κλάση που υπολογίζει το μοντέλο των πρωτοκόλλων πληθυσμών (ημιγραμμικά κατηγορήματα) και κατά δεύτερον έπρεπε να προσέξουμε να μην δώσουμε στο ένα μοντέλο περισσότερη ισχύ από το άλλο μέσω διαφορετικού γράφου επικοινωνίας (γνωρίζουμε π.χ. ότι ένας κατευθυνόμενος γραμμικός γράφος, που αποτελείται, δηλαδή, από ένα μόνο κατευθυνόμενο μονοπάτι, μπορεί να προσομοιώσει μία μηχανή Turing γραμμικού χώρου). Τέλος, πέραν από αυτό το απλό παράδειγμα (το κατηγόρημα $N_c = N_a \cdot N_b$) που χρησιμοποιήσαμε διότι βοηθούσε πολύ στο να αποδείξουμε τα λεγόμενά μας, φαίνεται ότι υπάρχουν πολλά ακόμα νέα πράγματα που προσφέρει το MPP μοντέλο. Για παράδειγμα, το μοντέλο των πρωτοκόλλων πληθυσμών δεν έχει τη δυνατότητα να βρίσκει υπογράφους και εμείς ήδη παρουσιάσαμε ορισμένα πρωτόκολλα με διαμεσολαβητή που το κάνουν με επιτυχία.

### 5.3.2 Μη-ομοιόμορφα Άνω Φράγματα Υπολογισιμότητας

**Ορισμός 21.** *Έστω **UMP** η κλάση των κατηγορημάτων που επιδέχονται διαμεσολαβητή σε οποιαδήποτε οικογένεια $\mathcal{G}$ μη-κατευθυνόμενων συνεκτικών γράφων επικοινωνίας και **DMP** η κλάση των κατηγορημάτων που επιδέχονται διαμεσολαβητή σε οποιαδήποτε οικογένεια $\mathcal{G}'$ κατευθυνόμενων συνεκτικών γράφων επικοινωνίας*

Έστω $m$ το πλήθος των ακμών οποιουδήποτε γράφου επικοινωνίας $G$.

**Θεώρημα 20.** *Κάθε κατηγόρημα που ανήκει είτε στην $DMP$ είτε στην $UMP$ ανήκει επίσης και στην κλάση $NSPACE(m)$.*

*Απόδειξη.* Έστω $\mathcal{A}$ ένα πρωτόκολλο με διαμεσολαβητή που υπολογίζει σταθερά ένα τέτοιο κατηγόρημα $p$ σε κάποια οικογένεια γράφων επικοινωνίας $\mathcal{G}$, και έστω $G \in \mathcal{G}$ οποιοσδήποτε γράφος αυτής της οικογένειας. Αφού ο $G$

είναι πάντοτε συνεκτικός, έχουμε ότι $m \geq n-1$ (απαιτούνται τουλάχιστον $n-1$ ακμές για να συνδέσουν $n$ κόμβους). Μία διαμόρφωση δικτύου μπορεί να αναπαρασταθεί αποθηκεύοντας μία κατάσταση για κάθε κόμβο και μία κατάσταση για κάθε ακμή του $G$. Αυτό χρειάζεται $\mathcal{O}(m)$ χώρο (στην πραγματικότητα είναι $m+n$, αλλά αφού $m \geq n-1$, το $m$ υπερισχύει). Γνωρίζουμε φυσικά ότι κάθε κατηγόρημα $p$ αντιστοιχεί σε μία γλώσσα $L$, όπου τα στοιχεία της γλώσσας είναι το στήριγμα του κατηγορήματος, δηλαδή, τα στοιχεία του πεδίου ορισμού τα οποία το κατηγόρημα αντιστοιχίζει στην τιμή 1. Άρα, χ.β.τ.γ. μπορούμε να πούμε ότι το $\mathcal{A}$ υπολογίζει σταθερά τη γλώσσα $L$ που αντιστοιχεί στο κατηγόρημα $p$.

