Διάλεξη 18: Πρόβλημα Βυζαντινών Στρατηγών

ΕΠΛ 432: Κατανεμημένοι Αλγόριθμοι

Τι θα δούμε σήμερα

- Ορισμός Προβλήματος
- Συνθήκες Συμφωνίας κάτω από Βυζαντινό Στρατηγό
- Πιθανοτικοί αλγόριθμοι επίλυσης Βυζαντινής Συμφωνίας
- Πιθανοτικός Αλγόριθμος όταν $n = 3, f=1$

Πρόβλημα Βυζαντινών Στρατηγών

- Μόνο ένας επεξεργαστής έχει είσοδο – **ο Στρατηγός**
- Όλοι οι επεξεργαστές γνωρίζουν τον στρατηγό
- Υπάρχουν το πολύ *f* επεξεργαστές που μπορεί να είναι Βυζαντινοί
  - Ανάμεσά τους μπορεί να είναι και ο Στρατηγός
  - Οι επεξεργαστές δεν γνωρίζουν αν ο στρατηγός είναι βυζαντινός ή όχι

Πρόβλημα Βυζαντινών Στρατηγών

- Ένας αλγόριθμος επιλύει το πρόβλημα της Συμφωνίας Βυζαντινών Στρατηγών αν ισχύουν:
  - ***Συνθήκη Τερματισμού***: Κάθε μη βυζαντινός επεξεργαστής πρέπει να αποφασίσει μια τιμή (ίδια με το πρόβλημα συμφωνίας)
    - Η απόφαση είναι μη αντιστρέψιμη
  - ***Συνθήκη Συμφωνίας***: Όλοι οι μη βυζαντινοί επεξεργαστές αποφασίζουν την ίδια τιμή (ίδια με το πρόβλημα συμφωνίας)
  - ***Συνθήκη Εγκυρότητας***: Αν ο Στρατηγός είναι μη βυζαντινός τότε η κοινή απόφαση πρέπει να αποτελεί την είσοδο του στρατηγού.
    - Αν ο στρατηγός είναι βυζαντινός τότε η συνθήκη αυτή ισχύει τετριμμένα

Ανασκόπηση Αποτελεσμάτων

- Σύγχρονο Μοντέλο
- Το πολύ f επεξεργαστές μπορούν να είναι εσφαλμένοι
- Στενά κάτω φράγματα για το μοντέλο ανταλλαγής μηνυμάτων

	Σφάλματα Κατάρρευσης	**Βυζαντινά Σφάλματα**
Αριθμός γύρων	$f + 1$	$f + 1$
Ολικός αριθμός επεξεργαστών	$f + 1$	$3f + 1$
Μέγεθος μηνυμάτων	Πολυωνυμικό	Πολυωνυμικό

Πιθανοτικοί Αλγόριθμοι

- Ένας αλγόριθμος είναι πιθανοτικός αν κάποια βήματα του αλγορίθμου εκτελούνται με κάποια μη μηδενική και μη μοναδιαία πιθανότητα
  - Τα βήματα δεν είναι ντετερμινιστικά (πιθανότητα 1)

- Μας επιτρέπουν να ικανοποιήσουμε συμφωνία μεταξύ των επεξεργαστών με κάποια πιθανότητα συμφωνίας
  - Χρήσιμοι όταν $n < 3f+1$
  - Όταν δεν μας πειράζει να εγγυηθούμε συμφωνία με κάποια μη μηδενική πιθανότητα

Πιθανότητα Συμφωνίας

- **Πιθανότητα Συμφωνίας Εκτέλεσης**:

$$P_A = \sum_{v \in V} P_\Sigma(v) = \sum_{v \in V} \prod_{G_i \in G} P_{G_i}(v)$$

  - V: Το σύνολο των τιμών που εξασφαλίζουν την Συνθήκη Εγκυρότητας
  - G: το σύνολο των επεξεργαστών
  - P_A: Πιθανότητα Συμφωνίας
  - P_Σ (v): Πιθανότητα Ισχύος Συνθήκης Συμφωνίας πάνω στην v
  - P_{Gi}(v): Πιθανότητα ο επεξεργαστής G_i να αποφασίσει v

- **Χειρότερη Εκτέλεση Αλγορίθμου**: Αυτή με την μικρότερη πιθανότητα συμφωνίας

- **Πιθανότητα Συμφωνίας Πιθανοτικού Αλγόριθμου**: είναι η πιθανότητα συμφωνίας της χειρότερης εκτέλεσης του αλγορίθμου.
  - Χρειάζεται απαρίθμηση όλων των εκτελέσεων

