Positional and Detection Games

Dissertation
zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Christian-Albrechts-Universität zu Kiel

vorgelegt von
Christian Glazik
Kiel, 2019

unter der Betreuung von
Prof.Dr. Anand Srivastav

Die Disputation fand am 23.10.2019 statt.

Doktorvater:	Prof. Dr. Anand Srivastav
Zweitgutachter:	Prof. Dr. Anusch Taraz
Drittgutachterin:	Dr. Małgorzata Bednarska-Bzdęga

Danksagung

Ohne die Unterstützung zahlreicher Personen hätte die vorliegende Arbeit niemals in dieser Form umgesetzt werden können.

An erster Stelle möchte ich meinem Doktorvater Prof. Dr. Srivastav für seine Begleitung und Unterstützung während meiner Forschungsarbeit danken.

Małgorzata Bednarska-Bzdęga habe ich zu verdanken, dass das Maker-Breaker Dreieckspiel seinen Weg in diese Arbeit gefunden hat. Für die inhaltliche Ausrichtung und produktive Zusammenarbeit bei den Themen Mastermind und Vertex-Destruction danke ich Gerold Jäger und Lasse Kliemann. Mein besonderer Dank gilt Jan Schiemann, ohne den viele gute Ideen nie entstanden und viele schlechte Ideen nicht so schnell verworfen worden wären. Auch allen anderen Mitgliedern der Arbeitsgruppe danke ich für die vielfältige Unterstützung.

Vielen Dank auch an Hannes und Basti, die sich die Zeit genommen haben, die Arbeit auf Form und Verständlichkeit zu überprüfen.

Natürlich danke ich auch meiner Familie, die mich immer unterstützt und durchgefüttert hat, bis ich auf eigenen Beinen stehen konnte und es auch weiterhin tut.

Meiner wundervollen Frau Lisa danke ich für ihre Geduld und ihre Ermutigungen; ohne sie wäre diese Arbeit vielleicht niemals fertig geworden.

Schließlich danke ich Gott, ohne den alles sinnlos wäre.

Contents

Deutsche Zusammenfassung

Das Thema dieser Arbeit sind neue Strategien für verschiedene kombinatotische Spiele.

In Kapitel 2 geht es um Positionsspiele auf Graphen. Beim sogenannten Maker-Breaker Dreiecksspiel wählen zwei Spieler, Maker und Breaker, abwechselnd Kanten eines vollständigen Graphen auf n Knoten. Maker gewinnt, falls er mit seinen Kanten ein Dreieck bilden kann, ansonsten gewinnt Breaker. Dabei wählt Maker jede Runde nur eine Kante, während Breaker q Kanten wählen darf. Ein klassisches Resultat von Chvátal und Erdős [12] besagt, dass Maker dieses Spiel gewinnt, falls $q \leq \sqrt{2n}$ und dass Breaker für $q \geq 2\sqrt{n}$ gewinnt. Seit über vierzig Jahren konnte diese Lücke nicht wesentlich verkleinert werden. Die einzige Verbesserung gelang Balogh und Samotij [5], die mit probabilistischen Argumenten zeigen, dass Breaker für $q \geq 1.935\sqrt{n}$ das Spiel gewinnen kann. Wir verbessern diese Schranke, indem wir eine neue Breaker-Strategie präsentieren, die für alle $q \geq \sqrt{(8/3+\epsilon)n}, \epsilon > 0$, also für $q \geq 1.633\sqrt{n}$ zu einem Sieg führt, falls n ausreichend groß ist. Dazu definieren wir eine Potentialfunktion und erlauben im Gegensatz zum gängigen Ansatz auch eine zwischenzeitliche Steigerung des Gesamtpotentials. Dieser Ansatz erfordert eine neue und verallgemeinerte Form der Analyse, mit deren Hilfe wir zeigen, dass trotz kurzzeitiger Steigungen des Potentials das Gesamtpotential niemals ein vorgegebenes kritisches Level überschreitet.

Kapitel 3 beschäftigt sich mit Varianten des Brettspiels Mastermind, bei dem ein Spieler sich einen geheimen Farbcode ausdenkt und der andere Spieler versucht, diesen in möglichst wenigen Spielrunden zu erraten. Dazu konstruiert er in jeder Runde selbst einen Farbcode, eine sogenannte Frage, und erhält vom anderen Spieler eine Rückmeldung zu den Übereinstimmungen zum geheimen Code. Bei der statischen Spielvariante muss der ratende Spieler zunächst alle seine Fragen stellen und erhält erst danach alle zugehörigen Rückmeldungen. Kann er mithilfe dieser den geheimen Code identifizieren, hat er gewonnen, ansonsten gewinnt sein Gegner. Unser Hauptresultat ist eine Strategie für statisches Permutations-Mastermind, bei der jede Farbe genau einmal im Code vorkommt. Eine Gewinnstrategie für dieses Spiel war bislang nicht bekannt. Die von uns präsentierte Strategie benötigt $\mathcal{O}(n^{1.525})$ Fragerunden bei einer Codelänge von n.

In Kapitel 4 werden Netzwerke von vielen Spielern auf ihre Stabiltät hin untersucht. Bei dem von uns betrachteten Modell sind die n Spieler die Knoten eines festgelegten zusammenhängenden Graphen. Ziel der Spieler ist es, nach der Entfernung eines Knotens aus dem Netzwerk noch mit möglichst vielen anderen Spielern verbunden zu sein. Dabei wird der zu entfernende Knoten immer so gewählt, dass der insgesamt entstehende Schaden (soziale Kosten) maximal wird (Extreme Vertex Destruction). Jeder Spieler hat zuvor die Möglichkeit, seine Position im Netzwerk zu verändern. Wir untersuchen dieses Modell auf Nash-Gleichgewichte, die in diesem Modell auch Swap-Equilibria genannt werden. Wir zeigen, dass Bäume sowie Graphen, bei denen es einen eindeutigen Knoten mit maximalem Schaden gibt, bis auf wenige Ausnahmen niemals Nash-Gleichgewichte sind und beweisen damit eine Vermutung von Kliemann et al. [23].

Introduction

When it comes to the interaction of two ore more parties with individual aims, it's all about finding an appropriate strategy. In most cases, the individual aim boils down to detection of information about the general situation or about your opponents and improvement of your own position. This goal becomes most clear and specific in the field of recreational games. In games like chess or tic-tac-toe, every player has complete information and the player's position decides over win and loss. On the contrary, in games like poker every player tries to find out the value of the other players' hands to play accordingly. This uncertainty of the opponent's hand is the factor that makes the game interesting. Since all results of this thesis are connected to the field of game theory, it seems important to mention that this research field is not about having fun with different kinds of games, but, in the contrary, it's about analysis of these games. The crucial difference between casual games and formal combinatorial games is that a combinatorial game is always assumed to be played by two players of infinite computational power. If the considered game is of complete information, the outcome of the game is already determined before it even started. The variety of games that are analyzed in this work ranges from popular recreational games as Mastermind over network-formation games to purely abstract games on graphs or hypergraphs.

Chapter 2 is dedicated to the field of Maker-Breaker games. In the so-called triangle game, two players alternately claim edges of a graph. While the first player tries to build a triangle, the second player tries to prevent him from doing so. The question which player wins this game under which circumstances is one of the oldest and most famous problems in the field of Maker-Breaker games. We present a Breaker-strategy that noticeably improves the former lower bound of Breaker-edges per turn for a Breaker's win.

In Chapter 3 we study the so-called static variant of the famous two player board game Mastermind where one player makes up a secret code and the other player tries to find out this codes by asking as few questions as possible. We present new upper and lower bounds on the number of questions needed in this variant, followed by a much more general lower bound that also applies to several non-static versions of the game.

In Chapter 4 the focus lies on structural properties of networks with many players rather than on individual strategies. We investigate on a certain kind of network formation game, where many players are part of a big network, modeled by a graph, and have certain options to change their individual position in this network by swapping an incident edge. We give some characterizations for swap equilibria in this model, i.e., stable networks, in which none of the players is able to improve his individual position.

Chapter 1

Introduction

In the following, we give a brief overview over the different research fields that are considered in this thesis, emphasizing our new techniques and results.

1.1 The Maker-Breaker game

Chapter 2 is about positional games on graphs. In a Maker-Breaker game, two players, called Maker and Breaker, play on the complete graph $K_n, n \in \mathbb{N}$. They alternately claim unclaimed edges of the graph. Maker wins if he can claim all edges of a certain structure, otherwise Breaker wins. In this thesis we consider one of the most famous Maker-Breaker games, namely the triangle game, in which Maker tries to build a triangle, while Breaker tries to prevent this. Both players are assumed to play perfectly, so the outcome of the game is determined from the beginning. If Maker and Breaker alternately claim one edge of the graph, the game clearly is a Maker's win, so instead Breaker is allowed to claim q edges per turn for some $q \in \mathbb{N}$ that can also depend on n. The question now is for the smallest value q^*, so that for $q = q^*$ the game is a Breaker's win. In their classic paper from 1978, Chvátal and Erdős [12] prove that $1.414\sqrt{n} < q^* < 2\sqrt{n}$ by presenting appropriate winning strategies for Maker and Breaker. Until then, the closing of this gap remained a famous open problem. The only improvement to this bounds was made by Balogh and Samotij [5], who used probabilistic arguments to prove the existence of a winning strategy for Breaker if $q \geq 1.935\sqrt{n}$. In this work we present a new and efficiently computable strategy for Breaker that works for all $q \geq \sqrt{(8/3+\epsilon)n}$ with $\epsilon > 0$ arbitrary small. Thereby, we push the upper bound to $q^* < 1.633\sqrt{n}$.

The main idea is the use of a *potential function* defined on the set of nodes. Each node is assigned a potential based on the ratio of incident Maker- and Breaker-edges, also accounting the additional Breaker-edges necessary to close all Maker-paths of length 2. Breaker's strategy basically is to keep the total potential (i.e. the sum over all nodes' potentials) as small as possible. In contrast to standard potential-based techniques, in our case the total potential may also increase during the game. That is why we use a more general approach that allows so called *critical turns*, i.e. turns, in which the total potential may increase. The technical challenge in the strategy analysis is to prove that

before a fixed number of critical turns occurs, we always obtain a decrease of the total potential that compensates all eventual increase, so that the total potential is always kept under a critical level. This way, Maker can be prevented from building a star of big size, which makes sure that Breaker always has enough edges to close all Maker-paths of length 2 and thereby prevent him from building a triangle.