Θα παρουσιάσουμε τώρα μία ανταιτιοκρατική (μη-ντετερμινιστική) μηχανή Turing $M_{\mathcal{A}}$ που διαγιγνώσκει την $L$ σε χώρο $\mathcal{O}(m)$. Η $M_{\mathcal{A}}$ λειτουργεί ως εξής: Για να αποδεχθεί κάποια ανάθεση εισόδου $x$, η $M_{\mathcal{A}}$ πρέπει να επαληθεύσει δύο συνθήκες:

1. Ότι υπάρχει κάποια διαμόρφωση $C$ που είναι προσβάσιμη από την $I(x)$ (όπου $I(x)$ αρχική διαμόρφωση που αντιστοιχεί στην ανάθεση εισόδου $x$), στην οποία όλες οι σχετικές καταστάσεις ικανοποιούν την οδηγία εξόδου $r$, και

2. ότι δεν υπάρχει διαμόρφωση $C'$ προσβάσιμη απ' την $C$, στην οποία η $r$ να παραβιάζεται.

Η πρώτη συνθήκη επαληθεύεται μαντεύοντας και ελέγχοντας μία ακολουθία διαμορφώσεων δικτύου, ξεκινώντας από την $I(x)$ και φτάνοντας σε μία τέτοια $C$. Η $M_{\mathcal{A}}$ μαντεύει κάποια $C_{i+1}$ κάθε φορά, επαληθεύει ότι $C_i \rightarrow C_{i+1}$ (ξεκινάει από την $C_0 = I(x)$, δηλαδή, για $i = 0$) και, εάν αυτό ισχύει, αντικαθιστά την $C_i$ με την $C_{i+1}$, αλλιώς "πετάει" αυτήν την $C_{i+1}$. Η δεύτερη συνθήκη είναι το συμπλήρωμα ενός παρόμοιου προβλήματος προσβασιμότητας. Αλλά η κλάση $NSPACE$ είναι κλειστή ως προς το συμπλήρωμα, όπως αποδείχθηκε από τον Immerman στο [15], για όλες τις χωρικές συναρτήσεις $\geq \log n$. Επομένως, η $M_{\mathcal{A}}$ διαγιγνώσκει την $L$ σε χώρο $\mathcal{O}(m)$. □

Αξίζει να παρατηρήσουμε ότι σε ό, τι αφορά στην $DMP$ ακόμα και ένα πρωτόκολλο πληθυσμού, όπως είδαμε και στην προηγούμενη ενότητα, του οποίου ο $G$ είναι μία κατευθυνόμενη γραμμή, μπορεί να προσομοιώσει μία αιτιοκρατική (ντετερμινιστική) μηχανή Turing γραμμικού χώρου [3]. Επομένως, αν λάβουμε υπ' όψιν το θεώρημα του Savitch [20], που διατυπώνει ότι $NSPACE(f(n)) \subseteq SPACE(f^2(n))$, μπορούμε άτυπα να πούμε ότι η $DMP$ βρίσκεται μεταξύ των κλάσεων $NSPACE(\sqrt{n})$ και $NSPACE(m)$. Ωστόσο, για την $UMP$ γνωρίζουμε μόνον ότι $SEM \subset UMP \subseteq NSPACE(m)$.

### 5.3.3 Προσομοιώνοντας το Πιθανοτικό MPP

**Ορισμός 22.** *Ένα **πιθανοτικό MPP** (είτε σε κατευθυνόμενο είτε σε μη-κατευθυνόμενο $G$) είναι ένα πρωτόκολλο πληθυσμού με διαμεσολαβητή του οποίου ο (δίκαιος) δρομολογητής επιλέγει κάθε φορά ισοπίθανα κάποια απ' τις ακμές του $G$ (ομοιόμορφη κατανομή) και ευ συνεχεία εφαρμόζει τον αντίστοιχο κανόνα μετάβασης.*

Έστω, $x_q$ το πλήθος των πρακτόρων στην κατάσταση $q$ κατά την διαμόρφωση $C$. Έστω $e_{ijt}$ το πλήθος των ακμών του $G$ που συνδέουν έναν πράκτορα στην κατάσταση $i$ με έναν πράκτορα στην κατάσταση $j$ και οι ίδιες είναι στην κατάσταση ακμής $t$.