- Στόχος: Η μεγιστοποίηση της ελάχιστης πιθανότητας (πρόβλημα μεγιστοποίησης ελαχίστου)

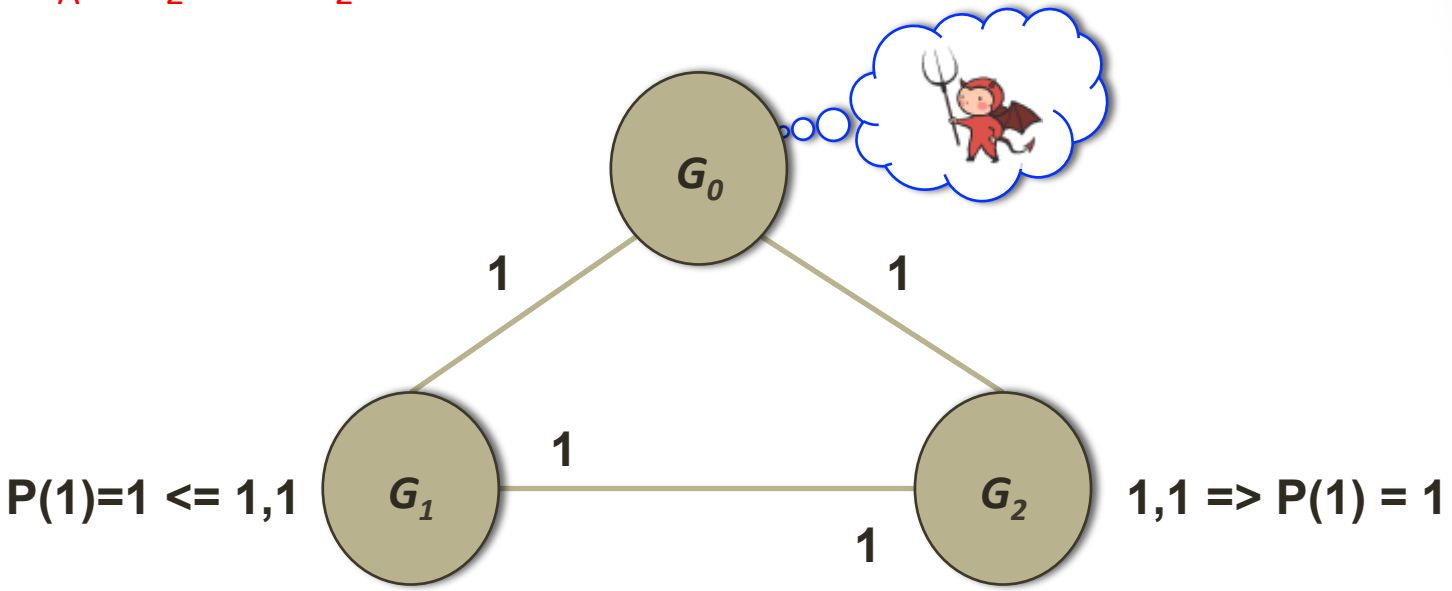
Αλγόριθμος 3 επεξεργαστών

- Έστω $n=3$ και $f=1$ και G_0 στρατηγός

- **Γύρος 1:**
  - Ο στρατηγός G_0 στέλνει την είσοδό του στους G_1 *και* G_2
- **Γύρος 2:**
  - Οι G_1 και G_2 διαβάζουν το μήνυμα του G_0
  - Ο G_1 στέλνει στον G_2 το μήνυμα που πήρε από τον G_0
  - Ο G_2 στέλνει στον G_1 το μήνυμα που πήρε από τον G_0
- **Γύρος 3:**
  - Αν ο G_1 λάβει το ίδιο μήνυμα από τους G_0 και G_2 τότε αποφασίζει αυτό το κοινό μήνυμα
  - Αλλιώς αποφασίζει 0 με πιθανότητα ½ και 1 με πιθανότητα ½
  - Όμοια για τον G_2

