Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία

Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών

Fast Asynchronous Byzantine Agreement with Optimal Resilience

Byzantine Agreement Problem

- Πρόβλημα των στρατηγών του Βυζαντίου
  - Στρατηγοί της αυτοκρατορίας του Βυζαντίου πρέπει να αποφασίσουν ομόφωνα αν θα επιτεθούν ή όχι.
  - Βρίσκονται σε διαφορετικές τοποθεσίες.
  - Μεταξύ των στρατηγών βρίσκονται προδότες.
  - Στόχος είναι όλοι οι καλοί οι στρατηγοί να συμφωνήσουν σε ένα κοινό σχέδιο δράσης.
  - Οτιδήποτε που αποκλίνει από αυτό είναι καταστροφικό.

Byzantine Agreement Problem

- Byzantine Agreement problem στο computing
  - n παίχτες (π.χ επεξεργαστές)
  - t από n είναι κακόβουλοι παίχτες.
  - Οι κακόβουλοι παίχτες μπορούν να συνεργαστούν όπως θέλουν.
  - Στόχος του πρωτοκόλλου όλοι οι καλόβουλοι παίχτες να έχουν output το ίδιο δυαδικό ψηφίο.

Byzantine Agreement Problem

- Διαφορετικές εκδοχές προβλήματος
  - Σύγχρονο, ασύγχρονο πρωτόκολλο.
  - Δυνατότητες εχθρού:
    - Υπολογιστική δύναμη
    - Διαθέσιμο ποσό πληροφορίας
  - Μέγιστο αριθμό κακόβουλων παιχτών που να ανέχεται το πρωτόκολλο (resiliency).
  - Πιθανοτικό, ντετερμινιστικό πρωτόκολλο.

Byzantine Agreement Problem

- Ορισμός Asynchronous BA protocol
  - Έστω π το πρωτόκολλο όπου κάθε παίχτης έχει δυαδικό input. Λέμε ότι το π είναι (1-ε)-terminating,t-resilient Byzantine Agreement Protocol εάν για κάθε t το πολύ στο πλήθος κακόβουλων παιχτών ισχύουν τα εξής:
    - Τερματισμός:

      Με πιθανότητα 1-ε όλοι οι καλόβουλοι παίχτες τερματίζουν τοπικά.
    - Ορθότητα:

      Όλοι οι καλόβουλοι παίχτες που έχουν τερματίσει, έχουν την ίδια έξοδο. Επιπρόσθετα, αν όλοι οι παίχτες έχουν την ίδια είσοδο, τότε αυτή θα είναι η έξοδος.

Byzantine Agreement Problem

- Ορισμός A-cast protocol
  - Το A-cast είναι πρωτόκολλο εκπομπής ενός μηνύματος σε δίκτυο n παιχτών, εκ των οποίων t κακόβουλοι. Ισχύουν οι παρακάτω ιδιότητες:
    - Τερματισμός:

      Αν καλόβουλος αποστολέας και όλοι οι καλόβουλοι συμμετέρχουν, τότε όλοι οι καλόβουλοι παίχτες θα τερματίσουν. Ακόμα, αν ένας καλός τερματίσει, τότε όλοι οι καλοί θα τερματίσουν.
    - Ορθότητα:

      Όλοι οι καλόβουλοι παίχτες που έχουν τερματίσει, έχουν την ίδια έξοδο. Αν ακόμα ο αποστολέας είναι καλόβουλος η έξοδος αυτή είναι η επιθυμητή.

Byzantine Agreement Problem

- Ορισμός Global Coin Protocol
  - Έστω π το πρωτόκολλο όπου κάθε παίχτης έχει τυχαίο input και δυαδικό output. Λέμε ότι το π είναι (1-ε)-terminating,t-resilient Global Coin Protocol εάν για κάθε t το πολύ στο πλήθος κακόβουλων παιχτών ισχύουν τα εξής:
    - Τερματισμός:

      Με πιθανότητα 1-ε όλοι οι καλόβουλοι παίχτες τερματίζουν τοπικά.
    - Ορθότητα:

