Nov 20, sun midnight pdf

1) Graph isomorphism — with interaction how to solve?

Input: G_1, G_2 (two undirected graph)

Output: If these two are structurally the same (isomorphism) then yes, else NO

we had graph non-isomorphism problem

two programs $P_1 \leftrightarrow P_2$

1) Answer

graph isomorphism prob (GI)

input: G_0, G_1

output: yes G_0, G_1 isomorphic

No, otherwise

as of yet

no ploy time alg is known

programs (A)

(B) poly time)

with interaction

→ can solve G1 with very high prob

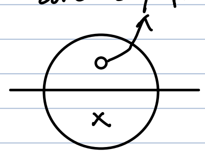
G_0, G_1

H, G_b'

if G_0, G_1 are isomorphic then after m rounds,

H, G_b' isomorphic

A can solve any problem



G_0, G_1

G_b

1. selects value b from {0, 1} randomly
2. computes a permutation denoted to π_1
   $H = \pi_1(G_b)$ // G_b, H
3. $A \xrightarrow{H} B$
4. ← $\boxed{\text{select } b' \text{ from } \{0, 1\}}$
5. computes a permutation π_2 // $H, G_{b'}$ isomorphism
   $H = \pi_2(G_{b'})$
   π_2 ?
6. $A \xrightarrow{\pi_2} B$

A computes

H G_0 G_1

π_2

GI

G_0, G_1, π_2

$G_0 = \pi(G_1)$

$A \longleftrightarrow B$

① $A \xrightarrow{\pi} B$ ○ G_0, G_1

② A gives the answer

$G_0 \ncong G_1$

③ A view B view

B has to solve GI problem

A: powerful mechanism

G_0, G_1

Answer: 1 bit info

Zero knowledge protocol

$A \rightarrow B$

G_0, G_1

IP = PSPACE

① completeness | 100%

② soundness | $\leq \frac{1}{2}$

Assume that there are two parties A, B.

A is computationally powerful, but B can use polynomial time resources only.

1. The two graphs G0, G1 are given to both parties. // G0, G1 - input

2. A selects a value, b from {0,1} randomly. 그랜험과
3. if b=0 then A uses G0. otherwise A uses G1.
4. A computes a permutation pi_1 and apply p_1 to Gb. // p_1(Gb) is isomorphic to Gb.
5. Let H be the result of step 4. that is H=pi_1(Gb).

6. A sends H to B. // note that B cannot compute a permutation p_1 from H.

7. B selects a value b' from {0,1} randomly and sends b' to A.

8. A computes a permutation pi_2 such that H=pi_2(Gb'). // Gb' is either G0 or G1

9. A sends pi_2 to B. // note that B can determine whether pi_2(Gb')=H or not.

10. B checks whether pi_2 is a correct isomorphims of H, Gb' or not.

Steps 2 to 10 are repeated for m times. If each time, (in step 10) the answer is correct, then B can conclude that G0 and G1 are isomorphic.

----

4 by 4 sudoku to graph coloring problem

- each cell becomes a node
- for any cell in 16 cells, 7 edges exist to other nodes

for example, the node (for the 2nd row, 2nd column) has edges with
(1) all nodes in the same row - 3 edges
(2) all nodes in the same column - 3 edges
(3) all nodes in the same block - 1 edge

if the resulting graph is 4 colorable, then the answer is yes.
otherwise, the answer is no.

2) Comparison of Resources

From the perspective of Algorithms.

- time
- space
- Random bits
- Interaction

similarities,
differences

Ex)

time | → DP
space | time ↔ space related

3) Sudoku : $n^2 \times n^2$, $n \geq 2$ (row, columns) $\{1, 2, 3, 4\}$

A

Rule:

	1		3
2			3

(1) each row - at most once

(2) each column - "

(3) each block - has to be with all numbers

Input: a grid (4x4) where Every Entry is filled with $\{1, 2, 3, 4\}$

Ex) Random filled

1	2	2	4
3	4	1	1
2	4	3	4
1	3	2	1

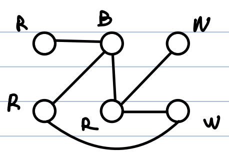
output : yes if this satisfy Rule, else no

K-colors Graph Coloring Problem ($k \geq 3$) ← a parameter

B

input : undirected graph

Output : yes if any two adjacent nodes are colored differently
else no



input $k=3$
$\{R, G, B\}$

Yes possible

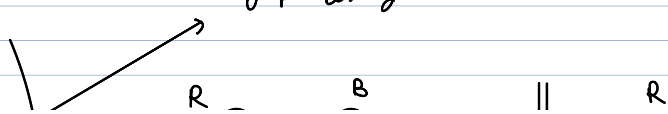
It is possible to transform A into problem B) Chapter 34, 36

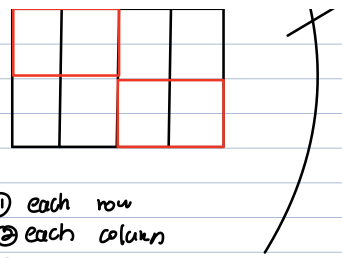
3) Solution

4x4 sudoku

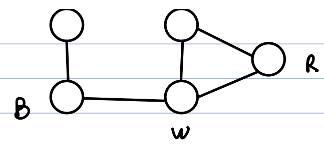
graph coloring

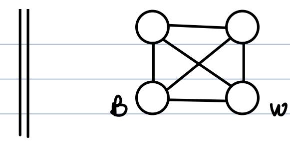
$\{1, 2, 3, 4\}$





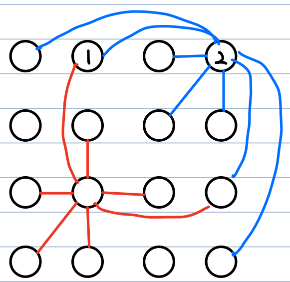
① each row
② each column
③ " block





4x4 Sudoku ≤ 4-coloring problem

Each entry ⟶ $\boxed{\text{a node}}$ — 7 edges



G } 4-colorable
1, 2, 3, 4

Example of Reduction

B's solution
↓
A's solution

A is reduced to B

A ≤ B

2+3=5

ab+cde = abcde (operator overloading)