Ανάλυση Εκτελέσεων

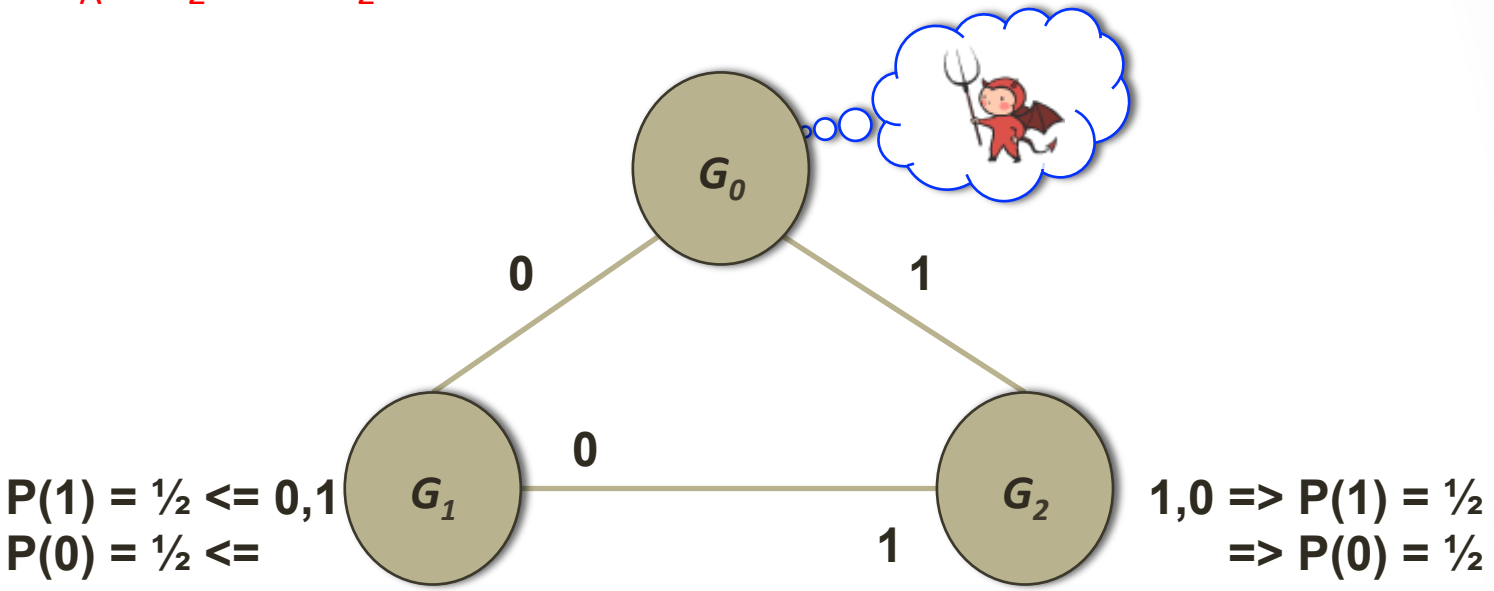
- Έστω G_0 βυζαντινός
  - $P_A = P_\Sigma(1) + P_\Sigma(0)$ (αφού η εγκυρότητα ισχύει τετριμμένα)



- $P_A = P_\Sigma(1) + 0 = 1$
  - Αφού οι μη εσφαλμένοι επεξεργαστές λαμβάνουν δύο 1
- Συμμετρικά η εκτέλεση όπου ο G_0 στέλνει δύο 0 έχει $P_A(0) = 1$

Ανάλυση Εκτελέσεων

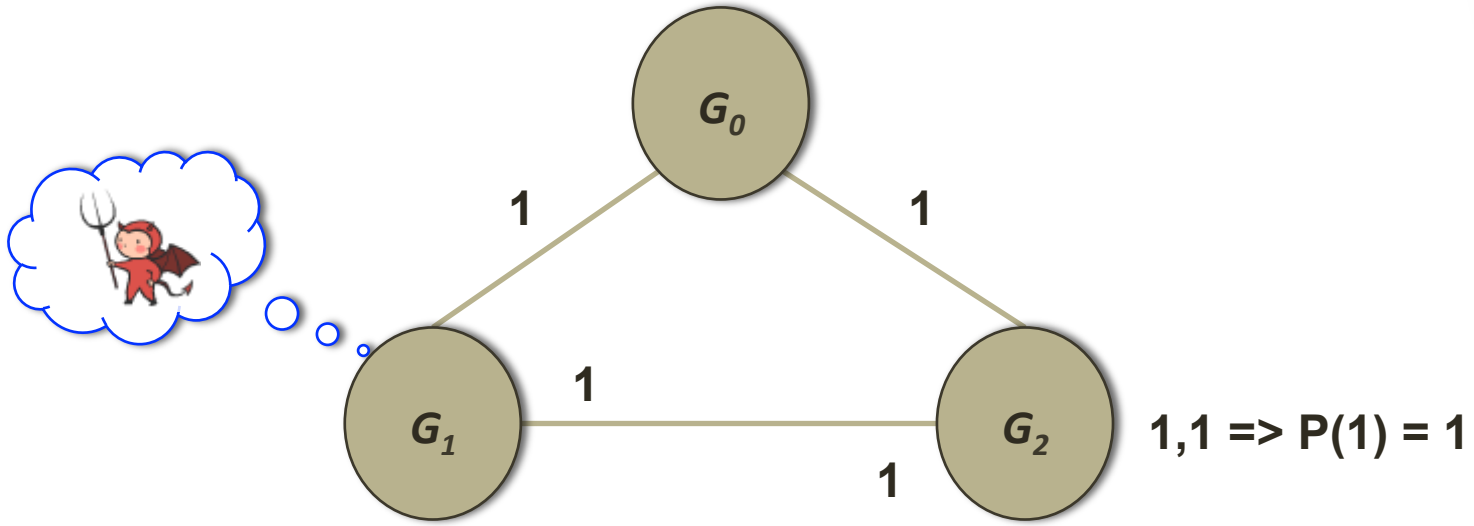
- Έστω G_0 βυζαντινός
  - $P_A = P_\Sigma(1) + P_\Sigma(0)$ (αφού η εγκυρότητα ισχύει τετριμμένα)



