Contents

[Task 1 2](#_Toc31195800)

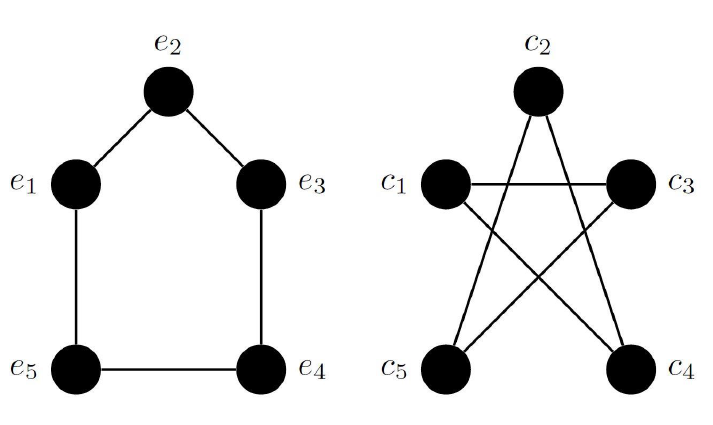
[Task 2 3](#_Toc31195801)

[Task 3 4](#_Toc31195802)

[References 5](#_Toc31195803)

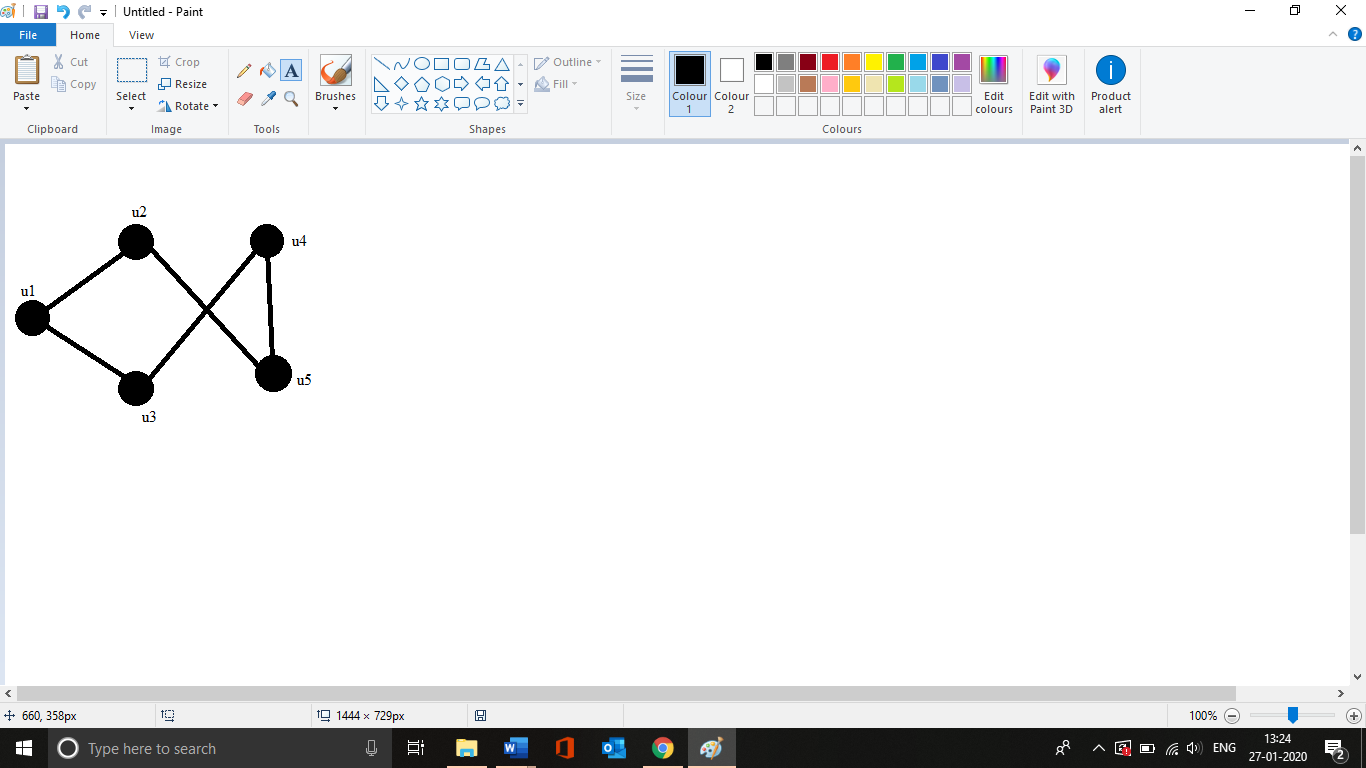
# Task 1

The given two graphs are isomorphic graphs. The reason is in order to qualify to be an isomorphic graph the graph should have same number of edges, connectivity and as well as vertices (Tutorialspoint, n.d.).