**Ορισμός 23.** *Ένα Peano κατηγόρημα πάνω στο $\{x_q, e_{ijt}\}$, όπου $i, j, q \in Q$ και $t \in S$, είναι ένα κατηγόρημα στην Peano αριθμητική πάνω στους αριθμούς $\{x_q, e_{ijt}\}$. Καλούμε τα κατηγορήματα αυτά με το όνομα αριθμητικά κατηγορήματα.*

Έστω τώρα ένα πιθανοτικό MPP $\mathcal{A}$ που διαγιγνώσκει ένα αριθμητικό κατηγόρημα (δηλαδή, τη γλώσσα που του αντιστοιχεί) με πιθανότητα $1/2 + \epsilon$, όπου $\epsilon > 0$. Ένα τέτοιο πιθανοτικό MPP επάγει μία Μαρκοβιανή αλυσίδα $\mathcal{M}$ με μόνο πολυωνυμικό πλήθος καταστάσεων ως προς το $n$, ως εξής:

1. Οι καταστάσεις της αλυσίδας είναι οι αριθμοί ($x_q$), $q \in Q$ και ($e_{ijt}$), $i, j \in Q$, $t \in S$ για μία διαμόρφωση $C$. Αφού $x_1 + \ldots + x_{|Q|} = n$, και $e_{ijt} \leq x_i \cdot x_j$, και $\sum_{i,j,t} e_{ijt} = m$, έχουμε το πολύ $n^{|Q|} \cdot m^{|S|}$ τέτοιες καταστάσεις, δηλαδή, έναν πολυωνυμικό (ως προς το $n$) αριθμό, $\lambda$, καταστάσεων.

2. Έστω $a$, $b$ δύο καταστάσεις της αλυσίδας όπως προηγουμένως. Μπορούμε εύκολα να υπολογίσουμε την πιθανότητα μετάβασης $p_{ab}$, λόγω της ανωνυμίας του $MPP$ και λόγω του ότι ο δρομολογητής επιλέγει ισοπίθανα μεταξύ των ακμών. Για τον κανόνα (μετάβαση) $r$ : $(q_1, q_2, s) \to (q_1', q_2', s')$ έχουμε $x_q(b) = x_q(a) - lhs_r(q) + rhs_r(q)$, για κάθε $q \in \{q_1, q_2, q_1', q_2'\}$, όπου το $lhs_r(q)$ ($rhs_r(q)$) συμβολίζει το πλήθος των εμφανίσεων του $q$ στο αριστερό (δεξί) σκέλος του κανόνα $r$ (χωρίς να συμπεριλαμβάνεται η πιθανότητα να ισχύει $s = q$), και εάν $q_1 = q_1'$, $q_2 = q_2'$, $s = s'$, τότε $e_{q_1', q_2', s'}(b) = e_{q_1', q_2', s'}(a)$, αλλιώς $e_{q_1', q_2', s'}(b) = e_{q_1', q_2', s'}(a) + 1$, και $e_{q_1, q_2, s}(b) = e_{q_1, q_2, s}(a) - 1$. Η πιθανότητα μετάβασης από την κατάσταση $a$ στην κατάσταση $b$ είναι απλώς $e_{q_1, q_2, s}(a)/m$. Δηλαδή, όλες οι $p_{ab}$ μπορούν να υπολογισθούν σε πολυωνυμικό χρόνο.

Έστω τώρα $\mathbb{P} = \{p_{ab}\}$ το μητρώο μεταβάσεων της Μαρκοβιανής αλυσίδας. Παρουσιάζουμε μία αιτιοκρατική μηχανή Turing, $TM_{\mathcal{M},\mathcal{A}}$, που λειτουργεί

ως εξής: Η $TM_{\mathcal{M},\mathcal{A}}$ επιλύει σε πολυωνυμικό χρόνο το σύστημα $\pi = \pi \cdot \mathbb{P}$ για το διάνυσμα γραμμής $\pi = [\pi_1 \dots \pi_\lambda]$ (ας παρατηρήσει ο αναγνώστης ότι $\sum_{i=1}^{\lambda} \pi = 1$), για να βρει την *ευσταθή κατανομή* $\pi$ της $\mathcal{M}$ εάν αυτή υπάρχει. Εάν μία τέτοια $\pi$ δεν υπάρχει, η $TM_{\mathcal{M},\mathcal{A}}$ απορρίπτει. Διαφορετικά, η $TM_{\mathcal{M},\mathcal{A}}$ μπορεί να προσδιορίσει το σύνολο, $L$, όλων των καταστάσεων της $\mathcal{M}$ που ικανοποιούν το αριθμητικό κατηγόρημα, και να υπολογίσει (αθροίζοντας) την αθροιστική πιθανότητά τους $\sum_{a \in L} \pi_a$. Εάν $\sum_{a \in L} \pi_a \geq 1/2 + \epsilon$, τότε η $TM_{\mathcal{M},\mathcal{A}}$ αποδέχεται, διαφορετικά, απορρίπτει. Επομένως, έχουμε μόλις αποδείξει το ακόλουθο θεώρημα:

**Θεώρημα 21.** *Το σύνολο των αριθμητικών κατηγορημάτων που είναι διαγνώσιμα από ένα πιθανοτικό πρωτόκολλο πληθυσμού με διαμεσολαβητή με πιθανότητα τουλάχιστον* $1/2 + \epsilon$*, όπου* $\epsilon > 0$*, ανήκουν στην κλάση* $P$ *(αιτιοκρατικός πολυωνυμικός χρόνος).*

# Βιβλιογραφία


[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: a Survey. In the *Journal of Computer Networks*, 38, 393-422, 2002.