- $P_A = P_\Sigma(1) + P_\Sigma(0) = ¼ + ¼ = ½$
  - $P_\Sigma(1) = P_{G1}(1) \cdot P_{G2}(1) = ½ \cdot ½ = ¼$
  - $P_\Sigma(0) = P_{G1}(0) \cdot P_{G2}(0) = ½ \cdot ½ = ¼$

Ανάλυση Εκτελέσεων

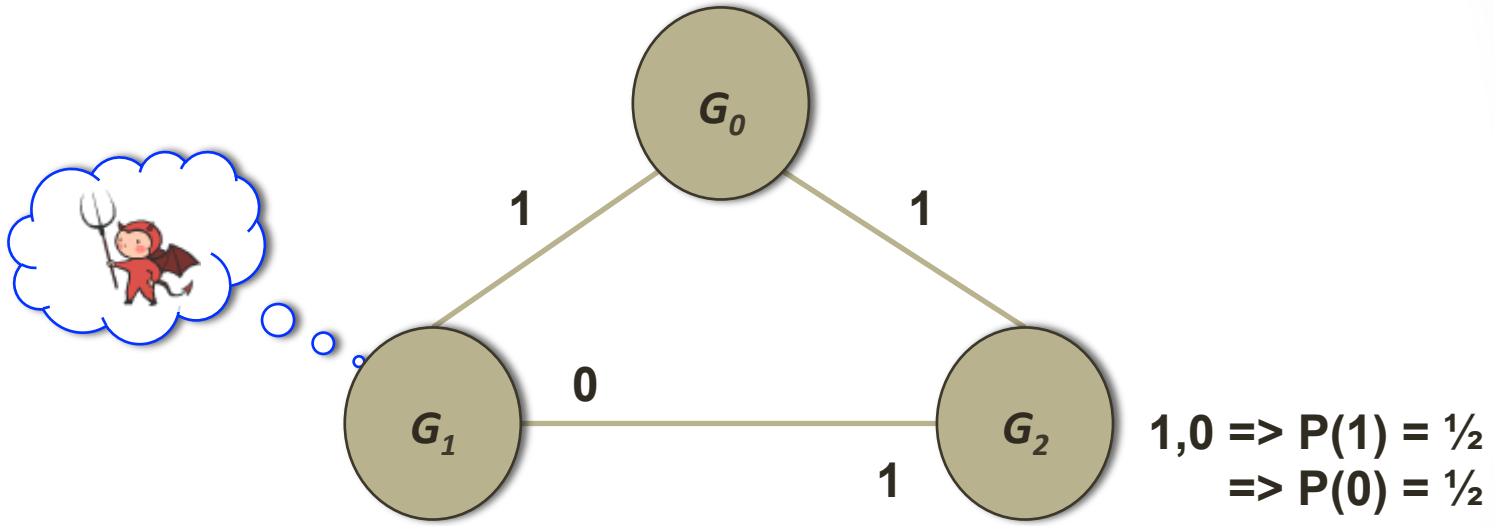
- Έστω G_1 βυζαντινός και είσοδος G_0 είναι 1
  - $P_A = P_\Sigma(1)$ (σύμφωνα με εγκυρότητα πρέπει να συμφωνήσουμε 1)