1.2 The Mastermind Game

In Chapter 3 we consider the black-peg Mastermind game, which is a two player board game, defined as follows. One player, called Codemaker, makes up a secret code consisting of p pegs. Each of the pegs has one of c colors ($p, c \in \mathbb{N}$). The other player, called Codebreaker, tries to find out this code in as few turns as possible. To this end he asks *questions*, each of them also being a sequence of p colored pegs. As an answer he receives the number of pegs that have the same color as in the secret code. A common variation of the game is the AB-Game, in which every sequence contains every color at most once (implying $c \geq p$). If additionally $p = c$, we write $n := p = c$ and talk of *permutation Mastermind*, because the secret code and every question are permutations of the set $\{1, \ldots, n\}$. In the *static* variant of the game, Codebreaker has to ask all of his questions at once, then receives all answers and has to determine the secret code. While there are several results for both the AB-Game and the static variant concerning the number of turns needed by Codebreaker in the worst case, until now no progress has been made for the combination of both variations.

In this work we prove a first upper bound for static black-peg permutation Mastermind by presenting a strategy that uses $\mathcal{O}(n^{1.525})$ questions. We start with a rather intuitive strategy, only consisting of transpositions and 3-cycles that are used to find out the colors of fixed pegs or positions of fixed colors. This strategy on it's own could be used to determine the secret code in $\Theta(n^2)$ questions. In a next step we introduce the term of *separation*, saying that a strategy separates a pair (X, Y) of permutations if at least one question from the strategy leads to different answers concerning X and Y. A successful strategy has to separate all possible pairs of permutations. We split this problem into two parts that we handle in different ways: For separating pairs of secrets with a low Hamming distance, we present an explicit strategy that is based on certain arithmetic progressions and only works if n is a prime number. For a general integer n, we may need up to $\mathcal{O}(n^{1.525})$ questions to find out enough positions and colors, so that only a prime number is left. The separating strategy then comes along with $\mathcal{O}(n^{1.5})$ questions. For pairs of secrets with high Hamming distance, we reduce the problem to a vertex cover problem on a hypergraph with large hyperedges. By applying a greedy algorithm, we can guarantee a solution of size $\mathcal{O}(n^{1.5} \log(n))$, which translates to a strategy of equal size. Since the constructed hypergraph has exponential size, this strategy is not efficiently computable. On the lower bound side, we use an information theoretical technique from Doerr et al. [13] to show that every feasible strategy for the static permutation game needs $\Omega(n \log(n))$ questions. Moreover, we introduce a new technique to prove a worst-case lower bound of c questions for the general (non-static)

Mastermind game that holds even if the secret code contains every color at most once, while the questions are not restricted. We simulate the worst case by allowing Codemaker to change the secret code in every turn, provided that old answers stay correct. By always choosing a secret that leads to the smallest possible answer, Codemaker can enforce the game to last at least c turns.

1.3 The Vertex Destruction game

Chapter 4 is about network formation games. In the standard network formation model, we consider a given network of n players that is modeled by a graph. Every player is represented by a vertex in the graph and the relations between players are represented by edges. In this work we investigate the *vertex destruction model*, where one vertex in the graph will be chosen by a given probability distribution and then will be destroyed, i.e., all of his incident edges will be deleted. The aim of every vertex is to stay connected to as many other vertices as possible after this deletion. For this sake, before the deletion takes place, he is allowed perform an *edge swap*, i.e., to delete one of his incident edges and create a new incident edge instead, providing the graph stays connected. This swap may not only change the individual position of the vertex in the graph, but may also influence the choice of the deleted vertex, because the underlying distribution is allowed to depend on the given network. In the *extreme destruction model*, the vertex to be destroyed is chosen uniformly at random from all *max-sep vertices*, i.e., those vertices whose destruction causes a maximum number of vertex pairs to be separated. We ask for *swap equilibria* (SE) in this model, i.e. graphs, in which none of the vertices can improve its position by swapping one of its incident edges. In this work we present two main results on swap equilibria under the extreme vertex destruction model. First we prove that apart from the path of length 3, there exists no SE tree with more than one max-sep vertex. We use the fact that every tree contains a 'central' vertex with relatively high separation to show that in every SE tree with at least two max-sep vertices a deletion of a max-sep vertex can never create a connected component of size $2n/3$ or bigger. We introduce the term of a *boundary vertex*, describing a max-sep vertex that, if deleted, leaves all other max-sep vertices connected. Finally, we are able to show that in a SE tree every max-sep vertex is a boundary vertex and is always able to improve its situation by a swap, unless the graph is a path of length 3.

In our second result we show that the only SE graphs with only one max-sep vertex are paths of length 2 or 4. Together with the first result this implies that all SE trees are small paths, proving a conjecture of Kliemann et al. [23]. The main idea is that vertices on a cycle often can expand this cycle so that it contains the max-sep vertex. If such a swap is not profitable, this leads to strong restrictions to the graph structure. We show that if the graph contains a cycle, the deletion of the max-sep vertex creates only two components, one of them being a tree while the other one doesn't contain any leaf. But even then, a vertex from the second component is able to perform a profitable cycle expansion, leading to a contradiction.

Chapter 2

The Maker-Breaker Game

2.1 Introduction

This chapter is based on a paper published in 2018 [18]. Maker-Breaker games belong to the family of positional games. For a detailed overview of these kind of games we refer to [19] or [30]. Consider a (usually finite) universe U and a family $\mathcal{W}$ of finite subsets $A \subseteq U$ called *winning sets*. The tuple $(U, \mathcal{W})$ is called the *game hypergraph*. Two players iteratively claim free elements from U. The player who is first to claim all elements of a winning set wins the game. If all elements are claimed by either of the players and no winning set was completely claimed by one player, the game is a draw. This kind of game is called *strong game* and probably is the most natural type of game, appearing in many casual games played by human players, as tic-tac-toe or Hex. Obviously, there are three distinct possible outcomes of the game: first player's win, second player's win and draw. In fact, every strong game will either end with first player's win or with a draw. This can be shown with the quite simple argument of *strategy stealing*: Assume for a moment that the second player has a winning strategy for the game. Then, the first player can claim some arbitrary element of U in his first move, ignore this element and then pretend to be the second player, copying the winning strategy. Whenever he can't follow the strategy because the next element to be claimed is an already claimed and ignored element, he may claim an arbitrary unclaimed element instead and ignore it. Following this strategy, first player will always win the game, hence the second player cannot have a winning strategy.

The fact that the second player has no chance to win, motivates a new kind of positional game: In a *Maker-Breaker game*, the first player, called *Maker*, still tries to claim all elements of a winning set, whereas the second player, called *Breaker*, wins the game if and only if after all elements are claimed, Maker didn't manage to claim a complete winning set. A very natural game universe is the set of edges of the complete graph $K_n, n \in \mathbb{N}$. Maker and Breaker iteratively claim edges from the graph K_n and while Maker tries to construct a certain structure (e.g. a spanning tree, a big star or a Hamiltonian cycle), Breaker tries to prevent this. These kind of games have been studied extensively by Beck [6, 7, 8]. Since many of them are a clear Maker's win, it

seems appropriate to modify the rules of the game, so that for every edge claimed by Maker, Breaker is allowed to claim q edges for some $q \in \mathbb{N}$. The bigger q is, the more power Breaker has to prevent Maker from building a winning structure. This gives rise to the question of an exact threshold bias $q^* := q^*(n)$ such that the game is a Maker's win for $q \leq q^*$ and a Breaker's win for $q > q^*$.

We want to emphasize two very general and useful results in this area:

Theorem 2.1 (Beck's Theorem [7])**.** *If*

$$\sum_{A \in \mathcal{W}} (1+q)^{-|A|} < \frac{1}{1+q},$$

then Breaker has a winning strategy for the corresponding Maker-Breaker game.

Note that this result does hold for arbitrary Maker-Breaker games played on an arbitrary finite universe, not only on graphs. The proof uses the crucial concept of a *potential function* and can be found in Section 2.6. Beck also presented a complementary winning criterion for Maker. The following result was proved by Bednarska and Łuczak and concentrates on a certain type of Maker-Breaker game. It was recently generalized for hypergraphs by Kusch et al. [31]. Given a fixed graph G and integers q and n, the game $(G; n, q)$ is the Maker-Breaker game played on the complete graph K_n, where Maker and Breaker alternately claim 1 and q edges, respectively. Maker wins if he can construct a copy of G and otherwise Breaker wins. Denote by $v(G)$ the number of nodes of G and by $e(G)$ the number of its edges.

Theorem 2.2 (Bednarska and Łuczak [9])**.** *Let G be a graph with at least two edges and define*

$$m(G) := \max\left\{\frac{e(H)-1}{v(H)-2} : H \subseteq G \text{ with } v(H) \geq 3\right\}.$$

Then there exist constants c_0, C_0 and n_0 such that for every $n \geq n_0$ the following holds.

(i) If $q \leq c_0 n^{1/m(G)}$, then the game $(G; n, q)$ is a Maker's win.

(ii) If $q \geq C_0 n^{1/m(G)}$, then the game $(G; n, q)$ is a Breaker's win.

This determines the asymptotic order of the threshold bias for a big family of games and gives rise to the question of the exact leading constant: Bednarska and Łuczak conjectured that c_0 and C_0 can be chosen arbitrarily close to each other. Until now, the exact leading constant is unknown for any Graph G containing a cycle. In fact, even the existence of such a constant couldn't be proved. In this chapter we will deal with the simplest of these problematic cases, namely the game $(K_3; n, q)$, where Maker tries to construct a triangle, while Breaker tries to prevent this (see Figure 2.1). This *triangle game* is one of the oldest and most famous Maker-Breaker games and was formulated by Chvátal and Erdős [12]. When introducing the problem, they also presented a winning strategy for Maker if $q < \sqrt{2n+2} - 5/2 \approx 1.414\sqrt{n}$ and a winning strategy for Breaker if $q \geq 2\sqrt{n}$. Both strategies are quite simple and will be dealt with in the next subsection.

