Zero-Knowledge Proofs

SOC InfoComm Camps on

Computational Problem Solving

Leong Hon Wai
Dept of Computer Science, NUS
http://www.comp.nus.edu.sg/~leonghw/

Amazing, fascinating, mind-boggling.

Copyright © 2007-8 by Leong Hon Wai

“Full-Knowledge” Proofs

Fact:

I have a proof of a theorem X.

Problem:

I want to convince you that *I have a proof of X*.

Traditional Method:

I *show* you my proof of X.

After verifying it, *you are convinced*.

Hon Wai Leong, SoC, NUS

Copyright © 2007-8 by Leong Hon Wai

"Zero-Knowledge" Proofs

Fact:

I have a proof of a theorem X.

Problem:

I want to convince you that *I have a proof of X*, *without letting you gain any information on my actual proof*, other than the fact that *"I have a proof of the theorem of X"*.

Issue:

Of course, I *cannot* show you my proof.

Hon Wai Leong, SoC, NUS

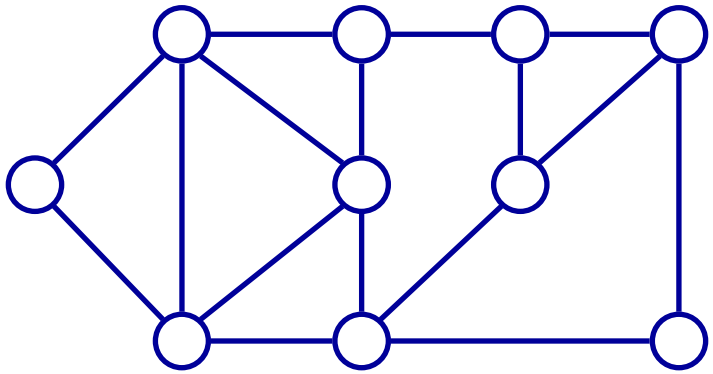
Copyright © 2007-8 by Leong Hon Wai

Graph Colouring Example (GC)

Example:

I want to convince you that the graph below is 3-colorable.

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

Copyright © 2007-8 by Leong Hon Wai

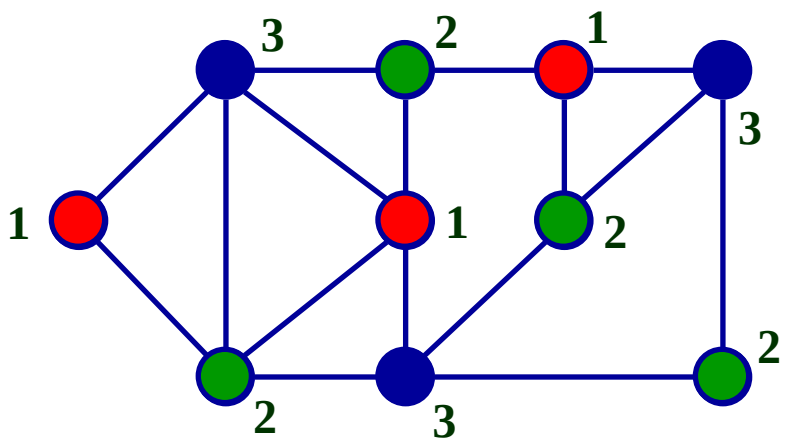
GC Example: Full-Knowledge

Example:

I want to convince you that the graph below is 3-colorable.

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**

Traditional Proof: **Show you the 3-coloring.**



10 nodes, 16 edges

But now,

you also *know* the proof!

