Coloring and Multicoloring of Graphs to Secure a Secret

Tanja Vojković

PMF Split, Croatia

27.09.2018.

Introduction

Our work so far:

- Vojković Tanja, Vukičević Damir and Zlatić Vinko. "Multicoloring of graphs to secure a secret." accepted for publication in Rad HAZU
- Vojković Tanja and Vukičević Damir. "Safe 3-coloring of graphs". submitted to Glasnik Matematički
- Vojković Tanja and Vukičević Damir. "Two types of attack in a colored graph". in preparation

Coloring and Multicoloring

- **Vertex k-coloring** of graph G is a function $\phi : V(G) \to \{1, 2, ..., k\}$ which colors every vertex of a graph in one of k colors.

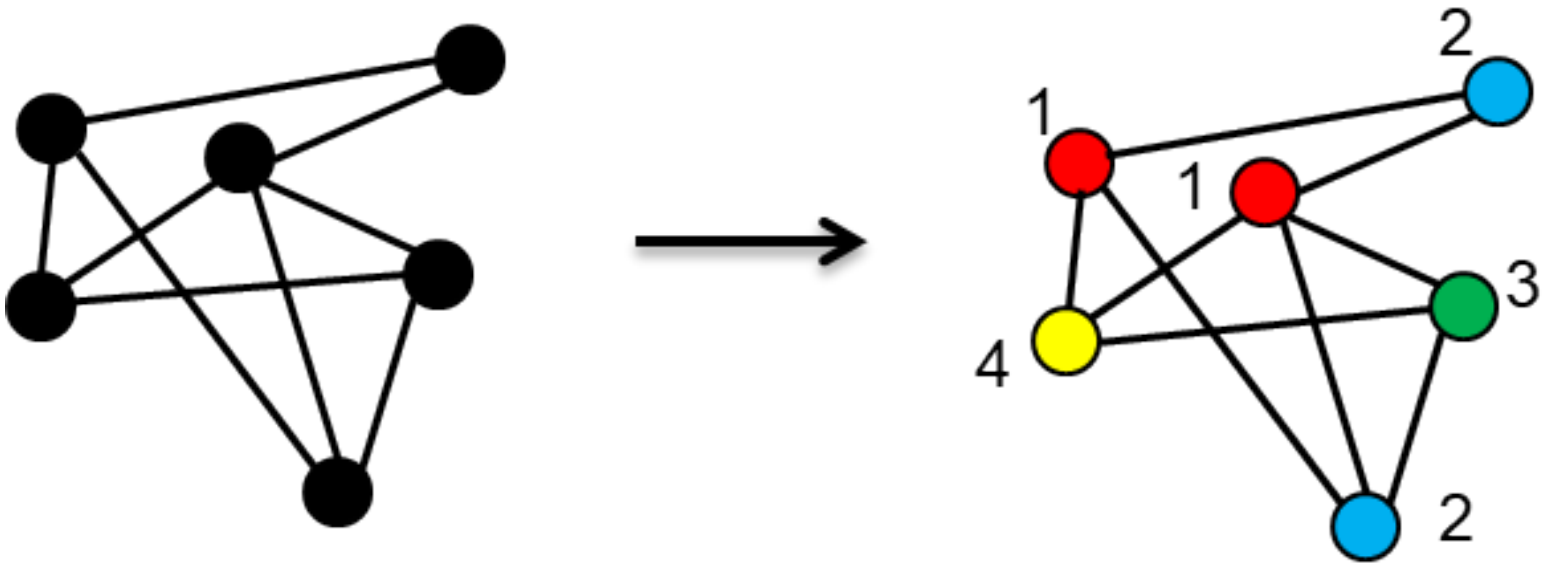


Figure 1: Vertex 4-coloring

- The coloring is proper if no adjacent vertices receive the same color.

Coloring and Multicoloring

- **Vertex k-multicoloring** of graph G is a function $\kappa : V(G) \to \mathcal{P}(\{1, ..., k\})$, where each vertex is colored with some subset of the set of k colors.