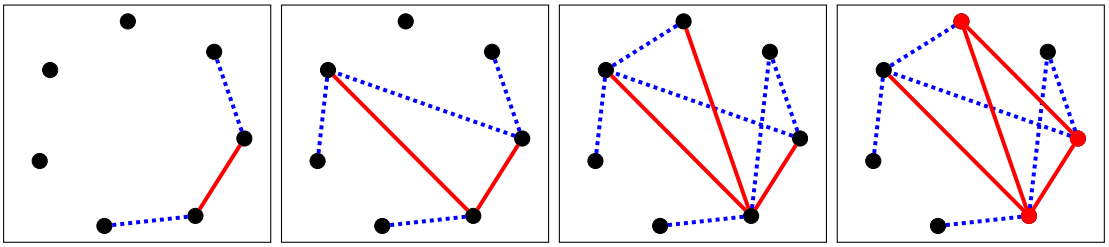

Figure 2.1: The triangle game with $n = 7$ and $q = 2$ is a Maker's win. Maker-edges are red, Breaker-edges blue.

These upper and lower bound could not be improved for a long time. In 2011, Balogh and Samotij [5] used probabilistic arguments to prove that for $q \geq 1.935\sqrt{n}$ the triangle game is a Breaker's win. In this chapter we present a new and efficiently computable winning strategy for Breaker if n is sufficiently large and $q \geq \sqrt{(8/3+\epsilon)n} \approx 1.633\sqrt{n}$.

2.1.1 Two simple strategies

In this subsection we present the strategies proposed by Chvátal and Erdős [12]. Although they are quite simple, they already give useful insights to the special mechanics of the triangle game.

Strategy 1. *This is a Maker's winning strategy for the case $q < \sqrt{2n - 7/4} - 3/2$ (note that Chvátal and Erdős assumed that Breaker starts the game, leading to the similar bound of $q < \sqrt{2n+2} - 5/2$). Maker fixes an arbitrary node v and then in every turn does the following:*

- *If there are nodes u, w such that Maker already owns the edges $\{v, u\}$ and $\{v, w\}$ and the edge $\{u, w\}$ is still free, Maker claims $\{u, w\}$.*
- *Otherwise, Maker claims an arbitrary edge incident in v.*

Assume that Maker doesn't win with this strategy. This means that there exists $t \in \mathbb{N}$ such that after the t-th turn there are no more unclaimed edges incident in v and Maker never had the chance to close a path of length 2 as described in the first step. Hence, Maker claimed all of his t edges incident in v. This implies that Breaker claimed the remaining $n - 1 - t$ edges incident in v and additionally closed all Maker-paths of length 2, for which he needs $t(t-1)/2$ additional edges. Because Breaker claimed q edges each turn, we get

$$n - 1 - t + t(t-1)/2 \leq qt.$$

A straightforward calculation shows that there is only a solution for this term if $q \geq \sqrt{2n - 7/4} - 3/2$.

Strategy 2. *This is a Breaker's winning strategy for the case $q \geq 2\sqrt{n}$. Suppose that q is even. Consider an arbitrary turn. Let $\{u, v\}$ be the edge that Maker claimed in this turn.*

- *Breaker uses at most $q/2$ edges incident in u and $q/2$ edges incident in v to close all Maker-paths of length 2.*
- *Then, Breaker claims his remaining edges such that in total he claimed $q/2$ edges incident in u and $q/2$ edges incident in v this turn. If there is no more unclaimed edge incident in u or v, he claims an arbitrary edge instead.*

It is obvious that if Breaker can play this strategy until the end of the game, he will win, since he always closes all Maker-paths of length 2 and Maker has no chance to complete a triangle. Hence, it suffices to show that $q/2$ edges incident in u and $q/2$ edges incident in v always suffice to close all Maker-paths. Because a Maker-edge $\{u, v\}$ leads to at most $\deg_M(u) + \deg_M(v)$ new paths of length 2, where $\deg_M(x)$ is the number of Maker-edges incident in vertex x (see Figure 2.2), it suffices to prove that all stars build by Maker have at most size $q/2$. So assume that Maker manages to construct a star of size $q/2 + 1$ and let v be the center node of the star that first reaches this size and let t be the corresponding turn. Before turn t, Breaker was able to play according to the strategy, which implies that for every Maker-edge incident in v he claimed $q/2$ edges incident in v. This is a total of $(q/2)^2 \geq n$ edges incident in v, a contradiction.

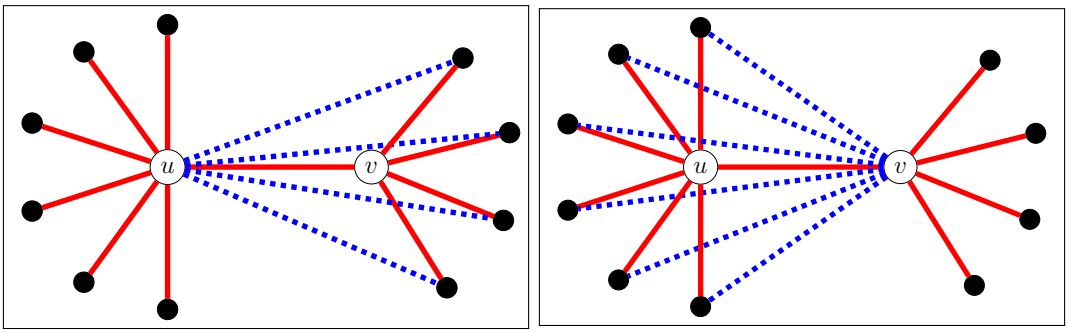

Figure 2.2: The Maker-edge $\{u, v\}$ enforces $\deg_M(v)$ Breaker-edges incident in u and $\deg_M(u)$ Breaker-edges incident in v.

2.1.2 Our Contribution

In our work we present a new deterministic strategy for Breaker that further improves the recent lower bound for Breaker's win to $q = \sqrt{(8/3 + o(1))n} \approx 1.633\sqrt{n}$, assuming n to be sufficiently large. The global idea of our strategy is as follows: Instead of claiming arbitrary edges incident in the nodes of the last edge claimed by Maker, as done in Strategy 2, Breaker claims only edges that connect the 'most dangerous' nodes, i.e., nodes that already have many incident Maker edges and rather few Breaker edges. Proceeding this way, Breaker needs fewer edges to prevent Maker from building a $q/2$-star. For the realization of this idea we use an (efficiently computable) *potential function* to decide which edges are most dangerous and should be claimed next to prevent Maker from building any triangle *or* big star. In contrast to Beck [7], our potential function

is defined directly on the set of nodes and not on the set of winning sets. However, the most significant difference to Beck and other previous potential-based approaches is that our potential function is not necessarily decreasing in every single turn. Some *critical* turns may occur in which the potential increases, so the challenge is to control the number and the impact of these critical turns. This new approach requires plenty of analytic work but turns out to be a more powerful technique than classic potential-based approaches and also might be of interest for other kinds of Maker-Breaker games.

2.2 Breaker's strategy

We start by introducing the potential function which forms the basis for Breaker's strategy. During the game, denote by M the Maker graph consisting of all edges claimed by Maker so far and let B denote the corresponding Breaker graph. For $v \in V$ and $H \in \{M, B\}$ let $\deg_H(v)$ denote the degree of v in H. For a turn t, $\deg_{H,t}(v)$ denotes the degree of v in H directly after turn t.

2.2.1 The potential function

Let $\epsilon^* > 0$ and $\beta = \frac{8}{3} + \epsilon^*$. In this chapter we consider the (n, q)-Triangle game with $q = \sqrt{\beta n}$. As mentioned in the introduction, for $\beta \geq 4$ there exist known winning strategies for Maker, so we will assume $\beta \leq 4$ if necessary. Fix $\delta \in (0, 1 - \frac{8}{3\beta})$.

Definition 2.3. *For every $v \in V$ define the* balance *of v as*

$$\mathrm{bal}(v) := \frac{8(n - \deg_B(v))}{q^2(1-\delta)(3+\delta) - 4\deg_M(v)(2q - \deg_M(v))}.$$

Moreover we define p_0 as the balance of a node in the very beginning of the game, i.e.

$$p_0 := \frac{8n}{q^2(1-\delta)(3+\delta)} = \frac{8}{\beta(1-\delta)(3+\delta)}.$$

The balance of a node is a measure of the ratio of Maker- and Breaker-edges incident in this node: The more Maker-edges and the fewer Breaker-edges incide in v, the bigger the balance value gets. A detailed interpretation of the balance value can be found in Section 2.2.2.

For the success of Breaker's strategy it is crucial that $p_0 < 1$ (e.g. for the choice of η in Section 2.3.3). This is assured by the next remark.

Remark 2.4. *It holds $\frac{8}{3\beta} < p_0 < \frac{8}{3\beta(1-\delta)} < 1$.*

Proof. The second and third inequality follow directly from $\delta \in (0, 1 - \frac{8}{3\beta})$. For the first inequality, note that $(1-\delta)(3+\delta) = 3 - 2\delta - \delta^2 < 3$, so we get $p_0 = \frac{8}{\beta(1-\delta)(3+\delta)} > \frac{8}{3\beta}$. □

During the game, Breaker will not be able to keep all nodes at their start balance. Some nodes will get more Breaker-edges than needed, others less. This *deficit* of a node will be used to define its potential.