- $P_A(1) = P_\Sigma(1) = P_{G2}(1) = 1$
  - Αφού ο G_2 λαμβάνει δύο 1

Ανάλυση Εκτελέσεων

- Έστω G_1 βυζαντινός και είσοδος G_0 είναι 1
  - $P_A = P_\Sigma(1)$ (σύμφωνα με εγκυρότητα πρέπει να συμφωνήσουμε 1)



- $P_A = P_\Sigma(1) = P_{G2}(1) = ½$

- Συμμετρικά μπορούμε να υπολογίσουμε τις ίδιες πιθανότητες όταν ο G_2 είναι βυζαντινός

Πιθανότητα Συμφωνίας

- Στην χειρότερη περίπτωση ο αλγόριθμος έχει πιθανότητα συμφωνίας ίση με ½

- Επομένως:

  Πιθανότητα Συμφωνίας Αλγορίθμου = ½

- Πως μπορούμε να βελτιώσουμε την πιθανότητα αυτή;

- **Δημιουργία Ασυμμετρίας στο Πρωτόκολλο**

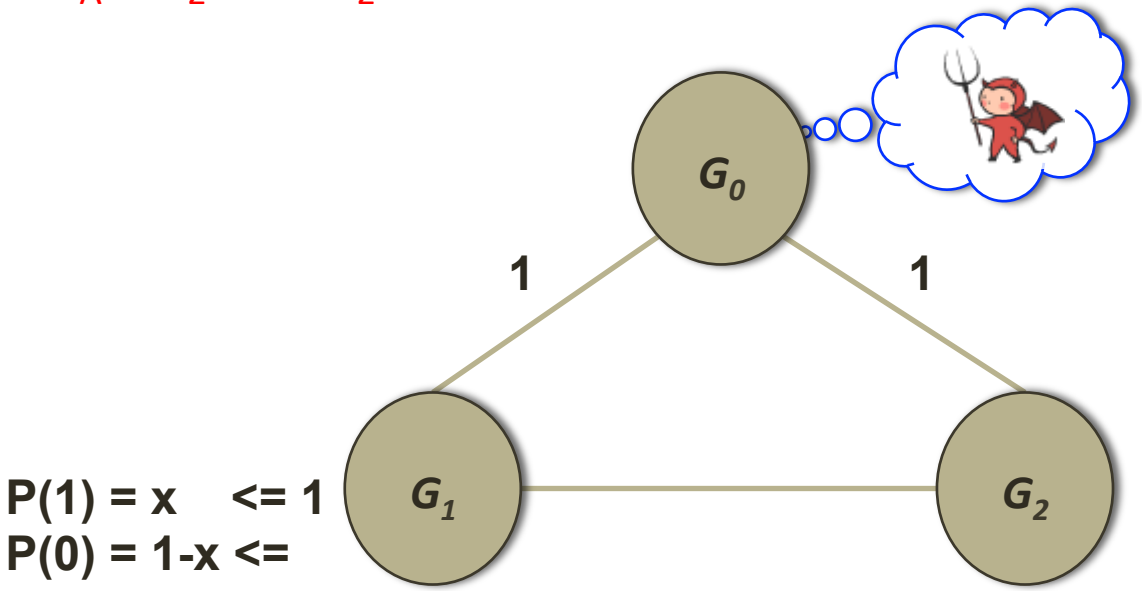
Βελτίωση Τριγωνικού Μοντέλου

- Έστω $n=3$ και $f=1$ και G_0 στρατηγός
  - Μη συμμετρικό προτόκολλο αφού οι G_1 *και* G_2 τρέχουν διαφορετικό αλγόριθμο.

- **Γύρος 1:**
  - Ο στρατηγός G_0 στέλνει την είσοδό του στους G_1 *και* G_2
- **Γύρος 2:**
  - Οι G_1 και G_2 διαβάζουν το μήνυμα του G_0
  - Αν ο G_1 πήρε τιμή ν από τον G_0 τότε αποφασίζει ν με πιθανότητα $P_{G1}(v) = x$ και $P_{G1}(1-v) = 1-x$
  - Ο G_1 στέλνει στον G_2 την απόφασή του
- **Γύρος 3:**
  - Αν ο G_2 λάβει το ίδιο μήνυμα από τους G_0 και G_1 τότε αποφασίζει αυτό το κοινό μήνυμα
  - Αλλιώς αποφασίζει εκείνο του G_0 με πιθανότητα $P_{G2}(G_0(v)) = y$ και εκείνο του G_1 με πιθανότητα $P_{G2}(G_1(v)) = 1- y$