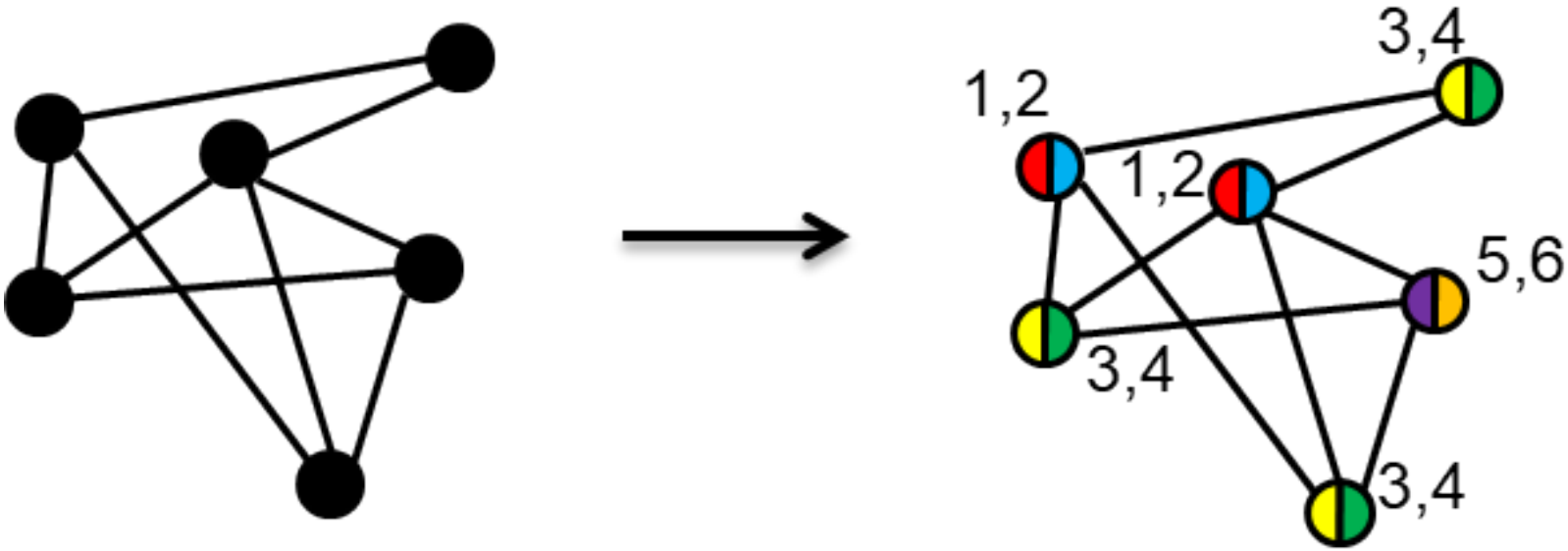


Figure 2: Vertex 6-multicoloring

Coloring and Multicoloring

- Coloring and multicoloring have various applications in scheduling, frequency allocations and timetabling.
- Many mathematicians have used different types of graph colorings to model and solve real-life situations and problems.
- Throughout the years, many different variations of coloring have been presented and studied, with many different conditions, for instance rainbow and anti-rainbow colorings of planar graphs, star colorings, list colorings...