Definition 2.5. *Consider the game at an arbitrary point of time. For a node $v \in V$ let* $\deg^*(v) \in \mathbb{R}$ *be the* balanced Breaker-degree *of this node, i.e. the Breaker-degree that would be necessary, so that* $\mathrm{bal}(v) = p_0$*. Formally we define*

$$\deg^*(v) := n - p_0 \left(\frac{q^2(1-\delta)(3+\delta)}{8} - \deg_M(v) \left(q - \frac{\deg_M(v)}{2} \right) \right).$$

The deficit *of v is defined by*

$$d(v) := \deg^*(v) - \deg_B(v).$$

Finally, let $\mu := 1 + \frac{6\beta \ln(n)}{\delta q}$. Define the potential *of v as*

$$\mathrm{pot}(v) := \begin{cases} 0 & \text{if } \deg_M(v) + \deg_B(v) = n - 1 \\ \mu^{d(v)/q} & \text{else} \end{cases}$$

and for an unclaimed edge $e = \{u, w\}$ define the potential *of e as* $\mathrm{pot}(e) := \mathrm{pot}(u) + \mathrm{pot}(w)$*. For every turn t we define* $\mathrm{pot}_t(v)$ *($\mathrm{pot}_t(e)$, resp.) as the potential of v (e, resp.) directly after turn t and* $\mathrm{pot}_0(v)$ *as the potential of v at the beginning of the game. Analogously we define* ${\deg^*}_t(v)$ *and* $d_t(v)$*. The* total potential *of a turn t is defined as* $\mathrm{POT}_t := \sum_{v \in V} \mathrm{pot}_t(v)$*. The* total starting potential *is defined as* $\mathrm{POT}_0 := \sum_{v \in V} \mathrm{pot}_0(v)$*.*

Lemma 2.6. *The total starting potential fulfills* $\mathrm{POT}_0 = n$*.*

Proof. Let $v \in V$ with $\deg_M(v) = \deg_B(v) = 0$. Then,

$$\deg^*(v) = n - p_0 \left(\frac{q^2(1-\delta)(3+\delta)}{8} \right) = n - p_0 \cdot n \cdot p_0^{-1} = 0.$$

This implies $\mathrm{pot}(v) = \mu^{d(v)/q} = \mu^{(\deg^*(v) - \deg_B(v))/q} = \mu^0 = 1$, so

$$\mathrm{POT}_0 = \sum_{v \in V} \mathrm{pot}_0(v) = \sum_{v \in V} 1 = n.$$

□

Breaker's aim is to keep the total potential as low as possible. The next lemma ensures that if Breaker can keep the potential of every single node below $2n$, he can prevent Maker from raising the Maker-degree of a node above $q/2$. We will later show (Theorem 2.10) that Breaker is even able to keep the *total* potential of the game below $2n$.

Lemma 2.7. *If n is sufficiently big, for every turn t and every node $v \in V$ the following holds:*

$$0 < \mathrm{pot}_t(v) \leq 2n \Rightarrow \deg_{M,t}(v) \neq \lceil q/2 \rceil - 1.$$

Proof. Let t be a turn and $v \in V$ with $\mathrm{pot}_t(v) > 0$ and $\deg_{M,t}(v) = \lceil q/2 \rceil - 1$. We show that $\mathrm{pot}_t(v) > 2n$. Because $\mathrm{pot}_t(v) \neq 0$, we have $\mathrm{pot}_t(v) = \mu^{d_t(v)/q}$. We claim (and later prove) that

$$d_t(v) \geq \frac{2\delta n}{3}. \tag{2.1}$$

This implies

$$\begin{aligned}\mathrm{pot}_t(v) = \mu^{d_t(v)/q} \geq \mu^{2\delta n/3q} &= \left(1 + \frac{6\beta \ln(n)}{\delta q}\right)^{2\delta n/3q} \\ &= \left(1 + \frac{6\beta \ln(n)}{\delta q}\right)^{\left(\frac{\delta q}{6\beta \ln(n)}+1\right)\left(\frac{\delta q}{6\beta \ln(n)}+1\right)^{-1}\frac{2\delta n}{3q}} \geq e^{\alpha},\end{aligned}$$

where

$$\alpha = \left(\frac{\delta q}{6\beta \ln(n)} + 1\right)^{-1} \frac{2\delta n}{3q} = \left(\frac{\delta q \mu}{6\beta \ln(n)}\right)^{-1} \frac{2\delta n}{3q} = \frac{4\beta n \ln(n)}{q^2 \mu} > 2\ln(n),$$

where for the last inequality we used that $\mu < 2$ if n is big enough. Finally we get $\mathrm{pot}_t(v) \geq e^{\alpha} > n^2$ and for $n \geq 2$ this is at least $2n$.

We still have to prove claim (2.1). Recall that $d_t(v) = \deg^*{}_t(v) - \deg_{B,t}(v)$. We estimate $\deg^*{}_t(v)$ as

$$\begin{aligned}\deg^*{}_t(v) &= n - p_0 \left(\frac{q^2(1-\delta)(3+\delta)}{8} - \deg_{M,t}(v)\left(q - \frac{\deg_{M,t}(v)}{2}\right)\right) \\ &\geq n - p_0 \left(\frac{q^2(1-\delta)(3+\delta)}{8} - \left(\frac{q}{2} - 1\right)\left(q - \frac{q}{4}\right)\right) \\ &= n + p_0 \left(q^2 \left(\frac{3 - (1-\delta)(3+\delta)}{8}\right) - \frac{3q}{4}\right) \\ &= n + p_0 \left(\frac{q^2\delta}{4} + q\Big(\underbrace{\frac{\delta^2 q}{8} - \frac{3}{4}}_{\geq 0 \text{ if } n \text{ suff. big}}\Big)\right) \\ &\geq n + \frac{p_0 \beta \delta n}{4} \geq n + \frac{2\delta n}{3}. \qquad \text{(Remark 2.4)}\end{aligned}$$

Therefore,

$$d_t(v) = \deg^*{}_t(v) - \deg_{B,t}(v) \geq n + \frac{2\delta n}{3} - n = \frac{2\delta n}{3}.$$

□

2.2.2 Intuition of the balance value

In the following we motivate the definition of the balance value of a node by giving an 'in-game'-example. Let $v \in V$ with $\deg_M(v) < \frac{q(1-\delta)}{2}$ and suppose that Maker decides

to concentrate on the node v, i.e., from this moment on he will claim all of his edges incident in v as long as there are unclaimed edges incident in v. Moreover suppose that Breaker's aim, besides closing all Maker-paths of length 2, is to keep $\deg_M(v)$ below $\frac{q(1-\delta)}{2}$. To achieve this, he must claim a certain number of edges incident in v himself. Denote this number by B_v. Let T denote the number of turns that Maker needs to raise $\deg_M(v)$ above $\left\lceil \frac{q(1-\delta)}{2} \right\rceil$. Then $B_{\text{total}} := Tb$ is the number of edges that Breaker can claim before $\deg_M(v) \geq \left\lceil \frac{q(1-\delta)}{2} \right\rceil$. But there is a certain number C of edges that Breaker has to claim at different places, not incident in v, to close new Maker-paths.

Setting $A := B_{\text{total}} - C$ as the number of available Breaker-edges, the term $\frac{B_v}{A}$ represents the fraction of *available* Breaker-edges necessary to prevent Maker from building a $q/2$-star. We will show that $\text{bal}(v)$ is an approximation of $\frac{B_v}{A}$, hence it is a measure for the 'danger' of v: The smaller $\frac{B_v}{A}$ is, the less attention Breaker has to spend to the node v. If $\frac{B_v}{A} > 1$, this means that Breaker cannot achieve his goal of keeping $\deg_M(v)$ below $q/2$.

For $f, g : \mathbb{N} \to \mathbb{R}$ we write $f \sim g$ if and only if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. We will close this subsection by showing that $\text{bal}(v) \sim \frac{B_v}{A'}$ for some $A' \leq A$. To prevent Maker from building a $\frac{q(1-\delta)}{2}$-star at v, at the end of the game Breaker must possess at least $n - \frac{q(1-\delta)}{2}$ edges incident in v. Hence, the number of edges still to claim is $B_v = n - \frac{q(1-\delta)}{2} - \deg_B(v) \sim n - \deg_B(v)$. Because Maker claims one edge per turn and concentrates on v, we get $T = \frac{q(1-\delta)}{2} - \deg_M(v)$ and $B_{\text{total}} = \frac{q^2(1-\delta)}{2} - q\deg_M(v)$. The exact value of C depends on the choices of Maker and on how many closing edges are already owned by Breaker. If we assume that all closing edges are previously unclaimed, we can upper bound C by

$$\begin{aligned} C' &:= \sum_{i=\deg_M(v)}^{\lceil q(1-\delta)/2 \rceil - 1} i \\ &= \frac{(\lceil q(1-\delta)/2 \rceil - 1) \cdot \lceil q(1-\delta)/2 \rceil}{2} - \frac{(\deg_M(v)+1)\deg_M(v)}{2} \\ &\sim \frac{q^2(1-\delta)^2}{8} - \frac{\deg_M(v)^2}{2}. \end{aligned}$$

Finally, for $A' := B_{\text{total}} - C' \leq A$ we get

$$\begin{aligned} \frac{B_v}{A'} &= \frac{B_v}{B_{\text{total}} - C'} \\ &\sim \frac{n - \deg_B(v)}{\frac{q^2(1-\delta)}{2} - q\deg_M(v) - \left(\frac{q^2(1-\delta)^2}{8} - \frac{\deg_M(v)^2}{2}\right)} \\ &= \frac{8(n - \deg_B(v))}{q^2(1-\delta)(3+\delta) - 4\deg_M(v)(2q - \deg_M(v))} = \text{bal}(v). \end{aligned}$$

2.2.3 The detailed strategy

As in Strategy 2, the basic idea is that Maker's task to build a triangle is closely related to the task of connecting big stars. Assume that at any time during the game Maker manages to build a path (u, v, w) of length 2. Then Breaker is forced to immediately *close* this path by claiming the edge $\{u, w\}$ if he doesn't already own this edge. So every sensible Breaker-strategy will follow the simple rule of immediately closing all Maker-paths of length 2. Hence, the only chance for Maker to win the game is to construct more than q paths of length 2 in a single turn, so that Breaker can't claim enough edges to close all of them immediately. By claiming an edge $\{u, v\}$, Maker is building $\deg_M(u) + \deg_M(v)$ new paths of length 2 (compare Figure 2.2). This implies that if Breaker at each turn closes all Maker-paths of length 2 and simultaneously manages to prevent Maker from building a $q/2$-star, he will win the game.