Ανάλυση Εκτελέσεων

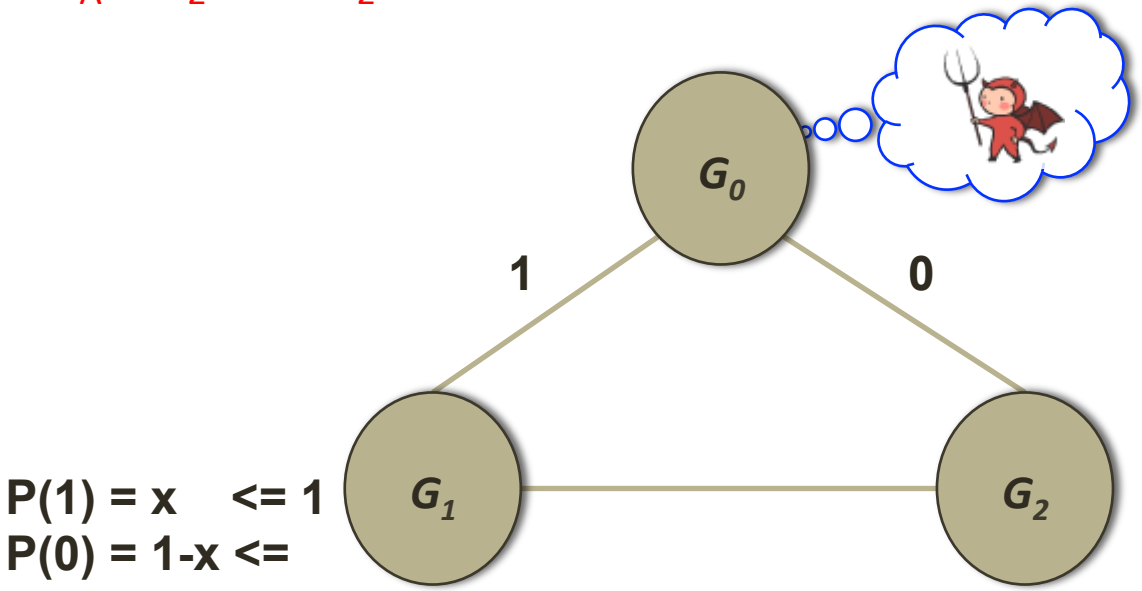
- Έστω G_0 βυζαντινός
  - $P_A = P_\Sigma(1) + P_\Sigma(0)$ (αφού η εγκυρότητα ισχύει τετριμμένα)



- $P_\Sigma(1) = P_{G_1}(1)P_{G_2}(1) = x.1$
- $P_\Sigma(0) = P_{G_1}(0)P_{G_2}(0) = (1-x)(1-y)$
- $P_A = P_\Sigma(1) + P_\Sigma(0) = 1.x + (1-x)(1-y) = \boxed{1-y-xy}$

Ανάλυση Εκτελέσεων

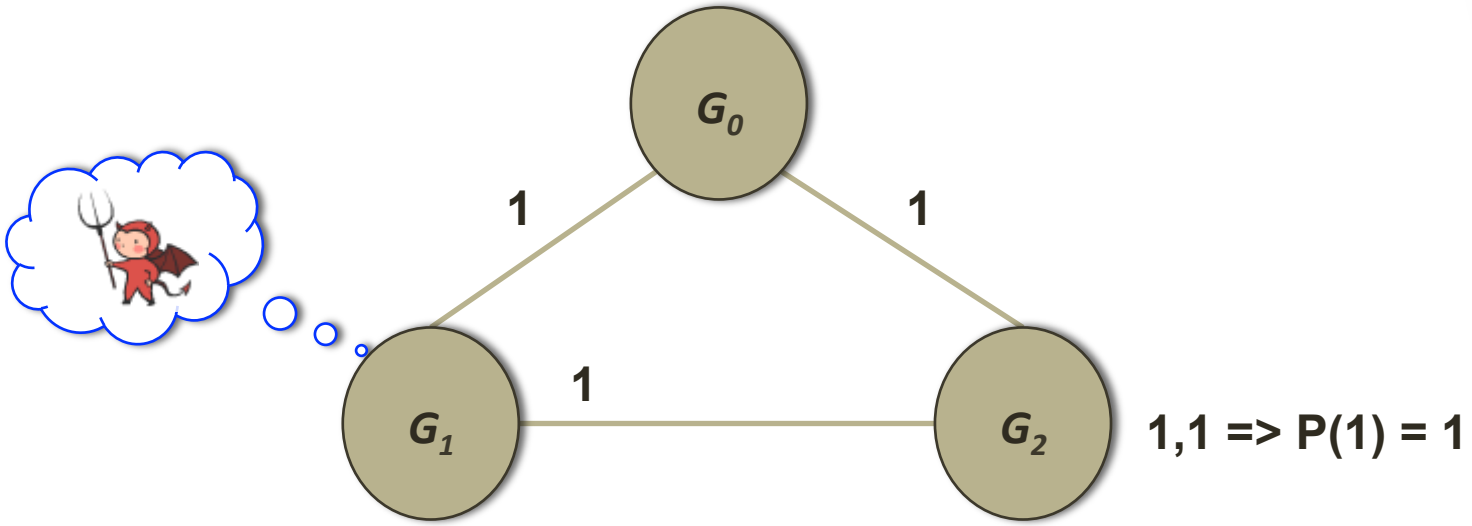
- Έστω G_0 βυζαντινός
  - $P_A = P_\Sigma(1) + P_\Sigma(0)$ (αφού η εγκυρότητα ισχύει τετριμμένα)