Copyright © 2007-8 by Leong Hon Wai

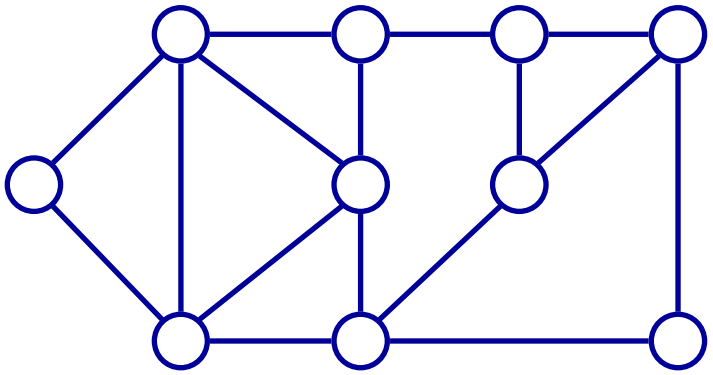
GC Example – ZK-Proof

Example:

I want to convince you that the graph below is 3-colorable.

But, don't want you to know anything about how it is done

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

Copyright © 2007-8 by Leong Hon Wai

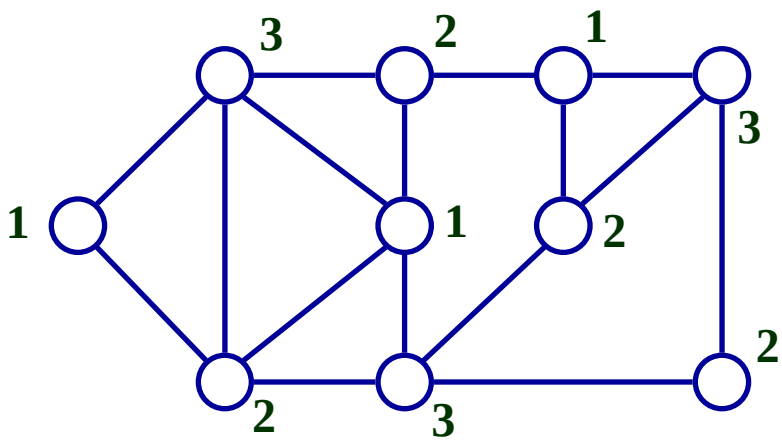
GC Example: ZK-Protocol (1)

Example:

I want to convince you that the graph below is 3-colorable.

But, don't want you to know anything about how it is done

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

PROTOCOL: One Stage

My move ::

1. Randomly permute f : {1,2,3} → {R, G, B}
2. Color vertex labelled k, with color $f(k)$;
3. Cover up all the vertices of the graph.

Your move ::

Randomly choose *one* edge e;

Check the two end-vertices of the edge e;

Copyright © 2007-8 by Leong Hon Wai

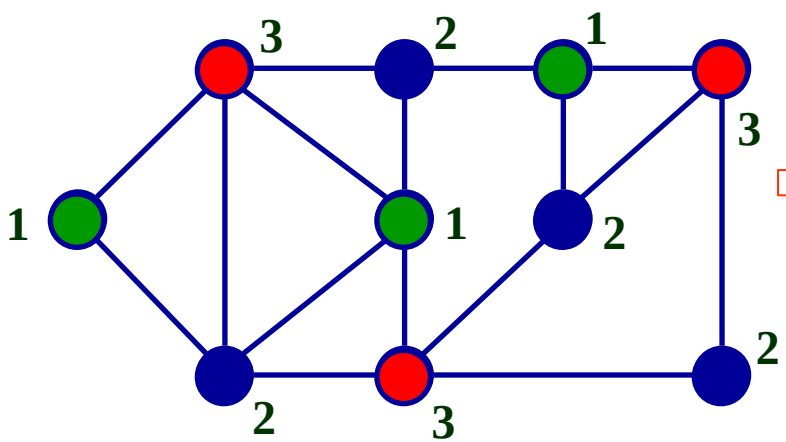
GC Example: ZK-Protocol – (2)

Example:

I want to convince you that the graph below is 3-colorable.

