Zero-Knowledge Proofs

(*Fun and Creative Problem Solving*

in Mathematics and Computer Science)

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

Amazing, fascinating, mind-boggling.

"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*.

"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:

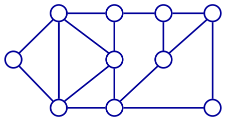
Of course, I *cannot* show you my proof.

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

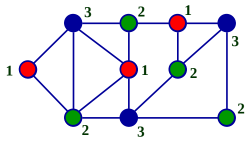
GC Example: Full-Knowledge

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.



But now,

you also *know* the proof!

10 nodes, 16 edges

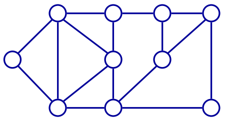
GC Example – ZK-Proof

Example:

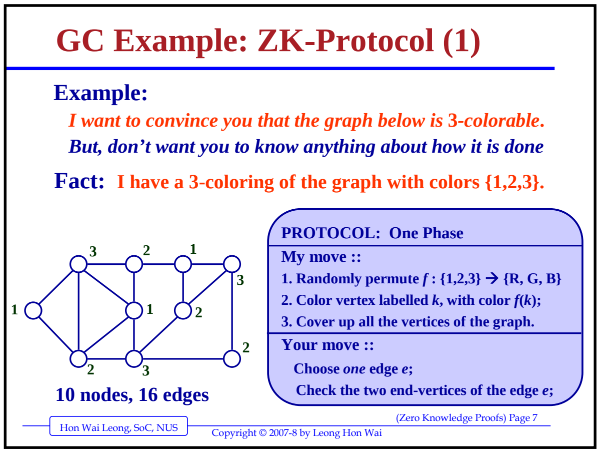
I want to convince you that the graph below is 3-colorable.

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



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

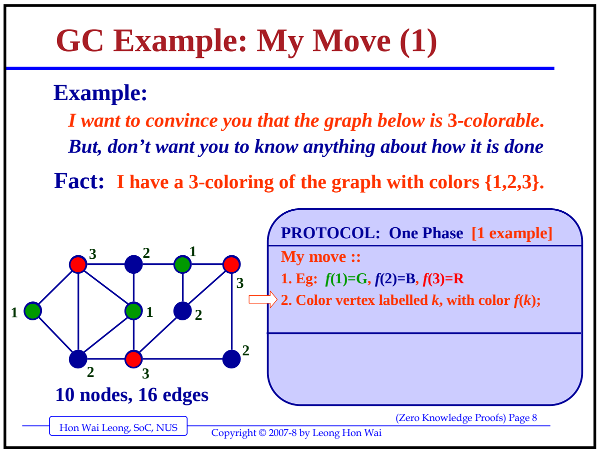
PROTOCOL: One Phase

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 ::

Choose *one* edge *e*;
Check the two end-vertices of the edge *e*;



GC Example: My Move (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

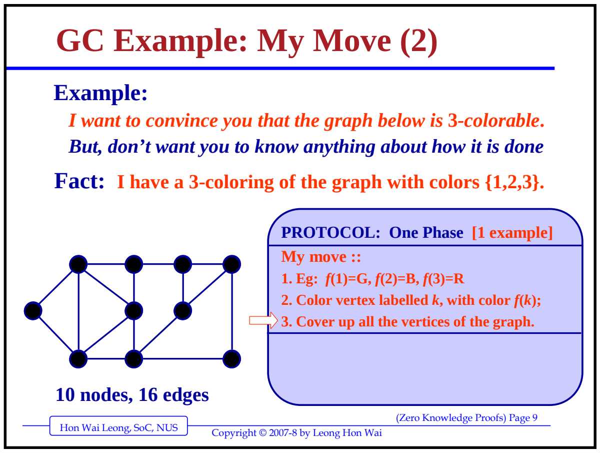
Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**

10 nodes, 16 edges

PROTOCOL: One Phase [1 example]

My move ::

1. Eg: *f*(1)=G, *f*(2)=B, *f*(3)=R
2. Color vertex labelled *k*, with color *f*(*k*);



GC Example: My Move (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

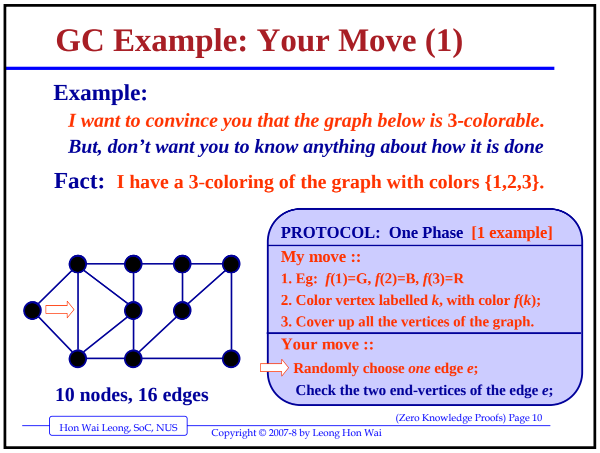
Fact: **I have a 3-coloring of the graph with colors {1,2,3}.**

10 nodes, 16 edges

PROTOCOL: One Phase [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.