Secret sharing

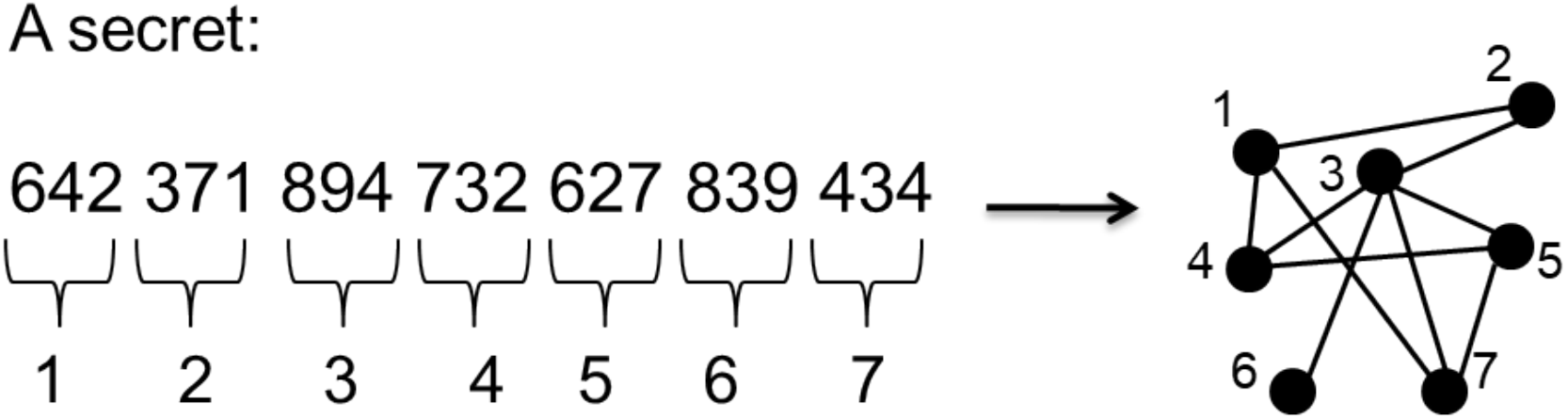
- Protecting secrets by dividing them into parts and distributing those parts to several persons or different locations

A secret:

64237189473262783943 4

Secret sharing

- Protecting secrets by dividing them into parts and distributing those parts to several persons or different locations.



Secret sharing

- How to make secret sharing safe from possible attackers?

Coloring the graph to secure a secret

- We represent parts of the secret by colors and color a graph in such a way that it is safe from the attackers.
- Depending on the attackers goals and behavior we define different kinds of coloring and explore its properties from the mathematical point of view.

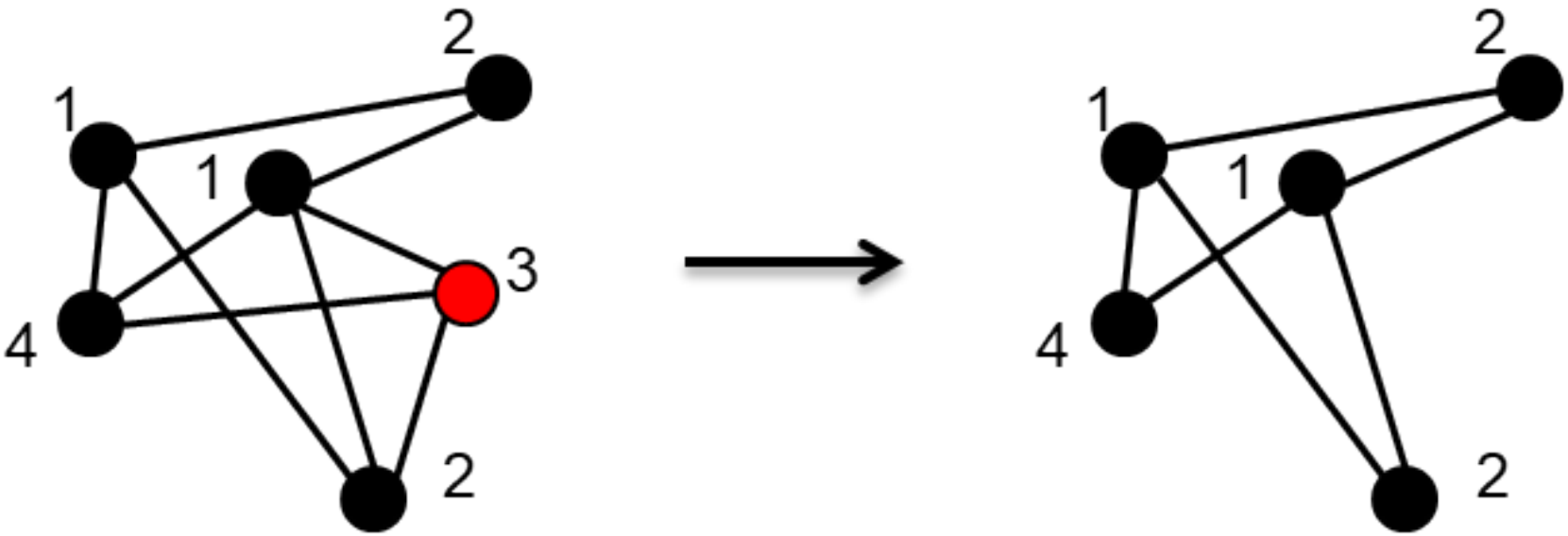
Two main problems in graph coloring:

- Determine the minimal number of colors needed for some kind of coloring - chromatic number.
- Analyze what families of graphs are colorable in some specific way.

Safe 3-coloring of graphs

The assumptions:

- Parts of the secret are distributed to graph vertices as colors and some number of vertices are the attackers
- The attacker's goal is to collect all parts of the secret or to disable the rest of the group from reading the secret
- The group is able to read the secret if there is a component with all parts, after the attacker vertices leave the graph



Safe 3-coloring of graphs

Definition

An a-**safe** k-**coloring** is a function $\phi : V(G) \to \{1, 2, ..., k\}$ such that for each subset $A \subset V(G)$, where $|A| = a$ it holds

1. $\bigcup_{u \in A} \phi(u) \neq \{1, ..., k\}$;
2. There is a component H of graph $G \backslash A$ such that

$$\bigcup_{u \in V(H)} \phi(u) = \{1, ..., k\}.$$

If some a-safe k-coloring exist for graph G we say that G is a-**safely** k-**colorable**.

Safe 3-coloring of graphs

- From condition 1. it follows $a \leq k-1$ so when $a = k-1$ we will call an a-safe k-coloring simply a **safe k-coloring**.

Question: **What are the graphs that allow a safe k-coloring?**

We explored that question for $k = 3$ and $\delta \geq 3$.

Safe 3-coloring of graphs

Theorem

Graph G with $\delta \geq 3$ is safely 3-colorable if at least one of the following stands:
i) G has at least three components;
ii) G has two components with at least 6 vertices each;
iii) G has at least one component with at least 9 vertices which is different from a double windmill.