But, don't want you to know anything about how it is done

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

PROTOCOL: One Stage [1 example]

My move ::

1. Eg: $f(1)=G$, $f(2)=B$, $f(3)=R$

2. Color vertex labelled k, with color $f(k)$;

Copyright © 2007-8 by Leong Hon Wai

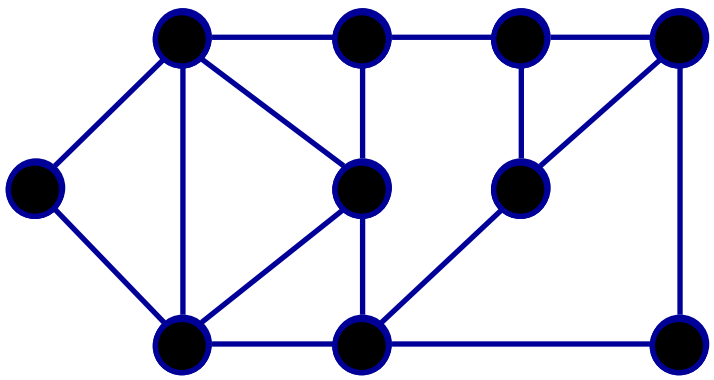
GC Example: ZK-Protocol – (3)

Example:

I want to convince you that the graph below is 3-colorable.

But, don't want you to know anything about how it is done

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

PROTOCOL: One Stage [1 example]

My move ::

1. **Eg: $f(1)=G$, $f(2)=B$, $f(3)=R$**
2. **Color vertex labelled k, with color $f(k)$;**
3. **Cover up all the vertices of the graph.**

Copyright © 2007-8 by Leong Hon Wai

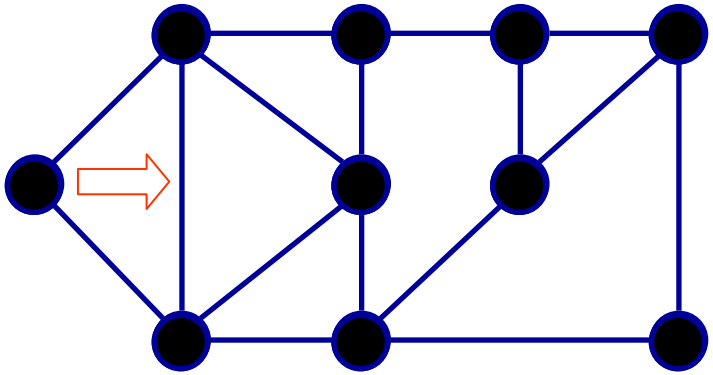
GC Example: ZK-Protocol – (4)

Example:

I want to convince you that the graph below is 3-colorable.

But, don't want you to know anything about how it is done

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

PROTOCOL: One Stage [1 example]

My move ::

1. Eg: $f(1)=G$, $f(2)=B$, $f(3)=R$
2. Color vertex labelled k, with color $f(k)$;
3. Cover up all the vertices of the graph.

Your move ::

Randomly choose *one* edge e;

Check the two end-vertices of the edge e;

Copyright © 2007-8 by Leong Hon Wai

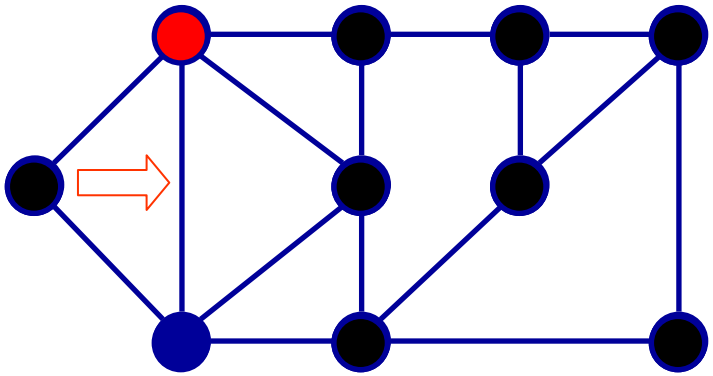
GC Example: ZK-Protocol – (5)

Example:

I want to convince you that the graph below is 3-colorable.

But, don't want you to know anything about how it is done

Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**



10 nodes, 16 edges

PROTOCOL: One Stage [1 example]

My move ::

1. Eg: $f(1)=G$, $f(2)=B$, $f(3)=R$
2. Color vertex labelled k, with color $f(k)$;
3. Cover up all the vertices of the graph.