      Για κάθε τιμή $\sigma \in \{0,1\}$, με πιθανότητα τουλάχιστον $\frac{1}{4}$ όλοι οι καλόβουλοι παίχτες να έχουν output σ

Byzantine Agreement Problem

- Vote protocol
  - Ντετερμινιστικό πρωτόκολλο
  - Στόχος πρωτοκόλλου είναι οι καλόβουλοι παίχτες να βρίσκουν πλειοψηφία με $\left\lceil \frac{n}{3} \right\rceil - 1$ παρουσία το πολύ κακών παιχτών.
  - (σ,2) συντριπτική πλειοψηφία τιμής σ
  - (σ,1) ευδιάκριτη πλειοψηφία τιμής σ
  - (Λ,0) όχι πλειοψηφία

Byzantine Agreement Problem

- Υλοποίηση Vote protocol για παίχτη P_i
  - 1ος γύρος

    A-cast το input. Με βάση 2t+1 πρώτα A-cast, υπολόγισε ψήφο.
  - 2ος γύρος

    A-cast ψήφο με ταυτότητες παιχτών.

    Με βάση 2t+1 πρώτα “συμβατά” A-casts, καθόρισε ψήφο.
  - 3ος γύρος

    A-cast τη δεύτερη ψήφο με ταυτότητες παιχτών 2ου γύρου.

    Λάβε υπόψη τα 2t+1 πρώτα “συμβατά με 2ο γύρο” A-casts
  - Έξοδος

    Ομοψηφία στον 2ο γύρο, (σ,2). Ομοψηφία στον 3ο γύρο, (σ,1). Αλλιώς, (Λ,0)

Byzantine Agreement Problem

- Λ1: Όλοι οι καλόβουλοι παίχτες τερματίζουν το VP
- Απόδειξη

  Όλοι οι καλόβουλοι τερματίζουν το A-cast

  Υπολογίζουν ψήφο αφού θα λάβουν 2t+1 A-casts

  Όλοι οι καλόβουλοι τερματίζουν το A-cast

  Υπολογίζουν ψήφο αφού όλοι οι συμβατοί είναι καλόβουλοι και ολοκληρώνουν 2t+1 “καλά” A-casts

  Ομοίως, για τον τρίτο γύρο.

Byzantine Agreement Problem

- Λ2: Αν όλοι οι καλόβουλοι παίχτες έχουν είσοδο σ ,τότε όλοι θα έχουν και έξοδο (σ,2)
- Απόδειξη

  Αν όλοι οι καλόβουλοι παίχτες έχουν είσοδο σ, τότε το πολύ t θα έχουν είσοδο $\overline{\sigma}$

  Οπότε κάθε συμβατό σύνολο καλόβουλου παίχτη θα πρέπει να έχει πάντα πλειοψηφία το σ.

  Έτσι, όλα τα συμβατά A-casts στον δεύτερο γύρο θα ψηφίζουν σ.

  Έτσι, όλοι οι καλόβουλοι παίχτες στην έξοδο (σ,2)

Byzantine Agreement Problem

- Λ3: Αν καλόβουλος παίχτης έχει έξοδο (σ,2), τότε όλοι οι καλόβουλοι θα έχουν (σ,1) ή (σ,2)
- Απόδειξη

  Στο 2ο γύρο ο παίχτης 1 παρατήρησε ομοφωνία στο σ.

  Αν παρατήρήσαν και κάποιοι άλλοι ομοφωνία στο σ, τότε αυτοί θα έχουν στην έξοδο (σ,2).

  Στον ίδιο γύρο όλοι οι υπόλοιποι θα λάβουν υπόψη τους t+1 κοινά στοιχεία με τον 1, το λιγότερο.

  Έχοντας t+1 ψήφους του σ, θα βρούν και αυτοί πλειοψηφία το σ. Όποτε στον 3ο γύρο θα ψηφίσουν όλοι το σ και θα έχουν τελικά στην έξοδο τους (σ,1).

Byzantine Agreement Problem

- Λ4: Αν καλόβουλος παίχτης έχει έξοδο (σ,1) και κανένας καλός (σ,2) τότε όλοι οι καλόβουλοι θα έχουν (σ,1) ή (Λ,0)
- Απόδειξη

  Ο παίχτης 1 έχει έξοδο (σ,1).