Screenshot 1 Given example

So, while seeing the above graphs we can understand that in graph 1 each vertices has connectivity with other 2 vertices (e1-> e2, e5). Also, in graph 2 the same condition applies. (c1-> c3, c4). So, we can conclude that both graphs are isomorphic.



Screenshot 2 New graph

Screenshot 2 shows the graph created using the vertices u1, u2, u3, u4 and u5. The vertices in new isomorphic graph corresponds with graph 1 given in example.

The corresponded vertices are,

* u1 -> e2
* u2->e3
* u3 -> e1
* u4->e4
* u5->e5

# Task 2

In general zero knowledge proofs are the methods used by a person to prove something to other without providing any additional information about it (Shaan, 2019). In cryptography zero knowledge proof deployed in cryptocurrency exchange. During the cryptocurrency exchange (Hyperledger, 2019) a prover can convince a verifier that the secret values is known by him without revealing any information related with it except the fact that he knows the secret value

For the given scenario to prove my colour-blind partner that the apples are different colour without revealing which one is which. The solution is I give both the apples to my partner without revealing which is red and which is green and ask my partner to put his hands in back. Then my partner may or may not exchange them. At this point the probability of exchanging the apples would be 50% and when my partner finally brings them in front, I can see whether they got exchanged or not.

By repeating this process for multiple times my partner eventually will get convinced that both the apples are in different colour.

So, this is a zero-knowledge proof that my partner knows both apples are different in colour without knowing which is which.

# Task 3

Practically, the isomorphic graph problem can be used to construct zero-knowledge proof. Assuming that, we have 2 isomorphic graphs named as Graph 1 and Graph 2. Now using zero knowledge proof I have to prove my partner that both the graphs are isomorphic without revealing him the concept of isomorphic graph. So I create one more graph named Graph 3 by randomly reconstructing the Graph 1. So, now Graph 3 is also isomorphic as same as Graph 1 and Graph 2. So far I know the isomorphism between Graph 1 & Graph 2, Graph 1 & Graph 3, and Graph 2 & Graph 3.

Now if I shows the Graph 3 to my partner I have to prove him that Graph 1 and Graph 3 are Isomorphic and as well as Graph 2 and Graph 3 are Isomorphic too.

Now partner try to verify whether my given answer is correct or not. Also, without using the isomorphism of graph 1 and graph 2 I would not have been created graph 3. So each time I can use graph 1’s permutation to produce graph 31 and graph 2’s permutation to produce graph 32.

Thus, changes are repeated multiple times to find the possibilities untill my partner gets convices. Also, there is only 4 possibilities each round.

* Sending Graph 31 and my partner asks for (31, 11) Correct answer
* Sending Graph 32 and my partner asks for (32, 2): Correct answer
* Sending Graph 31 and my partner asks for (31, 2): Wrong answer
* Sending Graph 32 and my partner asks for (32, 1): Wrong answer

So I will be left with 50% possibility that the answer I gave will be right since I know the isomorphism of Graph 1 and Graph 2. Also, my partner will get conveniced that the 3 graphs are isomorphic.

# References

Hyperledger. (2019). Research Paper: Validating Confidential Blockchain Transactions with Zero-Knowledge Proof – Hyperledger. Retrieved from <https://www.hyperledger.org/blog/2019/04/25/research-paper-validating-confidential-blockchain-transactions-with-zero-knowledge-proof>

Shaan, R. (2019). What are Zero Knowledge Proofs?. Retrieved from <https://towardsdatascience.com/what-are-zero-knowledge-proofs-7ef6aab955fc>

Tutorialspoint. Graph Theory - Isomorphism. Retrieved from <https://www.tutorialspoint.com/graph_theory/graph_theory_isomorphism.htm>

Lukas, K. (2017). How to prove that you know something, without revealing it? Zero-knowledge proofs, ZCash, Ethereum. Retrieved, from <https://hackernoon.com/how-to-prove-that-you-know-something-without-revealing-it-zero-knowledge-proofs-zcash-ethereum-43ce35d4d1c5>