Your move ::

Randomly choose *one* edge e;

Check the two end-vertices of the edge e;

Copyright © 2007-8 by Leong Hon Wai

Analysis: After 1 Phase…

- Are you convinced?
  - Of course NOT.
  - You have only seen 1 edge (out of 16 edges)
- How to convince you?
  - Allow you to open more edges?
    - *NO! Why not?*
- Question: What if I cheated?
  - I may "get lucky"
  - I may get caught.

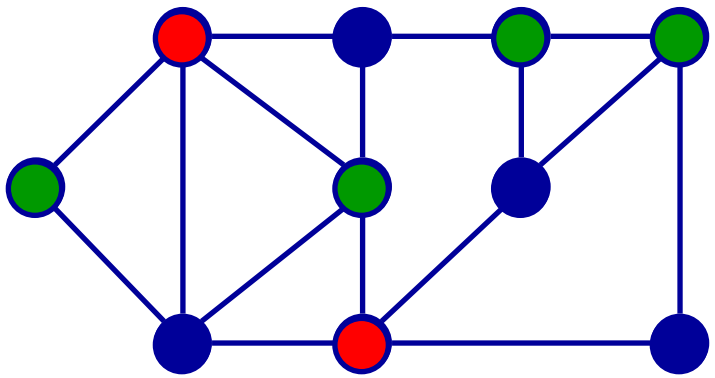
Hon Wai Leong, SoC, NUS
Copyright © 2007-8 by Leong Hon Wai

Analysis: What if I cheated…

If I do *not* have a 3-coloring, but I cheated.

Example: I have the *bad* coloring shown below…

On at least 1 edge, both nodes have the *same color*.



10 nodes, 16 edges

If I cheated on the coloring:

Prob (I cheated and get caught) ≥ 1 / 16

Prob (I cheated, but got lucky) ≤ 15 / 16

- **After 1 phase,**

$$\Pr(\text{I cheated, but got lucky}) \le \left(\frac{15}{16}\right)$$

Copyright © 2007-8 by Leong Hon Wai

Analysis: After *many* Phase…

- **What if we do 16 phases**
  - **And each time the "revealed colors" were different!**

$$\Pr(\text{I cheated, but got lucky each time}) \le \left(\frac{15}{16}\right)^{16} < 0.5$$

0.35607

- **What about after 16*100 phases?**

$$\Pr(\text{I cheated, but got lucky each time}) \le (0.5)^{100} = 7.889 \times 10^{-31}$$

- **What about after 16*1000 phases?**

$$\Pr(\text{I cheated, but got lucky each time}) \le (0.5)^{1000}$$

$$= 9.332 \times 10^{-302}$$

Copyright © 2007-8 by Leong Hon Wai

Analysis: the general case

For a graph with *m* edges,

- **After 1 phase,**

$$\Pr(\text{I cheated, but got lucky}) \le \left(\frac{m-1}{m}\right)$$

Approaches $1/e = 0.36788$

- **After *m* phases**

$$\Pr(\text{I cheated, but got lucky each time}) \le \left(\frac{m-1}{m}\right)^m < 0.5$$

- **After 1000*m* phases?**

$$\Pr(\text{I cheated, but got lucky each time}) \le (0.5)^{1000}$$

$$= 9.332 \times 10^{-302}$$

Copyright © 2007-8 by Leong Hon Wai

Analysis: Zero Knowledge?

- **Do you know how the graph is colored**
  - **After 1000*m* phases**
  - **Can you accumulate the "knowledge"**
    - ***from all the different edges***
    - ***from different phases?***
- **Zero-Knowledge Proof**
  - **Is amazing, mind-boggling!**
  - **Used in authentication (eg: among banks)**

Copyright © 2007-8 by Leong Hon Wai

Thank you!

NUS National University of Singapore

School of Computing

Copyright © 2007-8 by Leong Hon Wai