Strategy 3. *Consider an arbitrary turn t. Let $e_M = \{u, v\}$ be the edge claimed by Maker in this turn. Breaker's moves for this turn are split into two parts.*

Part 1: closing paths. *Breaker claims $\deg_{M,t-1}(v)$ edges incident in u and $\deg_{M,t-1}(u)$ edges incident in v to close all new Maker-paths of length 2. If such a path is already closed, he claims an arbitrary edge incident in u (v, resp.) instead. If all edges incident in u (v, resp.) are already claimed, we call the turn t an* isolation turn. *In this case, Breaker claims arbitrary unclaimed edges instead. We call the edges claimed during Part 1* closing edges. *u (v, resp.) is called the* head *of the closing edge, whereas the corresponding second node of the edge is called its* tail.

Part 2: free edges. *If after part 1 Breaker still has edges left to claim (we will later show that this is always the case), he iteratively claims an edge e with $\mathrm{pot}(e) \geq \mathrm{pot}(e')$ for all unclaimed edges e', until he claimed all of his q edges. We call the edges claimed in Part 2* free edges. *The number of free edges claimed in turn t is denoted by $f(t)$. Note that*

$$f(t) = q - \deg_{M,t-1}(u) - \deg_{M,t-1}(v). \tag{2.2}$$

Part 1 of the strategy is more or less obligatory, because a Maker-path of length 2 that is not closed by Breaker can be completed to a triangle in the next turn. Part 2 is more interesting. Our aim in the following sections is to prove Theorem 2.11, where we show that part 2 of the strategy prevents Maker from building a $q/2$-star, so that Breaker wins the game.

Observation 2.8. *We can assume that the game contains no isolation turns.*

Proof. Consider an arbitrary isolation t turn in the game, i.e., a turn, after which one of the nodes of the edge e_M claimed in this turn by Maker has no unclaimed incident edges left. Right after the turn, every triangle e_M belongs to is already blocked by Breaker, so the edge e_M is of no use for Maker from this time on. Breaker even could pretend that the edge e_M belongs to his own edges, so that in the turn t Breaker claimed $q + 1$ edges and Maker didn't claim any edge. Hence, a perfectly playing Maker will always try to avoid isolation turns. If he can't, he will definitely lose the game, since he can only claim useless edges until the end of the game. □

The following observation states that, as long as Breaker can keep the total potential below $2n$, he will have at least 2 free edges in every turn.

Observation 2.9. *For every turn t with $f(t) \leq 1$ there exists a turn $t' < t$ with $\mathrm{POT}_{t'} > 2n$.*

Proof. Let t be a turn with $f(t) \leq 1$ and let $\{u, v\}$ be the Maker-edge of this turn. Because $f(t) = q - \deg_{M,t-1}(u) - \deg_{M,t-1}(v)$, we get $\deg_{M,t-1}(u) + \deg_{M,t-1}(v) \geq q - 1$, so there exists $w \in \{u, v\}$ with $\deg_{M,t-1}(w) \geq \left\lceil \frac{q-1}{2} \right\rceil \geq \lceil \frac{q}{2} \rceil - 1$. Hence, there exists a turn $t' \leq t - 1$ with $\deg_{M,t'}(w) = \lceil \frac{q}{2} \rceil - 1$ and $\mathrm{pot}_{t'}(w) > 0$. We apply Lemma 2.7 and get $\mathrm{pot}_{t'}(w) > 2n$, so especially $\mathrm{POT}_{t'} > 2n$. □

2.2.4 Main results

In this subsection we prove that Strategy 3 works correctly and is a winning strategy. For both theorems in this subsection we assume that Breaker plays according to Strategy 3. We further assume that $q = \sqrt{(\frac{8}{3} + \epsilon^*)n}$ for some $\epsilon^* > 0$ as stated above and that n is sufficiently large. For Breaker's strategy it is crucial that the potential of every node is kept below a certain level. This is ensured by the following theorem.

Theorem 2.10. *For every turn s it holds $\mathrm{POT}_s < 2n$.*

The proof of this theorem is the mathematical core of this paper and is given in the next section. The main result of our work is:

Theorem 2.11. *At the end of the game there exists no node with Maker-degree of at least $q/2$ and Breaker wins the game.*

Proof. Assume that there exists a node v with $\deg_M(v) \geq q/2$ at the end of the game. Then, $\deg_M(v) \geq \lceil q/2 \rceil$. Let t denote the turn in which Maker claimed his $\lceil q/2 \rceil$-th edge incident in v, so $\deg_{M,t-1}(v) = \lceil q/2 \rceil - 1$. Due to Theorem 2.10 we know that $\mathrm{pot}_{t-1}(v) \leq \mathrm{POT}_{t-1} < 2n$. Note that after turn $t - 1$ there are still unclaimed edges incident in v, so $\mathrm{pot}_{t-1}(v) > 0$. We apply Lemma 2.7 and get $\deg_{M,t-1}(v) \neq \lceil q/2 \rceil - 1$, a contradiction.

With every edge $\{u, v\}$ that Maker chooses he creates less than $\deg_M(u) + \deg_M(v) < q$ new Maker-paths of length 2. Hence, Breaker always has enough edges to close all Maker-paths of length 2 and finally wins the game. □

2.3 Analysis

2.3.1 Outline of the proof

We proceed to prove Theorem 2.10. As it is depending on a series of lemmas, for the reader's convenience we first outline the argumentation in an informal way. We distinguish two types of turns. A turn is called *non-critical*, if a certain fraction of the

Breaker-edges in this turn suffices to compensate the total potential increase caused by Maker in this turn. Otherwise, we call it *critical*. We start with an arbitrary critical turn t_0 in which the potential exceeds n. Lemma 2.17 gives us a useful characterization of critical turns. This enables us to prove Theorem 2.18, where we state that before a constant number of additional critical turns is played, the total potential will sink below n again. Because a constant number of critical turns cannot increase the total potential considerably much (Lemma 2.21), we can prove that the total potential of the game never exceeds $2n$.

2.3.2 Potential change in a single turn

To analyze the potential change of a single turn, we first present a few tools for estimation of potential change caused by single Maker- and Breaker-edges. The next lemma shows how the addition of a single Maker-edge changes the deficit of a node.

Lemma 2.12. *Consider an arbitrary point of time in the game. Let $u \in V$ and let $\deg^{*\prime}(u), \deg'_M(u)$ and $d'(u)$ be the balanced Breaker-degree, Maker-degree and deficit of u after an additional edge incident in u was claimed by Maker. Then,*

$$d'(u) - d(u) = \deg^{*\prime}(u) - \deg^*(u) \leq p_0(q - \deg_M(u)).$$

Proof. The equation follows from the fact that an additional Maker-edge does not change $\deg_B(u)$. Using that $\deg'_M(u) = \deg_M(u) + 1$ we continue

$$\begin{aligned}
&\deg^{*\prime}(u) - \deg^*(u) \\
&= p_0 \deg'_M(u) \left(q - \frac{\deg'_M(u)}{2}\right) - p_0 \deg_M(u) \left(q - \frac{\deg_M(u)}{2}\right) \\
&= p_0 \left(\deg_M(u) \left(q - \frac{\deg_M(u)+1}{2}\right) + \left(q - \frac{\deg_M(u)+1}{2}\right)\right) \\
&- p_0 \deg_M(u) \left(q - \frac{\deg_M(u)}{2}\right) \\
&= p_0(q - \deg_M(u) - 1/2) \leq p_0(q - \deg_M(u)).
\end{aligned}$$

□

Lemma 2.13. *(i) A single edge e_M claimed by Maker increases the potential of a node by at most a factor of μ and causes a total potential increase of at most $(\mu - 1)\mathrm{pot}(e_M)$ (where $\mathrm{pot}(e_M)$ denotes the potential of e_M when claimed by Maker).*

(ii) A single edge e_B claimed by Breaker causes a total potential decrease of at least $(1 - \mu^{-1/q})\mathrm{pot}(e_B)$ (where $\mathrm{pot}(e_B)$ denotes the potential of e_B when claimed by Breaker).

Proof. (i). Let $e_M = \{u, v\}$. For $w \in V$ let $\mathrm{pot}(w)$ denote the potential of w before Maker claimed e_M and $\mathrm{pot}'(w)$ denote the potential of w directly after Maker claimed

e_M. If e_M is not incident in w, the potential of w remains unchanged. If e_M is the last unclaimed edge incident in w, $\text{pot}'(w) = 0$ and we are done. Otherwise we can apply Lemma 2.12 and Remark 2.4 and get

$$\frac{\text{pot}'(w)}{\text{pot}(w)} = \mu^{(d'(w)-d(w))/q} \leq \mu^{p_0(q-\deg_M(w))/q} \leq \mu.$$

Because e_M only changes the potential of u and v, the total potential increase is $\text{pot}'(v) - \text{pot}(v) + \text{pot}'(u) - \text{pot}(u) \leq (\mu - 1)\text{pot}(e_M)$.

(ii). Let $e_B = \{u, v\}$. Because e_B only changes the potential of u and v, the total potential decrease caused by e_B is $\text{pot}(v) - \text{pot}'(v) + \text{pot}(u) - \text{pot}'(u)$, where $\text{pot}(w)$ denotes the potential of w before Breaker claimed e_B and $\text{pot}'(w)$ denote the potential of w directly after Breaker claimed e_B. We show that

$$\text{pot}(v) - \text{pot}'(v) \geq (1 - \mu^{-1/q})\text{pot}(v).$$

Because the same holds for u, the claim (ii) follows. If e_B is the last unclaimed edge in v, $\text{pot}'(v) = 0$. Otherwise,

$$\frac{\text{pot}'(v)}{\text{pot}(v)} = \mu^{(d'(u)-d(u))/q} = \mu^{-1/q},$$

where the last equation follows from the fact that a Breaker-edge does not change $\deg^*(v)$ and increases $\deg_B(v)$ by 1. □

Every turn t starts with a Maker move, i.e. an edge $\{u, v\}$ being claimed by Maker followed by q Breaker moves. While the Maker move causes a potential increase, Breaker's moves cause a decrease. For every node $w \in V$, we denote its potential increase by $I_t(w)$ and its potential decrease by $D_t(w)$. Note that every claimed edge only changes the potential of its two incident nodes. When following Breaker's strategy, there are four possible ways of potential decrease for the node w: decrease caused by free edges, denoted by $D_t^{\text{free}}(w)$ and decrease caused by closing edges, either w being their head, denoted by $D_t^{\text{heads}}(w)$, or their tail, denoted by $D_t^{\text{tails}}(w)$. In the special case in which Maker or Breaker claim the last unclaimed edge incident in w, the potential of w is set to 0, which causes an additional potential decrease. For technical reasons, this additional decrease is considered separately and denoted by $D_t^0(w)$. If for example Breaker claims a free edge that is the last unclaimed edge incident in w, this edge contributes both to $D_t^{\text{free}}(w)$ and $D_t^0(w)$. For the contribution to $D_t^{\text{free}}(w)$ we only compute the potential change caused by the change of the balance value and for the contribution to $D_t^0(w)$ we take the real potential decrease caused by the edge and subtract the computed contribution to $D_t^{\text{free}}(w)$. Moreover, we further split $D_t^{\text{heads}}(w)$ into two parts $D_t^{\text{heads}}(w) = D_t^-(w) + D_t^+(w)$, where

$$D_t^-(w) := \min\{I_t(w), D_t^{\text{heads}}(w)\} \quad \text{and} \quad D_t^+(w) := \max\{D_t^{\text{heads}}(w) - I_t(w), 0\}.$$

If Maker claims an edge that connects two nodes with a very high Maker-degree, it might happen that $D_t^{\text{heads}}(w) > I_t(w)$ for one or both of the newly connected nodes. Otherwise, $D_t^+ = 0$ and $D_t^-(w) = D_t^{\text{heads}}(w)$.