GC Example: Your Move (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

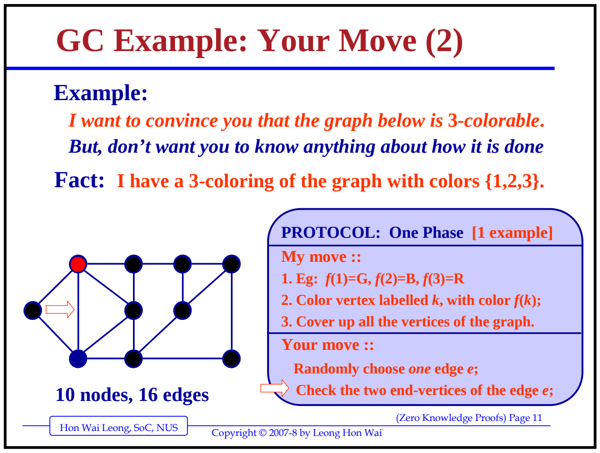
PROTOCOL: One Phase [1 example]

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*;



GC Example: Your Move (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 Phase [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*;

ToDo-2008: Do one more phase

Update: (Dec 2009)

- ❖ **Goto GraphBench DEMO**

(Thanks go to Melvin for
programming this demo…)

Analysis: After 1 Phase…

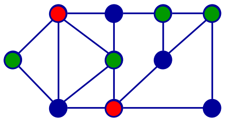
- ❑ **Are you convinced?**
  - ❖ **Of course NOT.**
  - ❖ **You have only seen 1 edge (out of 16 edges)**
- ❑ **How to convince you?**
  - ❖ **Allow you to open more edges?**
    - ◆ ***NO! Why not?***
- ❑ **Question: What if I cheated?**
  - ❖ **I may "get lucky"**
  - ❖ **I may get caught.**

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,**

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

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?**

$$\Pr(\text{I cheated, but got lucky each time}) \le (0.5)^{1000}$$
$$= 9.332 \times 10^{-302}$$

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?**

$$\Pr(\text{I cheated, but got lucky each time}) \le (0.5)^{1000}$$
$$= 9.332 \times 10^{-302}$$

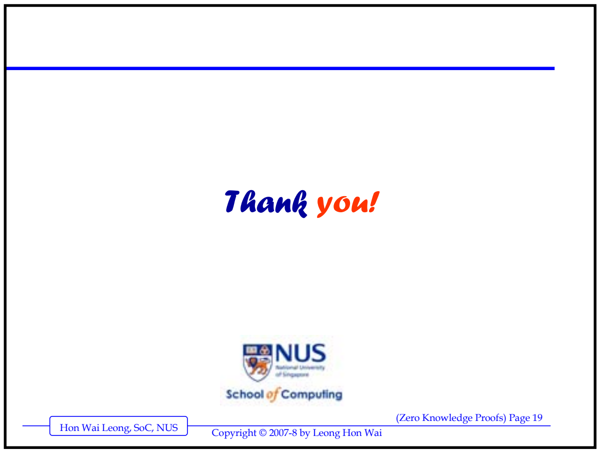
Analysis: Zero Knowledge?

- ❑ **After 1000m phases**
  - ❖ **Is totally convinced of *"the fact"*!**
    - ◆ ***That you know how to color graph with 3 colours***
  - ❖ **But have no (negligible) knowledge**
    - ◆ ***of how the graph is colored***
- ❑ **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 Protocal

- ❑ **Zero-Knowledge Protocol**
  - ❖ **Is amazing, mind-boggling!**
- ❑ **Applications**
  - ❖ **Used in authentication (eg: among banks)**
- ❑ **Practical Technical Issues:**
  - ❖ **how to prevent cheating in the protocol.**

  - ❖ **Outside the scope of this presentation**
  - ❖ **See Dr. Soo Yuen Jien's talk on "Encryption: The Art of Secret Keeping"**



Thank you!

Hon Wai Leong, SoC, NUS

(Zero Knowledge Proofs) Page 19