Safe 3-coloring of graphs

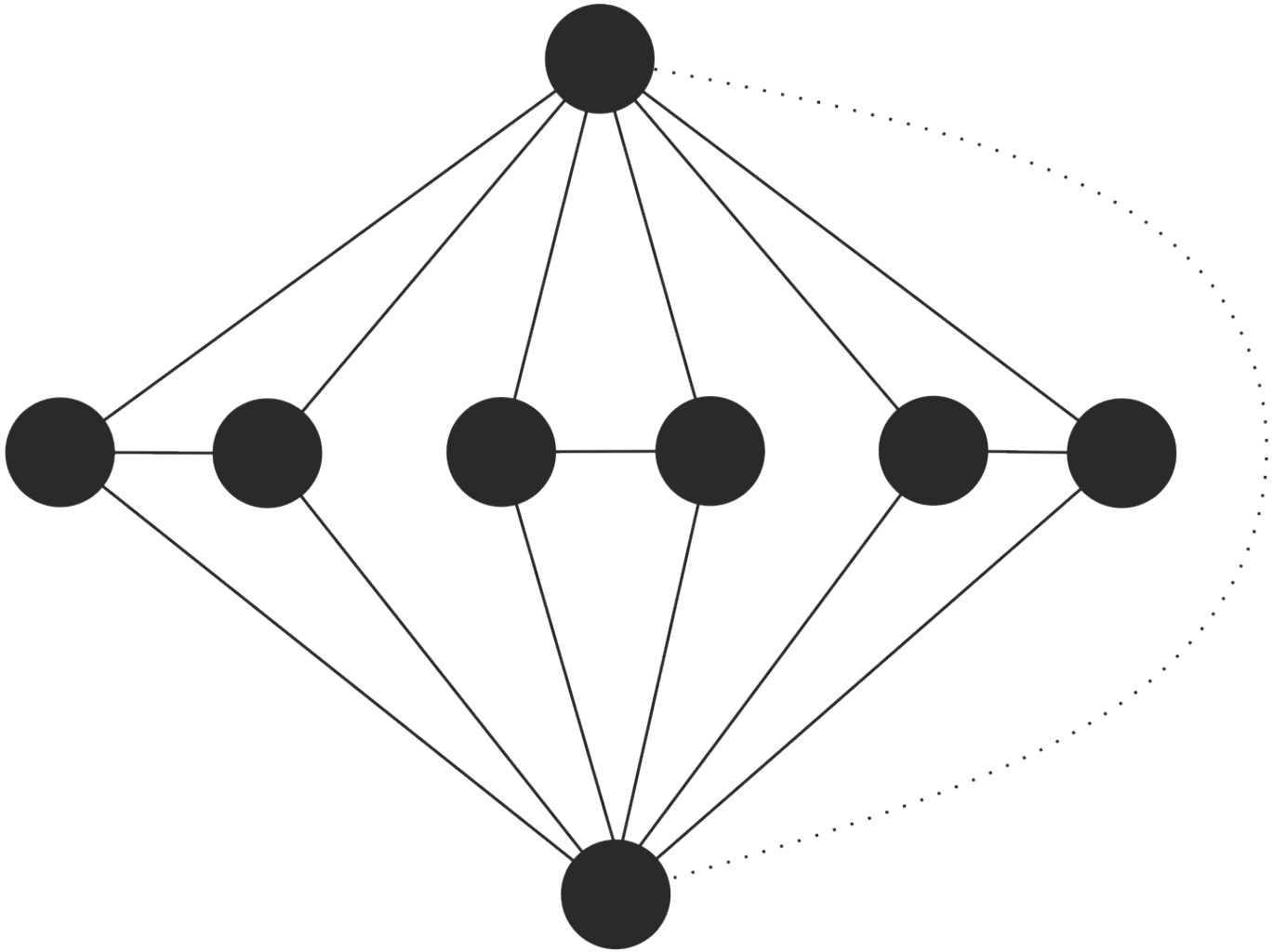
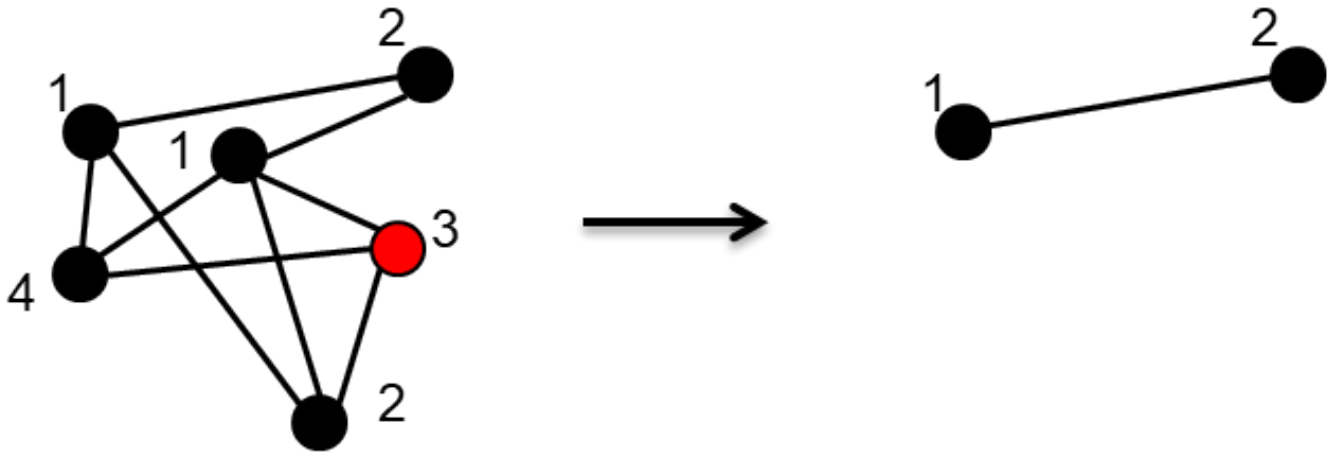