[2] D. Angluin, J. Aspnes, M. Chan, M. J. Fischer, H. Jiang, and R. Peralta. Stably computable properties of network graphs. In Proc. Distributed Computing in Sensor Systems: 1st IEEE International Conference, pages 63-74, 2005.

[3] D. Angluin, J. Aspnes, Z. Diamadi, M.J. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. In *23rd Annual ACM Sympsium on Principles of Distributed Computing* (*PODC*), pages 290-299, New York, NY, USA, 2004. ACM.

[4] D. Angluin, J. Aspnes, Z. Diamadi, M.J. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. *Distributed Computing*, 18(4): 235-253, 2006.

[5] D. Angluin, J. Aspnes, and D. Eisenstat. Fast computation by population protocols with a leader. *Distributed Computing*, 21(3): 183-199, Sept. 2008.

[6] D. Angluin, J. Aspnes, and D. Eisenstat. Stably computable predicates are semilinear. In *Proc. 25th Annual ACM Symposium on Principles of Distributed Computing*, pages 292-299, 2006.

[7] D. Angluin, J. Aspnes, D. Eisenstat, and E. Ruppert. The computational power of population protocols. *Distributed Computing*, 20(4): 279-304, November 2007.

[8] D. Anlguin, L. G. Valiant. Fast probabilistic algorithms for Hamiltonian circuits and matchings. *Journal of Computer and Systems Sciences*, 18, 1979, pages 155-193.

[9] J. Aspnes and E. Ruppert. An introduction to population protocols. *Bulletin of the European Association for Theoretical Computer Science*, 93:98-117, October 2007. Columns: *Distributed Computing*, Editor: M. Mavronicolas.

[10] J. Beauquier, J. Clement, S. Messika, L. Rosaz, and B. Rozoy. Self-stabilizing counting in mobile sensor networks. Technical Report 1470, LRI, Université Paris-Sud 11, 2007.

[11] I. Chatzigiannakis, O. Michail, and P. G. Spirakis. Experimental Verification and Performance Study of Extremely Large Sized Population Protocols. FRONTS Technical Report FRONTS-TR-2009-3, http://fronts.cti.gr/aigaion/?TR=61, Jan. 2009.

[12] Z. Diamandi and M. J. Fishcer. A simple game for the study of trust in distributed systems. *Wuhan University Journal of Natural Sciences*, 6(1-2):72-82, Mar. 2001. Also appears as Yale Technical Report TR-1207, Jan. 2001.

[13] S. Ginsburg and E. H. Spanier. Semigroups, Presburger formulas, and languages. *Pacific Journal of Mathematics*, 16, 285-296, 1966.

[14] R. Guerraoui and E. Ruppert. Even small birds are unique: Population protocols with identifiers. Technical Report CSE-2007-04, Department of Computer Science and Engineering, York University, 2007.

[15] N. Immerman. Nondeterministic space is closed under complementation. *SIAM J. Comput*, 17(5):935-938, Oct. 1988 (see also page 153 C. H. Papadimitriou "Computational Complexity").

[16] H. Karl and A. Willig. *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, Ltd, 2005.

[17] M. Kracht. The Mathematics of Language. *Studies in Generative Grammar*, vol. 63, Mouton de Gruyter, 2003, ISBN 3-11-017620-3.

[18] S. Lang. *Algebra (Revised Third Edition)*. Springer-Verlang, 2002.

[19] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes-Rendus du I Congrès de Mathématiciens des Pays Slaves*, pages 92-101, Warszawa, 1929.

[20] W. J. Savitch. Relationship between nondeterministic and deterministic tape classes. *J.CSS*, 4, pages 177-192, 1970 (see also page 149-150 C. H. Papadimitriou "Computational Complexity").

[21] V. Vazirani. *Approximation Algorithms*. Springer-Verlag, 2001.