If for one of these values we omit the argument, we always mean the total potential increase (decrease) added up over all nodes. For example, $I_t := \sum_{v \in V} I_t(v)$. For every turn t we have

$$\mathrm{POT}_t - \mathrm{POT}_{t-1} = I_t - D_t = I_t - (D_t^{\mathrm{free}} + D_t^- + D_t^+ + D_t^{\mathrm{tails}} + D_t^0).$$

Lemma 2.14. *Let t be an arbitrary turn. Let e_M be the Maker-edge of this turn. Then,*

(i) for every $w \in V$ it holds $I_t(w) - D_t^-(w) \leq (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(w)$.

(ii) $I_t - D_t^- \leq (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(e_M)$.

Proof. *(i).* Let $e_M = \{u, v\}$. First note that if $D_t^-(w) \neq D_t^{\mathrm{heads}}(w)$, it follows that $D_t^-(w) = I_t(w)$, so there is nothing more to show. Otherwise, the term $I_t(w) - D_t^-(w)$ describes the change of the potential of w from the beginning of the turn t to the end of part 1 of Breaker's moves in the same turn, where we ignore the changes caused by tails of closing edges. For $w \notin \{u, v\}$ this is 0 and we are done. So let $w \in \{u, v\}$ and let $\deg_{M,t}^{(1)}(w), \deg_{B,t}^{(1)}(w), \deg^*{}_t^{(1)}(w)$ and $d_t^{(1)}(w), \mathrm{pot}_t^{(1)}(w)$ be the Maker-degree, Breaker-degree, balanced degree, deficit and potential of w after part 1 of Breaker's moves (i.e. after all closing edges have been claimed). To compute the change of the potential of w, we start by computing the change of its deficit. We have

$$\begin{aligned} d_t^{(1)}(w) - d_{t-1}(w) &= \deg^*{}_t^{(1)}(w) - \deg_{B,t}^{(1)}(w) - \deg^*{}_{t-1}(w) + \deg_{B,t-1}(w) \\ &= (\deg^*{}_t^{(1)}(w) - \deg^*{}_{t-1}(w)) - (\deg_{B,t-1}^{(1)}(w) - \deg_{B,t}(w)). \end{aligned}$$

The first term describes the change of $\deg^*(w)$. Since Breaker-edges do not influence this value, this change is caused solely by e_M. Due to Lemma 2.12, this is at most $p_0(b - \deg_{M,t-1}(w))$. The second term simply describes the number of closing edges claimed incident to w. Due to Observation 2.8, t is no isolation turn, so in case of $w = u$, this is $\deg_{M,t-1}(v)$ and in case of $w = v$ this is $\deg_{M,t-1}(u)$. Together with (2.2) and Remark 2.4 this gives

$$d_t^{(1)}(u) - d_{t-1}(u) = p_0(q - \deg_{M,t-1}(u)) - \deg_{M,t-1}(v) \leq p_0 f(t) \tag{2.3}$$

and

$$d_t^{(1)}(v) - d_{t-1}(v) = p_0(q - \deg_{M,t-1}(v)) - \deg_{M,t-1}(u) \leq p_0 f(t). \tag{2.4}$$

This implies

$$\begin{aligned} I_t(w) - D_t^-(w) &= \mathrm{pot}_t^{(1)}(w) - \mathrm{pot}_{t-1}(w) = \mu^{d_t^{(1)}(w)/q} - \mathrm{pot}_{t-1}(w) \\ &= (\mu^{(d_t^{(1)}(w) - d_{t-1}(w))/q} - 1)\mathrm{pot}_{t-1}(w) \\ &\overset{(2.3),(2.4)}{\leq} (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(w). \end{aligned}$$

(ii). Note that $I_t = I_t(u) + I_t(v)$ and $D_t^- = D_t^-(u) + D_t^-(v)$, so we have

$$\begin{aligned} I_t - D_t^- &= I_t(u) + I_t(v) - (D_t^-(u) + D_t^-(v)) \\ &= I_t(u) - D_t^-(u) + I_t(v) - D_t^-(v) \\ &\overset{(i)}{\leq} (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(u) + (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(v) \\ &= (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(e_M). \end{aligned}$$

□

2.3.3 Critical turns

Since $\mu \overset{n\to\infty}{\longrightarrow} 1$, with Remark 2.4 and n big enough we get $\mu p_0 < 1$. Fix $\eta \in (0, 1 - \mu p_0)$ and define the following parts of potential change.

Definition 2.15. *For every turn t let*

$$\Delta_t := I_t - D_t^- - (1 - \eta)D_t^{\mathrm{free}}$$

and

$$r_t := D_t^+ + D_t^{\mathrm{tails}} + \eta D_t^{\mathrm{free}} + D_t^0.$$

We call t critical, *if $\Delta_t > 0$ and* non-critical *otherwise.*

Note that $\mathrm{POT}_t - \mathrm{POT}_{t-1} = \Delta_t - r_t$. Since $r_t \geq 0$, every turn t with $\mathrm{POT}_t > \mathrm{POT}_{t-1}$ is critical.

Lemma 2.16. *For all $x \in \mathbb{R}$ with $x \geq 1$ it holds $x(1 - \mu^{-1/q}) \geq 1 - \mu^{-x/q}$.*

Proof. We define $g(x) := x(1 - \mu^{-1/q})$ and $h(x) := 1 - \mu^{-x/q}$, so we have to show $g(x) \geq h(x)$ for all $x \geq 1$. First note that $g(1) = h(1)$, so it suffices to show that $g'(x) \geq h'(x)$ for all $x \geq 1$. We have $g'(x) = 1 - \mu^{-1/q}$ and $h'(x) = \mu^{-x/q}\frac{\ln(\mu)}{q}$. Because for all $x > 0$ we have $h''(x) = -\mu^{-x/q}\left(\frac{\ln(\mu)}{q}\right)^2 < 0 = g''(x)$, it suffices to show that $g'(1) \geq h'(1)$. To see this, we use the fact that $e^y - 1 \geq y$ for all $y \geq 0$, so especially $\mu^{1/q} - 1 \geq \frac{\ln(\mu)}{q}$. If we multiply both sides with $\mu^{-1/q}$, we get

$$1 - \mu^{-1/q} \geq \mu^{-1/q}\frac{\ln(\mu)}{q}.$$

Because the left hand side is $g'(1)$ and the right hand side is $h'(1)$, we are done. □

The following lemma provides an important characterization of critical turns by an upper bound for the potential of all edges still unclaimed after the turn.

Lemma 2.17. *Let t be a critical turn with $f(t) \geq 2$ and let e_M be the edge chosen by Maker in this turn. For every edge e that is still unclaimed after t it holds*

$$\mathrm{pot}_t(e) < \frac{\mu p_0}{(1 - \eta)}\mathrm{pot}_{t-1}(e_M).$$

Proof. Let $e_M = \{u, v\}$. By Lemma 2.14 (ii) we have

$$\begin{aligned} I_t - D_t^- &\leq (\mu^{p_0 f(t)/q} - 1)\mathrm{pot}_{t-1}(e_M) \\ &= \mu^{p_0 f(t)/q}(1 - \mu^{-p_0 f(t)/q})\mathrm{pot}_{t-1}(e_M) \\ &\leq \mu(1 - \mu^{-p_0 f(t)/q})\mathrm{pot}_{t-1}(e_M) \end{aligned}$$

We apply Lemma 2.16 with $x := p_0 f(t)$ (note that due to Remark 2.4 we have $x > \frac{8}{3\beta} f(t) > \frac{8}{12} f(t) \geq \frac{16}{12} > 1$) and get

$$I_t - D_t^- \leq \mu p_0 f(t)(1 - \mu^{-1/q})\mathrm{pot}_{t-1}(e_M).$$

Because t is a critical turn, we get

$$\begin{aligned} 0 < \Delta_t &= I_t - D_t^- - (1-\eta)D_t^{\mathrm{free}} \\ &\leq \mu p_0 f(t)(1 - \mu^{-1/q})\mathrm{pot}_{t-1}(e_M) - (1-\eta)D_t^{\mathrm{free}}, \end{aligned}$$

implying

$$(1-\eta)D_t^{\mathrm{free}} < \mu p_0 f(t)(1 - \mu^{-1/q})\mathrm{pot}_{t-1}(e_M). \tag{2.5}$$

Now let e be an edge that after turn t still is unclaimed. Then every free edge claimed by Breaker in turn t has at least a potential of $\mathrm{pot}_t(e)$ because Breaker iteratively chooses the edge with maximum potential and every edge claimed by Breaker only decreases potential. Due to Lemma 2.13 (ii) every free edge causes a total potential decrease of at least $\mathrm{pot}_t(e)(1 - \mu^{-1/q})$ and hence we get

$$D_t^{\mathrm{free}} \geq f(t)\mathrm{pot}_t(e)(1 - \mu^{-1/q}).$$

Together with (2.5) this implies $\mathrm{pot}_t(e) < \frac{\mu p_0}{(1-\eta)}\mathrm{pot}_{t-1}(e_M)$. □

2.3.4 Increase of total potential

With our strategy we cannot guarantee that $\mathrm{POT}_t \leq \mathrm{POT}_{t-1}$ for all turns t. But we will show that each turn t_0 at which the potential exceeds n is followed closely by a turn at which the total potential is at most as big as it was before t_0. So in the long run we obtain a decrease of the total potential, which will ensure Breaker's win.