- $P_\Sigma(1) = P_{G_1}(1)P_{G_2}(1) = x(1-y)$
- $P_\Sigma(0) = P_{G_1}(0)P_{G_2}(0) = (1-x).1$
- $P_A = P_\Sigma(1) + P_\Sigma(0) = x - xy + 1 - x = \boxed{1-xy}$

Ανάλυση Εκτελέσεων

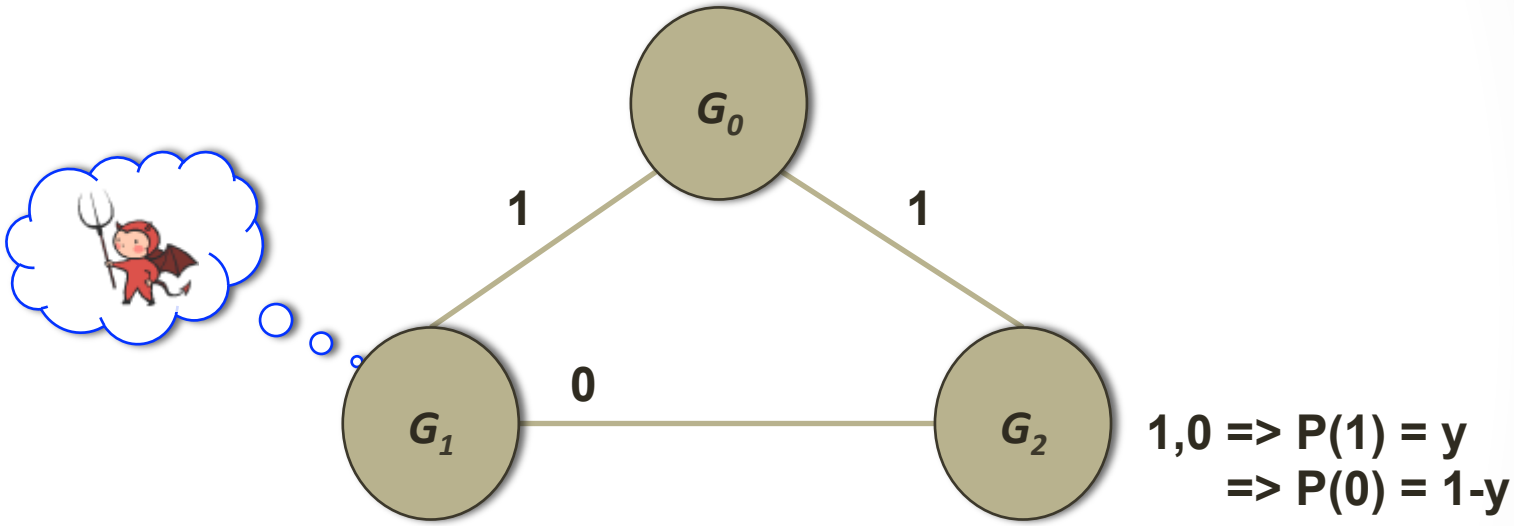
- Έστω G_1 βυζαντινός και είσοδος G_0 είναι 1
  - $P_A = P_\Sigma(1)$ (σύμφωνα με εγκυρότητα πρέπει να συμφωνήσουμε 1)