  Έτσι, το πολύ t ψήφισαν στον τρίτο γύρο $\bar{\sigma}$

  Κανένας καλόβουλος παίχτης δε θα έχει έξοδο $(\bar{\sigma},1)$

  Τουλάχιστον t+1 ψήφισαν σ στον δεύτερο γύρο.

  Κανένας καλόβουλος παίχτης δε θα έχει έξοδο $(\bar{\sigma},2)$

Byzantine Agreement Problem

- Ορισμός Asynchronous BA protocol
  - Έστω π το πρωτόκολλο όπου κάθε παίχτης έχει δυαδικό input. Λέμε ότι το π είναι (1-ε)-terminating,t-resilient Byzantine Agreement Protocol εάν για κάθε t το πολύ στο πλήθος κακόβουλων παιχτών ισχύουν τα εξής:
    - Τερματισμός:

      Με πιθανότητα 1-ε όλοι οι καλόβουλοι παίχτες τερματίζουν τοπικά.
    - Ορθότητα:

      Όλοι οι καλόβουλοι παίχτες που έχουν τερματίσει, έχουν την ίδια έξοδο. Επιπρόσθετα, αν όλοι οι παίχτες έχουν την ίδια είσοδο, τότε αυτή θα είναι η έξοδος.

Byzantine Agreement Problem

- Υλοποίηση Byzantine Agreement για παίχτη P_i
  - Εκτέλεσε Voting protocol με το input.
  - Εκτέλεσε Global Coin protocol.
  - Αν (σ,2), A-cast (Complete with σ)
  - Αν (σ,1), το input σου στον επόμενο γύρο είναι το σ
  - Αν (Λ,0), το input σου στον επόμενο γύρο είναι το αποτέλεσμα του Global Coin protocol.
  - Επανέλαβε το πρωτόκολλο μέχρι να λάβεις 2t+1 A-casts του τύπου (Complete with σ). Τότε βγάλε στην έξοδό σου σ.

Byzantine Agreement Problem

- Λ5: Αν όλοι οι καλόβουλοι παίχτες έχουν είσοδο σ, τότε όλοι οι καλόβουλοι παίχτες τερματίζουν το πρωτόκολλο με έξοδο σ
- Απόδειξη

  Από λήμμα 2, όλοι οι καλοί θα έχουν (σ,2) από το VP.

  Έτσι, όλοι οι καλοί θα κάνουν A-cast (Complete with σ)

  Έτσι, όλοι οι καλοί θα λάβουν 2t+1 A-casts του τύπου (Complete with σ) και το πολύ t A-casts για την άλλη τιμή. Έτσι θα τερματίσουν το πρωτόκολλο με έξοδο σ.

Byzantine Agreement Problem

- Πρόταση 1:

  Αν ένας καλόβουλος παίχτης κάνει A-cast (Complete with σ), τότε όλοι οι καλόβουλοι παίχτες θα κάνουν A-cast (Complete with σ)

- Απόδειξη

  Από λήμμα 3, έχουμε ότι οι καλόβουλοι παίχτες θα έχουν (σ,2) ή (σ,1).

  Αν (σ,2), τότε θα κάνουν A-cast (Complete with σ)

  Αν (σ,1), θα ψηφίσουν όλοι σ στον επόμενο γύρο.

  Από το λήμμα 2, στον επόμενο γύρο θα έχουν όλοι (σ,2) και έτσι θα κάνουν A-cast (Complete with σ).

Byzantine Agreement Problem

- Λ6: Αν ένας καλόβουλος παίχτης έχει έξοδο σ, τότε όλοι οι καλόβουλοι παίχτες θα έχουν έξοδο σ
- Απόδειξη

  Αφού έχει έξοδο σ, τουλάχιστον ένας καλόβουλος παίχτης έκανε A-cast (Complete with σ).

  Από Πρόταση 1, όλοι οι καλόβουλοι παίχτες θα κάνουν A-cast (Complete with σ).

  Έτσι, όλοι οι καλόβουλοι παίχτες θα έχουν 2t+1 A-casts (Complete with σ) και το πολύ t A-casts για την άλλη τιμή.