Fix constant parameters $\gamma \in (0, 1)$, and $\epsilon > 0$ with

$$\frac{1-\eta}{(1+\epsilon)\mu p_0} > 1. \tag{2.6}$$

Recall that this possible, because $\eta < 1 - \mu p_0$ by the choice of η. Define

$$c := \left\lceil \frac{1 - \log(1-\gamma)}{\log(1-\eta) - \log(1+\epsilon) - \log(\mu p_0)} \right\rceil$$

and note that $c > 0$ due to (2.6). Although c depends on n, it is bounded by constants because $1 < \mu < 2$ for n sufficiently big. Let t_0 be a turn with $\mathrm{POT}_{t_0} > n, \mathrm{POT}_{t_0-1} \leq n$ and $\mathrm{POT}_t < 2n$ for all $t < t_0$. Then, t_0 is a critical turn and due to Observation 2.9 it holds $f(t_0) \geq 2$. Let $e_0 = \{u, v\}$ be the edge claimed by Maker in this turn and w.l.o.g. let $\mathrm{pot}_{t_0-1}(u) \geq \mathrm{pot}_{t_0-1}(v)$. We consider three points of time:

- Let t_1 be the first turn after $t_0 - 1$ with $\mathrm{pot}_{t_1}(u) \leq (1-\gamma)\mathrm{pot}_{t_0-1}(u)$.
- Let t_2 be the first turn after t_0 with $\mathrm{pot}_{t_2}(w) \geq (1+\epsilon)\mathrm{pot}_s(w)$ for some $w \in V$ and some turn s with $t_0 \leq s < t_2$.
- Let t_3 be the c-th critical turn after $t_0 - 1$.

If the game ends before the turn t_i is reached, let $t_i := \infty$. We set $t^* := \min(t_1, t_2, t_3)$ (note that $t^* = \infty$ is possible) and aim to prove the following theorem

Theorem 2.18. *Let n sufficiently big. If the game is not ended before turn t^*, then $\mathrm{POT}_{t^*} \leq \mathrm{POT}_{t_0-1}$.*

Since the proof is quite involved, it is split into several parts. We start with an observation, that between the turns t_0 and t_2 the total potential will not exceed $2n$.

Observation 2.19. *If n is sufficiently large, for every turn t with $t_0 \leq t < t_2$ it holds $\mathrm{POT}_t < 2n$.*

Proof. Because $t < t_2$, for every $v \in V$ it holds $\mathrm{pot}_t(v) \leq (1+\epsilon)\mathrm{pot}_{t_0}(v)$ by definition of t_2. This implies

$$\mathrm{POT}_t = \sum_{v \in V} \mathrm{pot}_t(v) \leq \sum_{v \in V} (1+\epsilon)\mathrm{pot}_{t_0}(v) = (1+\epsilon)\mathrm{POT}_{t_0}.$$

By Lemma 2.14 (ii) we have

$$\begin{aligned}\mathrm{POT}_{t_0} &= \mathrm{POT}_{t_0} - \mathrm{POT}_{t_0-1} + \mathrm{POT}_{t_0-1} \leq I_{t_0} - D^-_{t_0} + \mathrm{POT}_{t_0-1} \\ &\leq \mu^{p_0 f(t_0)/q}\mathrm{POT}_{t_0-1} \leq \mu \mathrm{POT}_{t_0-1},\end{aligned}$$

so finally,

$$\mathrm{POT}_t \leq (1+\epsilon)\mathrm{POT}_{t_0} \leq \mu(1+\epsilon)\mathrm{POT}_{t_0-1} \leq \mu(1+\epsilon)n < \tfrac{3}{2}\mu n.$$

For sufficiently large n we have $\mu < \frac{4}{3}$ and the proof is complete. □

In the following we assume that the game is not ended before turn t^* is reached. In the next lemma we further refine the characterization of critical turns from Lemma 2.17. We only consider turns between t_0 and t_2 and prove that the number of critical turns in this interval affects the maximum possible potential of unclaimed edges exponentially.

Lemma 2.20. *Let s be a turn with $t_0 \leq s \leq t^*$ and $s < t_2$. Let $\mathrm{crit}(s) \in [c]$ be the number of critical turns between t_0 and s (including t_0 and s). Then, for every edge e unclaimed after turn s it holds*

$$\mathrm{pot}_s(e) < \left(\frac{(1+\epsilon)\mu p_0}{(1-\eta)}\right)^{\mathrm{crit}(s)} 2\mathrm{pot}_{t_0-1}(u).$$

Proof. Via induction over $\mathrm{crit}(s)$.

Let $\mathrm{crit}(s) = 1$. Recall that $e_0 = \{u, v\}$ is the edge claimed by Maker in turn t_0 and that $\mathrm{pot}_{t_0-1}(u) \geq \mathrm{pot}_{t_0-1}(v)$. Let $e = \{x, y\}$ be an edge unclaimed after turn s. Because $s < t_2$, we know that

$$\mathrm{pot}_s(e) = \mathrm{pot}_s(x) + \mathrm{pot}_s(y) \leq (1+\epsilon)\mathrm{pot}_{t_0}(x) + (1+\epsilon)\mathrm{pot}_{t_0}(y) = (1+\epsilon)\mathrm{pot}_{t_0}(e)$$

and because $f(t_0) \geq 2$, by Lemma 2.17

$$(1+\epsilon)\mathrm{pot}_{t_0}(e) < (1+\epsilon)\frac{\mu p_0}{(1-\eta)}\mathrm{pot}_{t_0-1}(e_0) \leq \frac{(1+\epsilon)\mu p_0}{(1-\eta)} 2\mathrm{pot}_{t_0-1}(u).$$

Now let the claim be true for all s' with $\mathrm{crit}(s') = i, i \in [c-1]$. Let s be a turn with $\mathrm{crit}(s) = i+1$. Let s' be the last critical turn before s (if s is critical, let $s' = s$). Then $\mathrm{crit}(s'-1) = i$. Let e_M be the edge claimed by Maker in turn s'. We get

$$\begin{aligned}
\mathrm{pot}_s(e) &\leq (1+\epsilon)\mathrm{pot}_{s'}(e) && (t < t_2)\\
&\leq (1+\epsilon)\frac{\mu p_0}{(1-\eta)}\mathrm{pot}_{s'-1}(e_M) && (\text{Lemma 2.17})\\
&\leq (1+\epsilon)\frac{\mu p_0}{(1-\eta)}\left(\frac{(1+\epsilon)\mu p_0}{1-\eta}\right)^i 2\mathrm{pot}_{t_0-1}(u) && (\text{IH})\\
&= \left(\frac{(1+\epsilon)\mu p_0}{1-\eta}\right)^{i+1} 2\mathrm{pot}_{t_0-1}(u).
\end{aligned}$$

Note that for the above application of Lemma 2.17, we need to ensure that $f(s') \geq 2$. Due to Observation 2.9, it suffices to show that $\mathrm{POT}_t < 2n$ for all $t < s'$. By choice of t_0, we already know that $\mathrm{POT}_t < 2n$ for all $t < t_0$ and because $s' \leq s < t_2$, for all $t_0 \leq t < s'$ we can apply Observation 2.19 and get $\mathrm{POT}_t < 2n$. □

Lemma 2.21. *For every $\xi > 0$, if n is sufficiently big, we have*

$$\sum_{\substack{t_0 \leq s \leq t^* \\ s \text{ critical}}} I_s \leq 2c(\mu-1)\mathrm{pot}_{t_0-1}(u) < \xi \mathrm{pot}_{t_0-1}(u).$$

Proof. Let $\xi > 0$. First note that due to Lemma 2.13 (i)

$$I_{t_0} \leq (\mu-1)\mathrm{pot}_{t_0-1}(e_0) \leq 2(\mu-1)\mathrm{pot}_{t_0-1}(u). \tag{2.7}$$

Now let s be a critical turn with $t_0 < s \leq t^*$. Let e_M be the edge claimed by Maker in this turn. We get

$$\begin{aligned}
I_s &\leq (\mu-1)\mathrm{pot}_{s-1}(e_M) && (\text{Lemma 2.13 (i)})\\
&< (\mu-1)\left(\frac{(1+\epsilon)\mu p_0}{(1-\eta)}\right)^{\mathrm{crit}(s-1)} 2\mathrm{pot}_{t_0-1}(u) && (\text{Lemma 2.20})\\
&\overset{(2.6)}{\leq} (\mu-1)2\mathrm{pot}_{t_0-1}(u).
\end{aligned}$$

So for every critical turn s with $t_0 \leq s \leq t^*$ we have

$$I_s \leq 2(\mu - 1)\mathrm{pot}_{t_0-1}(u). \tag{2.8}$$

Because $t \leq t_3$, there are at most c critical turns between t_0 and t^*, so finally we get

$$\sum_{\substack{t_0 \leq s \leq t^* \\ s \text{ critical}}} I_s \leq \sum_{\substack{t_0 \leq s \leq t^* \\ s \text{ critical}}} 2(\mu - 1)\mathrm{pot}_{t_0-1}(u) \leq 2c(\mu - 1)\mathrm{pot}_{t_0-1}(u).$$

Recall that $(\mu - 1) = 6\ln(n)\beta/\delta q = 6\ln(n)\sqrt{\beta}/\delta\sqrt{n} \overset{n\to\infty}{\longrightarrow} 0$, whereas c is bounded by a constant. So for n sufficiently big, the whole term is smaller than $\xi\mathrm{pot}_{t_0-1}(u)$. □

By definition, t^* always has one of the three values t_1, t_2, t_3. In the following three lemmas we consider all possible cases. These lemmas combined directly imply Theorem 2.18. We always assume n to be sufficiently big if needed.