Figure 3: A double windmill

Highly a-resistant vertex k-multicoloring

The assumptions:

- When the attacker vertices are removed from the graph their neighboring vertices are also removed
- The attacker's goal is to collect all parts of the secret or to disable the rest of the group from reading the secret
- The group is able to read the secret if there is a component with all parts, after the attacker vertices leave the graph



Highly a-resistant vertex k-multicoloring

Definition

Let $a \in \mathbb{N}$. Vertex k-multicoloring of a graph G is called a-**resistant vertex** k-**multicoloring** if the following holds:
For each $A \subseteq V(G)$ with a vertices, there is a component H of the graph $G \backslash M_G(A)$ such that

$$\bigcup_{u \in V(H)} \kappa(u) = \{1, ..., k\}.$$

a-resistant vertex k-multicoloring is called **highly** a-**resistant vertex** k-**multicoloring** if for each $A \subseteq V(G)$ with a vertices it holds that

$$\bigcup_{u \in A} \kappa(u) \neq \{1, ..., k\}.$$

Highly a-resistant vertex k-multicoloring

What is the minimal number of vertices a graph must have in order to have a highly a-resistant vertex multicoloring, for a fixed a, and what is the minimal number of colors needed for coloring of such a graph?

We answered these questions for $a = 1, 2, 3, 4$.

Highly a-resistant vertex k-multicoloring

a	number of vertices n	minimal number of colors
1	≥ 4	2
2	≥ 9	3
3	14,15	7
3	≥ 16	4
4	21	10