  Οπότε, θα έχουν έξοδο σ.

Byzantine Agreement Problem

- Λ7: Αν όλοι οι καλόβουλοι παίχτες έχουν ολοκληρώσει την κ-επανάληψη. Τότε όλοι οι καλόβουλοι παίχτες με πιθανότητα $\frac{1}{4}$ τουλάχιστον, θα έχουν το ίδιο input στην επόμενη επανάληψη
- Απόδειξη

  α) Όλοι οι καλόβουλοι παίχτες έχουν για επόμενο input αυτό, το αποτέλεσμα του Global Coin Protocol

  Από ιδιότητες GC, θα έχουν το ίδιο input στην επόμενη επανάληψη με πιθανότητα τουλάχιστον $\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$

Byzantine Agreement Problem

β) Τουλάχιστον ένας καλόβουλος παίχτης βρήκε κάποιου είδους πλειοψηφία στο VP

Φιξάρουμε το σ της πλειοψηφίας.

Από λήμμα 3 και 4, κανένας καλόβουλος παίχτης δε θα έχει $(\bar{\sigma},1)$ ή $(\bar{\sigma},2)$

Οπότε ή θα βρουν πλειοψηφία με το σ ή θα χρησιμοποιήσουν το Global Coin Protocol που από τις ιδιότητες του, θα έχουν όλοι σ με πιθανότητα τουλάχιστον $\frac{1}{4}$

Byzantine Agreement Problem

- Λ8: Έστω οτι όλοι οι καλόβουλοι παίχτες για κάθε επανάληψη που έχουν ξεκινήσει, την έχουν ολοκληρώσει. Τότε όλοι οι καλόβουλοι παίχτες θα τερματίσουν το πρωτόκολλο σε σταθερό μέσο χρόνο εκτέλεσης. $\frac{1}{4}$
- Απόδειξη

  Όπως είδαμε πριν αν κάποιος κάνει A-cast (Complete with σ), τότε όλοι οι καλόβουλοι παίχτες θα ολοκληρώσουν το πρωτόκολλο το πολύ στον επόμενο γύρο. Αποδεικνύεται οτι τα A-casts χρειάζονται σταθερό χρόνο. Αρκεί να δείξουμε λοιπόν, πως χρειάζεται σταθερός μέσος χρόνος μέχρι το πρώτο A-cast (Complete with σ)

Byzantine Agreement Problem

Συμβολίζουμε το ενδεχόμενο να ισχύει η υπόθεση με C.

Συμβολίζουμε το ενδεχόμενο να ισχύει η υπόθεση μέχρι και την κ επανάληψη με C_k

Συμβολίζουμε με τ τον αριθμό των επαναλήψεων του πρωτοκόλλου μέχρι το πρώτο A-cast (Complete with σ)

$$Prob\{\tau > k|C_k\} = Prob\{\tau \neq 1|C_k\} \cdot \ldots \cdot Prob\{\tau \neq k|C_k \cap \tau \neq k-1 \cap \ldots \cap \tau \neq 1\}$$

$$\Rightarrow \quad Prob\{\tau > k|C_k\} \leq (\frac{3}{4})^k$$

$$\Rightarrow \quad E\{\tau|C\} \leq 16$$

Byzantine Agreement Problem

- Λ9: Η πιθανότητα να συμβεί το C, είναι αυθαίρετα μεγάλη
- Απόδειξη

$$Prob(\overline{C}) \leq \sum_{i \geq 1} Prob\{\tau > k \cap \overline{C_{k+1}} | C_k\} \leq \sum_{i \geq 1} Prob\{\tau > k | C_k\} Prob\{\overline{C_{k+1}} | C_k \cap \tau > k\}$$

$$Prob\{\tau > k | C_k\} \leq (\frac{3}{4})^k \leq (\frac{3}{4})^{k-1}$$

$$Prob\{\overline{C_{k+1}} | C_k \cap \tau > k\} \leq \frac{\epsilon}{4}$$

$$\Rightarrow Prob(\overline{C}) \leq \sum_{i \geq 1} \frac{\epsilon}{4} \cdot (\frac{3}{4})^{k-1} = \epsilon$$