- $P_A(1) = P_\Sigma(1) = P_{G2}(1) = 1$
  - Αφού ο G_2 λαμβάνει δύο 1

Ανάλυση Εκτελέσεων

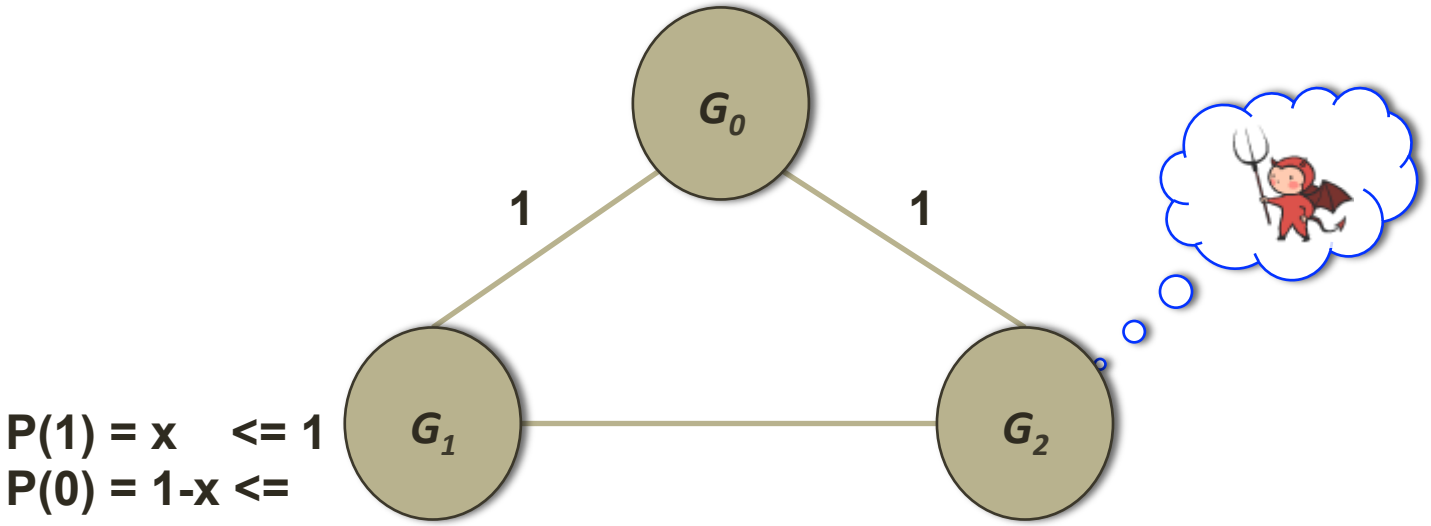
- Έστω G_1 βυζαντινός και είσοδος G_0 είναι 1
  - $P_A = P_\Sigma(1)$ (σύμφωνα με εγκυρότητα πρέπει να συμφωνήσουμε 1)



- $P_A = P_\Sigma(1) = P_{G2}(1) = y$

Ανάλυση Εκτελέσεων

- Έστω G_2 βυζαντινός και είσοδος G_0 είναι 1
  - $P_A = P_\Sigma(1)$ (σύμφωνα με εγκυρότητα πρέπει να συμφωνήσουμε 1)



- $P_A(1) = P_\Sigma(1) = P_{G1}(1) = x$
  - Μόνο αυτή η περίπτωση αφού ο G_1 δεν λαμβάνει μήνυμα από G_2

Πιθανότητα Συμφωνίας Αλγορίθμου

- Προσοχή: Οι εκτελέσεις όπου ο G_0 στέλνει 0 αντί 1 θα δώσουν τις ίδιες τιμές.
  - Πάλι ο G_1 θα αποφασίσει 0 με πιθανότητα x!

- Επομένως το σύνολο των δυνατών πιθανοτήτων του αλγορίθμου είναι:

  {1, 1-xy, 1+xy-y, x, y}

- Το 1 αποκλείεται να είναι η πιθανότητα της χειρότερης εκτέλεσης άρα αρκεί να μελετήσω τα:

  {1-xy, 1+xy-y, x, y}

Πιθανότητα Συμφωνίας Αλγορίθμου

- Πειραματικά προσπαθούμε να εντοπίσουμε την χειρότερη περίπτωση

- Θέτουμε
  - x=0.1 , 0.2,…,0.9
  - y=0.1 , 0.2,…,0.9

- Για να πάρουμε την μέγιστη πιθανότητα στην χειρότερη εκτέλεση πρέπει να θέσουμε
  - x=0.62, y=0.62

- Με τις πιο πάνω τιμές παίρνουμε

Πιθανότητα Συμφωνίας Αλγορίθμου = 0.62

Ερωτήσεις;