Highly a-resistant vertex k-multicoloring

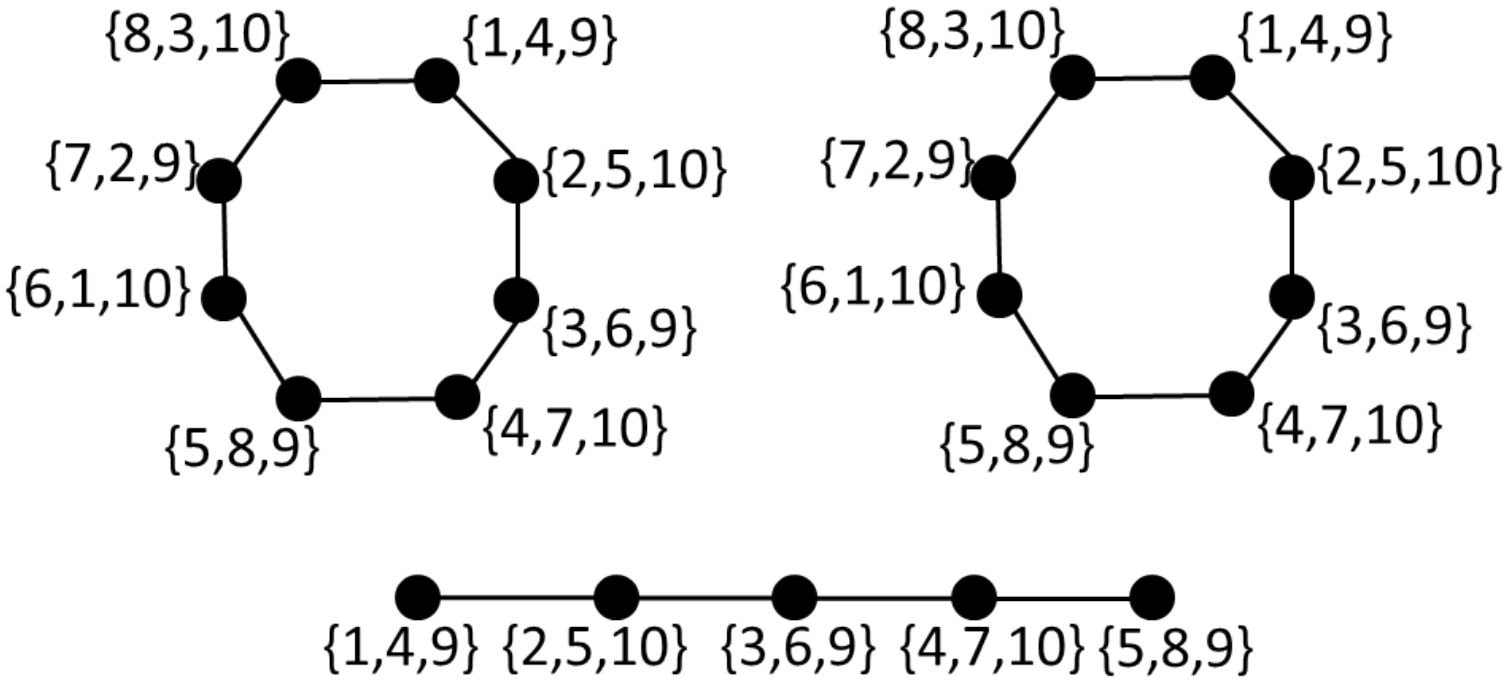


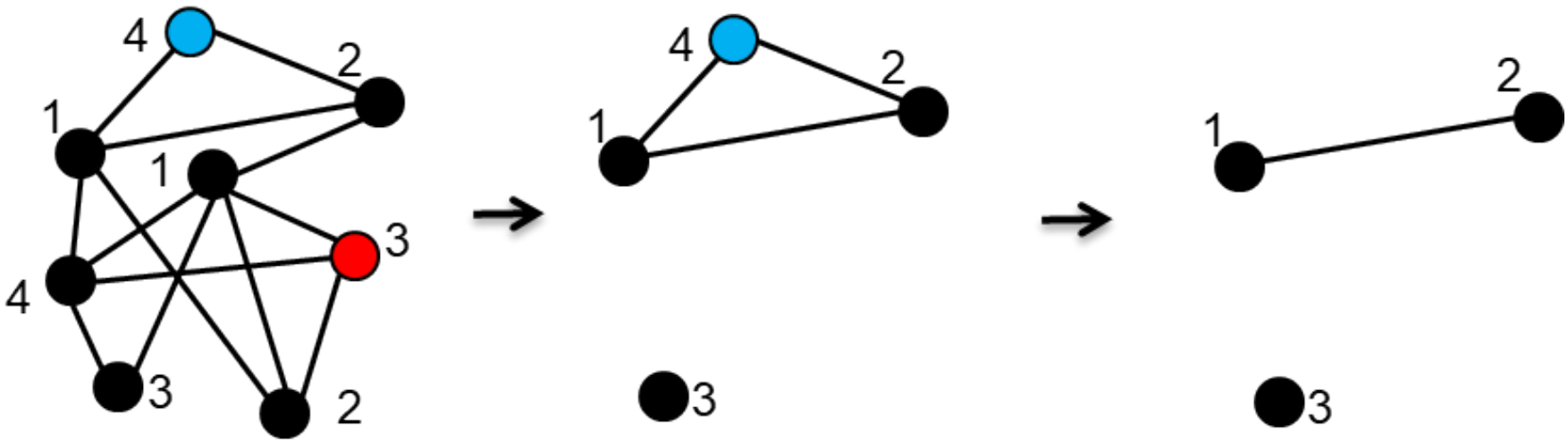
Figure 4: A graph G with 21 vertices and a highly 4-resistant vertex 10-multicoloring

