CS355 Course Project

Shuxian Jiang

Sep. 25, 2015
Project Overview

• Topic
  Implement the Zero-Knowledge interactive protocol for Subgraph Isomorphism

• Group (less than 5 people)

• Write codes

• Demo to TA
Project Steps

• Topic
  Understand the protocol: see soln for HW2 Q4

• Group (1-4 people)
  Send email to TA on group composition
  (one email per group)

• Write codes
  Submit electronic version to TA by email

• Demo to TA
  choose a time slot on doodle
Project Timelines

• Topic
  Understand the protocol: see soln for HW2 Q4

• Group (1-4 people) (Oct. 5)
  Send email to TA on group composition
  (one email per group)

• Write codes (Nov. 23)
  Submit electronic version to TA by email

• Demo to TA (Nov. 30-Dec. 11)
  all group members need to be present
• Implement the Zero-Knowledge interactive protocol for Subgraph Isomorphism

P
(G1, G2, subgraph G' of G2
Isomorphism G' and G1)

Random Perm α of G2
α(G2)=Q

Request α, Q
or π, Q'

Verify: Q, α(G2)=Q?
or Q’, π(G1)=Q’?
Project Requirements:

- Language: C, C++, JAVA or Python
- Input: undirected graph
- Output: Accept(1) or Reject(0)
- P and V communicate through network
  Implement Socket
- Commitment
Project Requirements: Input

• Format
  
  Adjacency matrices: given in files
  line i: row i of the adjacency matrix
  EX: first line:0 1 0 0 1 1 1 0 0 0
  the graph has 10 nodes and there are edges
  between node 1 and nodes 2, 5, 6, 7.

• Size
  
  Small size (less than 10 nodes) to many hundreds
  nodes size
Grading Policy

• Plus all hws, Total 35%
• Report: (optional)
• Codes:
  no runtime error  
correct result  
other important parts  
sockets(20’), commitment(20’), random gen(5’), multiple runs(5’), different graph sizes(5’), ...

• Late Policy
  -10’ first day, -30’ second day, not accepted after 2 days
Demo Requirements

• All members need to attend and present their own parts
  One grade for one group

• Place  LWSN B116
  Bring your own laptop for demo

• Input graphs
  two sets decided by your own (one small size, one large size),
  at least one set of test graphs given by TA