TOPIC: 6.857 - Computer & Network Security

DATE: 4/14/14

FILE UNDER:

PAGE: L18.1

Admin:

- Quiz in-class Wed (4/16)
  open notes. Closed texts, phones, laptops
  Coverage through today's lecture.

Today:

ZK Proofs (& POK)

- [ ] Quality control
- [ ] Suddoku
- [ ] 3-colorability
- [ ] isomorphism of graphs
- [ ] hamiltonian path
- [ ] discrete log

TOPIC:

DATE:

FILE UNDER:

Quality control

Suppose a widget-making machine either

(A) – works perfectly

(B) – makes 1 out of k widgets defective (randomly) k known

on a given day. You can test widgets.

Can you tell which is case?

O O ⊗ ⊗ O O ⊗ O ⊗ O O O X

Pick tk to test

$$\text{Prob}(\text{no defects found} \mid B) = (1 - 1/k)^{tk}$$

$$\approx (e^{-1/k})^{tk}$$

$$= e^{-t}$$

for sufficiently large t (e.g. $t = 20$) this is ≈ 0,

so you can conclude A holds. (Proper analysis needs

Bayes Rule & priors on A & B...)

TOPIC:

DATE:

FILE UNDER:

PAGE: L18,3

Sudoku

How can I convince you I know soln, without telling you anything about soln?

						3	6	
	1			9	8		5	
		9	6		3	8		
		8	9		5	4		
		5	7		4	1		
	9		4	5			2	
	8	2						

"zero-knowledge proof of knowledge" (ref next page)

Using cards

Using commitments

A	B	C	D	E	F	G	H	I
9	2	8	1	6	3	7	4	5

- commit to letter for each position
- commit to table
- pick two in same row (column, or block) & test

or test table

or test known square

TOPIC:

DATE:

FILE UNDER:

P = prover

V = verifier

$P \longleftrightarrow V$

Interactive Proof: (of proposition x)
↖ e.g. "puzzle has soln"

Properties:

Completeness: if x true, V accepts

Soundness: if x false, V rejects with prob $\geq$ constant > 0. (ε)

Zero-knowledge: verifier learns nothing else except whether x is true

May iterate protocol to reduce soundness error

t times $\Rightarrow$ for false x, prover succeeds (verifier accepts) with probability $\leq (1-\varepsilon)^t$

Proof of knowledge: Verifier becomes convinced that P actually knows solution

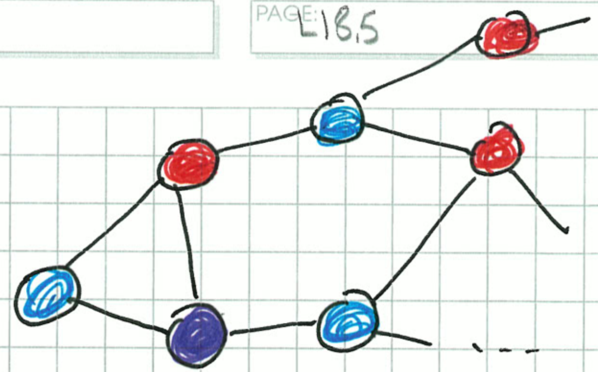
TOPIC:

DATE:

FILE UNDER:

PAGE: L18.5

Graph 3-colorability



How can I convince you that I know 3-coloring of vertices, without telling you anything about the coloring I know?

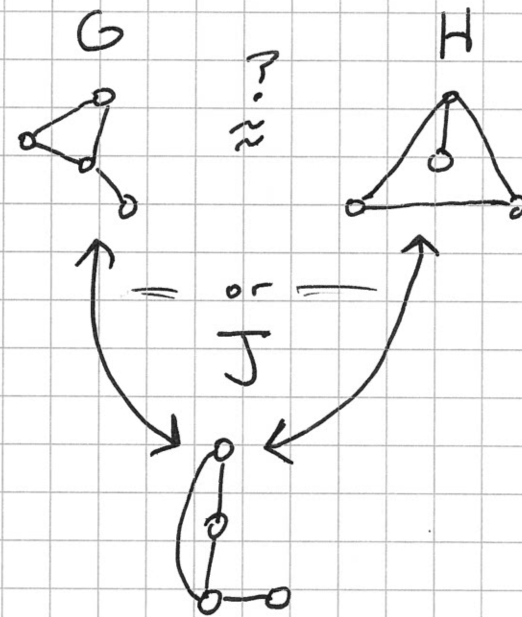
TOPIC:

DATE:

FILE UNDER:

PAGE: L18,6

Graph isomorphism



How can I prove to you that G & H are isomorphic, without revealing isomorphism?