Two types of attackers

The assumptions:

- There are two types of attackers, the ones that want to steal the secret or disable the rest of the group from reading the secret and the ones who are just removed from the graph (malfunctioning nodes)
- When the first type attacker vertices are removed from the graph their neighboring vertices are also removed

- There are a attackers and m disabled nodes



Two types of attackers

What is the minimal number of vertices a graph must have in order to have a highly (a, m)-resistant vertex multicoloring, for a fixed a and m, and what is the minimal number of colors needed for coloring of such a graph?

We answered these questions for pairs

$$(1, m), m \in \mathbb{N};$$

$$(2, 1), (2, 2), (2, 3);$$

$$(3, 1).$$

Two types of attackers

a	m	number of vertices n	minimal number of colors
1	m	$> 2 + m + \sqrt{4m+1}$	$\lfloor \frac{1}{2}(n-m-\sqrt{n^2+m^2-4n-2mn+4}) \rfloor + 1$
2	1	≥ 12	3
2	2	15	3
2	3	16, 17	6
2	3	≥ 18	3
3	1	18,19	6 or 7
3	1	≥ 20	4

Two types of attackers

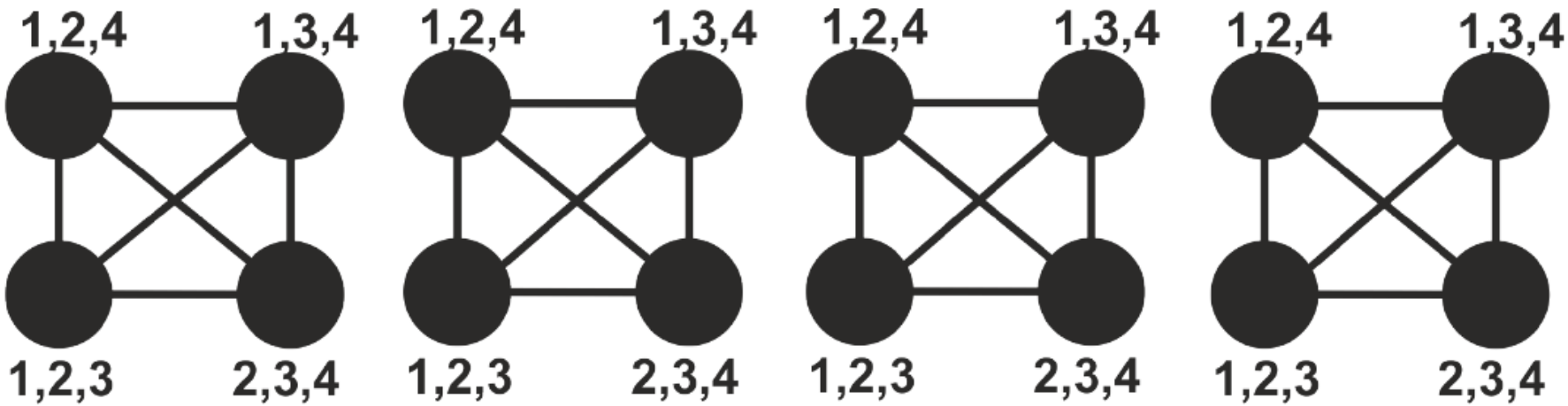


Figure 5: A graph G with 16 vertices and a highly $(1, 8)$-resistant vertex 4-multicoloring

Further work

- Generalize the results for two types of attackers for any $(a, m) \in \mathbb{N}$
- Solve the open problem of $a = 3$, $m = 1$, $n = 18, 19$, is the minimal number of colors 6 or 7
- Analyze families of graphs that admit a highly resistant coloring for different parameters
- Analyze families of graphs that admit a safe coloring for number of colors different from 3

Further work

Thank you for your attention!