PRACTICAL EXERCISES 1 (3 p. maximum)	
Code : *TCPT* Acad.Year : *2018-2019* Semester : *SUMMER* Date : *03.04.2019* Duration : *30 min*	Last Name : Name : Student ID : Signature : 2 QUESTIONS ON 1 PAGE
1.	2.

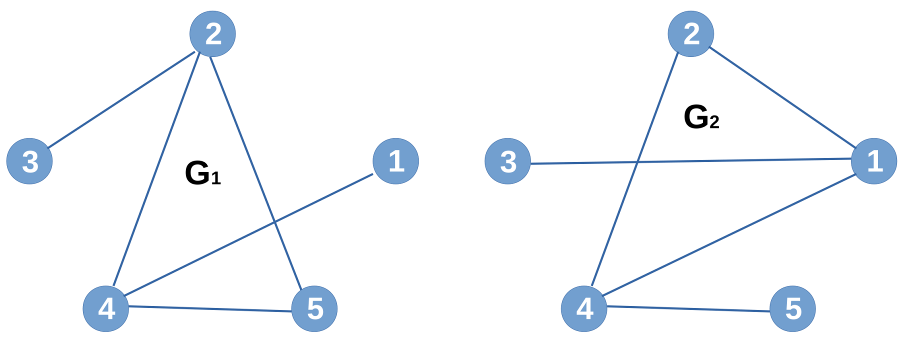
No calculators, cell-phones, computers and books allowed.

If H = 1 then
- Ex.1: $j = 1$, $s = 3$
- Ex.2: $j = 1$

If H = 2 then
- Ex.1: $j = 2$, $s = 4$
- Ex.2: $j = 2$

Exercise 1. 1.2 P.

Graph Theory



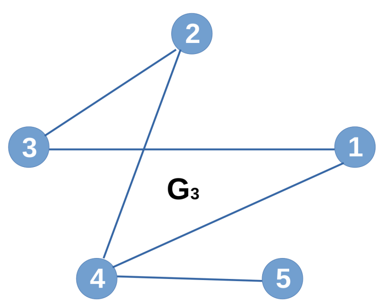
(a) write G_j in formula (j is give above).

Proof. **Solution for** $j = 1$**.**
$G_1 = (\{1, 2, 3, 4, 5\}, \{(1, 4), (2, 3), (2, 4), (2, 5), (4, 5)\})$ □

(b) draw G_s, where (s is given above)
$G_3 = (\{1, 2, 3, 4, 5\}, \{(1, 3), (2, 4), (2, 3), (1, 4), (4, 5)\})$
$G_4 = (\{1, 2, 3, 4, 5\}, \{(1, 2), (2, 3), (3, 4), (1, 4), (4, 5)\})$

Proof. **Solution for** $s = 3$**.**

□



(c) are G_j and G_s isomorphic? Justify your answer.

Proof. **Solution for $j = 1$ and $s = 3$.**
No they are not isomorphic. In fact,

# vertices	5	5	same
# edges	5	5	same
degree	3	3	same
# vertices of degree 3	2	1	different

G_1 has two vertices of degree 3 (i.e. "2" and "4") and G_3 has only 1 vertex of degree 3 (i.e. "4"). □

Note: this $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ represents a permutation and this $G_1 = (\{1,2,3,4\}, \{(1,2),(2,3),(3,4),(2,4)\})$ a graph. This notation $(1,2,3,4,2)$ has no meaning. If we apply a permutation to a graph we obtain another graph, which means that you have to write it as a graph. In particular, for $G_1 = (V, E)$, $E = \{(1,2),(2,3),(3,4),(2,4)\}$ represents the connections of the vertices V.

Exercise 2. 1.8 P.
Zero-Knowledge Protocol
Let $G_0 = \{\{1,2,3,4\}, \{(1,2),(1,3),(2,4),(3,4),(1,4)\}\}$,
where $\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ and $\phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

(a) write a permutation different from ϕ_1, ϕ_2 and identity,
$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \dots & \dots & \dots & \dots \end{pmatrix}$

Proof. For example, I choose $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ □

(b) compute $G_1 = \pi(G_0)$ in formula.

Proof. We apply π to each edge of G_0:
$\pi(1,2) = (4,3)$, $\pi(1,3) = (4,1)$, $\pi(2,4) = (3,2)$, $\pi(3,4) = (1,2)$ and $\pi(1,4) = (4,2)$.
Therefore, $G_1 = \pi(G_0) = (\{1,2,3,4\}, \{(3,4),(1,4),(2,3),(1,2),(2,4)\})$. □

(c) set $\phi = \phi_j$ and compute ϕ^{-1} (j is given above).

Proof. **Solution for $j = 2$.** that is $\phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. We switch the rows: $\begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ then we sort the first row maintaining the correspondences. $\phi_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

□

(d) compute $\pi \circ \phi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ ... & ... & ... & ... \end{pmatrix}$

Proof. **Solution for $j = 2$.** $\pi \circ \phi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ We have to Apply before ϕ^{-1}, then π: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. □

(e) apply Zero-Knowledge Protocol for one iteration.

Prover **Verifier**

System parameters: $G_0 = (\{1, 2, 3, 4\}, \{(1, 2), (1, 3), (2, 4), (3, 4), (1, 4)\})$,
$G_1 = (\{1, 2, 3, 4\}, \{(3, 4), (1, 4), (2, 3), (1, 2), (2, 4)\})$

- Prover: $G_1 = \pi(G_0)$ where $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$
- Prover: generates $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, and compute $G_2 = \phi(G_0) =$ $(\{1, 2, 3, 4\}, \{(2, 3), (2, 4), (3, 1), (4, 1), (2, 1)\})$

$\xrightarrow{G_2}$

- Verifier: chooses a bit $b \in_R \{0, 1\}$

$\xleftarrow{b = 1}$

- Prover: sends back $\psi = \pi \circ \phi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

$\xrightarrow{\psi}$

- Verifier: checks $G_1 \stackrel{?}{=} \psi(G_2)$
  $\phi(G_2) =$
  $(\{1, 2, 3, 4\}, \{(4, 3), (1, 4),$
  $(2, 3), (1, 2), (2, 4)\})$

Proof.

Note that $G_2 = \phi(G_0)$ and $G_1 = \phi(G_2)$ are computed as in (b). □