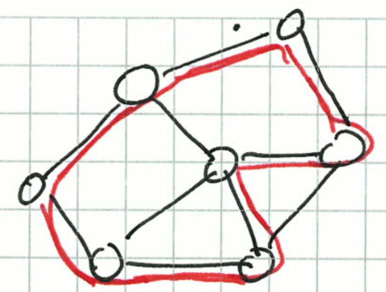
TOPIC:

DATE:

FILE UNDER:

PAGE: L18.7

Hamiltonian graph



Hamiltonian path

TOPIC:

DATE:

FILE UNDER:

Discrete logarithm POK (Schnorr) (ZK)

p = large prime
q divides $p-1$, q prime

g generates subgroup $G_q = \langle g \rangle$ of order q

$x = SK \qquad x \in Z_q$
$y = g^x = PK \qquad y \in G_q$

How can Alice prove to Bob she knows x? in ZK?

A		B
$k \in_R Z_q$, $a = g^k$	$\xrightarrow{a}$ "commitment"
$\xleftarrow{c}$ "challenge"	$c \in_R Z_q$
$r = cx + k$	$\xrightarrow{r}$ "response"	check $y^c \cdot a \stackrel{?}{=} g^r \pmod p$

Pf: $g^{cx} g^k \stackrel{?}{=} g^r$

$g^{cx+k} = g^r$ ✓

Thm: Protocol is complete.

(If Alice knows x, Bob always accepts.)

TOPIC:

DATE:

FILE UNDER:

PAGE: L18, 10

Thm. (Soundness & POK)

$$\left.\begin{array}{l}\text{Alice can play game} \\ \Rightarrow \text{Alice "knows" } x\end{array}\right] \overset{\text{or}}{\equiv} \left[\begin{array}{l}\text{Alice doesn't know } x \\ \quad \Rightarrow \text{Alice can't play game}\end{array}\right.$$

PF: Alice can play game $\triangleq$ for any a & almost all c she can produce r

Fix $a = g^k$

Suppose Alice can succeed for c & for $c' \neq c$

$$\begin{array}{l} r = cx + k \\ r' = c'x + k \\ \hline \end{array}$$

$$r - r' = (c - c') \cdot x$$

$$x = (r - r') / (c - c') \quad \therefore \text{Alice "knows" } x \quad \blacksquare$$

(Note: Schnorr protocol can be turned into signature scheme by letting $c = \text{hash}(a, \underset{\uparrow \text{message}}{M})$)

TOPIC:

DATE:

FILE UNDER:

Thm: Protocol is ZK (for honest verifier)

Pf: Bob learns transcript (a,c,r). Nothing more.

Transcript is a random variable; Bob gets sample.

Bob can generate such samples <u>on his own</u>!

With correct distribution!

$$c \xleftarrow{R} \mathbb{Z}_q \qquad \text{(assuming honest verifier)}$$

$$r \xleftarrow{R} \mathbb{Z}_q \qquad (r \text{ uniform in } \mathbb{Z}_q \text{ since } k \text{ is})$$

$$a = g^r / y^c$$

$\Rightarrow$ (a,c,r) has exactly same distribution as in protocol.

$\therefore$ Bob learns nothing (except that Alice can play game)

$\therefore$ protocol is ZK. $\blacksquare$

TOPIC:

DATE:

FILE UNDER:

Thm: Any problem in NP has a ZK proof! (GMW)

NP problems have form:

$$f(x) \equiv (\exists w)\, P(x, w)$$

true/false predicate

input instance

witness

poly-time predicate

I can convince you that $f(x) = \text{True}$
without showing w!

$\equiv$ Proof of knowledge of w

Pf: Use 3-colorability, which is NP-complete.

TOPIC:

DATE:

FILE UNDER:

More examples:

- My modulus has exactly two prime factors
- All these ciphertexts encrypt the same message.
- The plaintext for this message contains another message & signature on it by Bank

$$X = E\left(PK, (M, \sigma_B(M))\right)$$

- I know w s.t. $x = \text{hash}(w)$ (pre-image)

Extensions:

- Non-interactive ZK. (NIZK)

use Fiat-Shamir heuristic:

challenge = hash (commitment || statement to be proved)

so Prover can derive challenge & write it all down