Lemma 2.22. *If $t_1 \leq t_2$ and $t_1 \leq t_3$, then $\mathrm{POT}_{t_0-1} \geq \mathrm{POT}_{t^*}$.*

Proof. Let $\xi \in (0, \eta\gamma)$. By assumption $t^* = \min(t_1, t_2, t_3) = t_1$ and hence, by definition of t_1 we have $\mathrm{pot}_{t^*}(u) \leq (1-\gamma)\mathrm{pot}_{t_0-1}(u)$. Let $R := \sum_{t_0 \leq s \leq t^*} r_s$. Then,

$$\begin{aligned}
\mathrm{POT}_{t^*} - \mathrm{POT}_{t_0-1} &= \sum_{t_0 \leq s \leq t^*} \mathrm{POT}_s - \mathrm{POT}_{s-1} = \sum_{t_0 \leq s \leq t^*} \Delta_s - r_s \\
&= \sum_{\substack{t_0 \leq s \leq t^* \\ s \text{ critical}}} \Delta_s + \underbrace{\sum_{\substack{t_0 \leq s \leq t^* \\ s \text{ non-critical}}} \Delta_s}_{\leq 0} - R \\
&\leq \sum_{\substack{t_0 \leq s \leq t^* \\ s \text{ critical}}} \Delta_s - R \\
&\leq \xi\mathrm{pot}_{t_0-1}(u) - R, && \text{(Lemma 2.21)}
\end{aligned}$$

hence it suffices to show that $R \geq \xi \text{pot}_{t_0-1}(u)$. We have

$$\begin{aligned}
&\xi \text{pot}_{t_0-1}(u) \\
&\leq \eta\gamma \text{pot}_{t_0-1}(u) \\
&\leq \eta(\text{pot}_{t_0-1}(u) - \text{pot}_{t^*}(u)) && (t^* = t_1) \\
&= \eta \left(\sum_{t_0 \leq s \leq t^*} D_s(u) - I_s(u) \right) \\
&= \eta \left(\sum_{t_0 \leq s \leq t^*} D_s^-(u) + D_s^+(u) + D_s^{\text{tails}}(u) + D_s^{\text{free}}(u) + D_s^0(u) - I_s(u) \right) \\
&\leq \eta \left(\sum_{t_0 \leq s \leq t^*} D_s^+(u) + D_s^{\text{tails}}(u) + D_s^{\text{free}}(u) + D_s^0(u) \right) && (D_s^-(u) \leq I_s(u)) \\
&\leq \sum_{t_0 \leq s \leq t^*} D_s^+(u) + D_s^{\text{tails}}(u) + \eta D_s^{\text{free}}(u) + D_s^0(u) \\
&\leq \sum_{t_0 \leq s \leq t^*} r_s = R.
\end{aligned}$$

□

Lemma 2.23. *If $t_2 < t_1$ and $t_2 \leq t_3$, then $\text{POT}_{t_0-1} \geq \text{POT}_{t^*}$.*

Proof. Let $\xi > 0$ with $\xi \leq \eta(1-\gamma)(1-(1+\epsilon)^{-1/p_0})$. We have $t^* = t_2$, so there exists a turn s_0 with $t_0 \leq s_0 < t^*$ and a vertex $w \in V$, such that $\text{pot}_t(w) \geq (1+\epsilon)\text{pot}_{s_0}(w)$. Because $t^* < t_1$, the potential of u was not set to 0 and as in the proof of Lemma 2.22 it suffices to show that $R \geq \xi \text{pot}_{t_0-1}(u)$. We start by showing that for all turns t with $s_0 \leq t \leq t^*$ it holds

$$\text{pot}_t(w) \leq \text{pot}_{s_0}(w) \prod_{s_0 < s \leq t} \mu^{p_0 f(s)/q}. \tag{2.9}$$

We prove (2.9) via induction over t. For $t = s_0$ the claim obviously holds. Now let $t > s_0$. Then, $t - 1 \geq s_0$ and by Lemma 2.14 (i) we have

$$\text{pot}_t(w) - \text{pot}_{t-1}(w) \leq I_t(w) - D_t^-(w) \leq \text{pot}_{t-1}(w)(\mu^{p_0 f(t)/q} - 1),$$

so

$$\text{pot}_t(w) \leq \text{pot}_{t-1}(w)\mu^{p_0 f(t)/q}.$$

By applying the induction hypothesis we finish the proof of (2.9):

$$\text{pot}_t(w) \leq \left(\text{pot}_{s_0}(w) \prod_{s_0 < s \leq t-1} \mu^{p_0 f(s)/q} \right) \mu^{p_0 f(t)/q} = \text{pot}_{s_0}(w) \prod_{s_0 < s \leq t} \mu^{p_0 f(s)/q}.$$

Using (2.9), we get

$$(1+\epsilon)\mathrm{pot}_{s_0}(w) \le \mathrm{pot}_{t^*}(w) \le \mathrm{pot}_{s_0}(w) \prod_{s_0<s\le t^*} \mu^{p_0 f(s)/q},$$

so

$$(1+\epsilon) \le \prod_{s_0<s\le t^*} \mu^{p_0 f(s)/q} = \mu^{\left(p_0 \sum_{s_0<s\le t^*} f(s)\right)/q}$$

which,taking the logarithm gives

$$\sum_{s_0<s\le t^*} f(s) \ge \frac{q\ln(1+\epsilon)}{p_0 \ln(\mu)} =: x,$$

so at least x free edges were claimed by Breaker between the turns s_0 and t^*. Because $t^* < t_1$, at the whole time from t_0 to t^* the potential of u is at least $(1-\gamma)\mathrm{pot}_{t_0-1}(u)$. Hence, during this time every unclaimed edge incident in u has a potential of at least $(1-\gamma)\mathrm{pot}_{t_0-1}(u)$, so especially every free edge claimed by Breaker has at least this potential and, due to Lemma 2.13 (ii), causes a decrease of the total potential of at least $(1-\gamma)\mathrm{pot}_{t_0-1}(u)(1-\mu^{-\frac{1}{q}})$. Therefore, we get

$$\begin{aligned}
R &\ge \eta \sum_{s_0<s\le t^*} D_s^{\mathrm{free}} \\
&\ge \eta x(1-\gamma)\mathrm{pot}_{t_0-1}(u)\left(1-\mu^{-\frac{1}{q}}\right) \\
&\ge \eta(1-\gamma)\mathrm{pot}_{t_0-1}(u)\left(1-\mu^{-\frac{x}{q}}\right) && \text{(Lemma 2.16)} \\
&\ge \eta(1-\gamma)\mathrm{pot}_{t_0-1}(u)\left(1-(1+\epsilon)^{-\frac{1}{p_0}}\right) \\
&\ge \xi \mathrm{pot}_{t_0-1}(u).
\end{aligned}$$

□

Lemma 2.24. $t_3 \ge \min(t_1, t_2)$.

Proof. Let us assume that $t_3 < \min(t_1, t_2)$. Then $t^* = t_3$, so t^* is the c-th critical turn after $t_0 - 1$. We apply Lemma 2.20 to $s = t^* < t_2$ and obtain that for every unclaimed edge e after turn t^* it holds

$$\mathrm{pot}_{t^*}(e) < \left(\frac{(1+\epsilon)\mu p_0}{(1-\eta)}\right)^c 2\mathrm{pot}_{t_0-1}(u) \le (1-\gamma)\mathrm{pot}_{t_0-1}(u)$$

by the choice of c. Since $t^* < t_1$, we have $\mathrm{pot}_t(u) \ge (1-\gamma)\mathrm{pot}_{t_0-1}(u)$, so directly after turn t^*, every unclaimed edge incident in u has a potential of at least $(1-\gamma)\mathrm{pot}_{t_0-1}(u)$. Hence, after turn t^* there exists no unclaimed edge incident in u and this implies that the potential of u must have been set to 0 at some turn s with $t_0 \le s \le t^*$. But then $t_1 \le s \le t^* = t_3$, a contradiction. □

Proof of Theorem 2.10. Let s be some turn with $\mathrm{POT}_t < 2n$ for all $t < s$. We show that this already implies $\mathrm{POT}_s < 2n$.

If $\mathrm{POT}_s < n$, there is nothing to show, so let $\mathrm{POT}_s > n$. Let t_0 be maximal satisfying $t_0 \leq s$ and $\mathrm{POT}_{t_0-1} \leq n$ (t_0 exists due to Lemma 2.6). Define t^* as in Section 2.3.4. If $s = t^*$, we can apply Theorem 2.18 and get $\mathrm{POT}_s = \mathrm{POT}_{t^*} \leq \mathrm{POT}_{t_0-1} \leq n$, so we may assume $s < t^*$. But then, $s < t_2$, so we can apply Observation 2.19 and obtain that $\mathrm{POT}_s < 2n$. □

2.4 Open Questions

We have narrowed the gap for the threshold bias to $[1.414\sqrt{n}, 1.633\sqrt{n}]$. Of course, the question about the exact threshold value remains. At first sight our strategy still has some unused potential for improvement, since the secondary goal of preventing Maker from building a $q/2$-star is very restricting. Breaker could allow Maker to build a few bigger stars, if at the same time he is able to claim all edges connecting these stars. For $q \leq \sqrt{8n/3}$ the strategy still could be used to prevent Maker from building an αq-star for some $\alpha > 1/2$. But it certainly needs some additional variations of the strategy to prevent Maker from connecting stars of size at least $q/2$.

2.5 List of variables

- n : number of nodes in the game graph
- q : number of Breaker-edges per turn
- β : defined as $\beta := \frac{q^2}{n}$; the strategy in this paper works for $\beta > \frac{8}{3}$.
- ϵ^* : a strictly positive constant.
- $\deg_{M,t}(v)$: *Maker-degree of* v; number of Maker-edges incident in v after turn t
- $\deg_{B,t}(v)$: *Breaker-degree of* v; number of Breaker-edges incident in v after turn t
- δ : a constant with $0 < \delta < 1 - \frac{8}{3\beta}$; chosen in Section 2.2.1
- $\mathrm{bal}(v)$: the *balance* of v; a measure of the ratio of Maker and Breaker-edges incident in v; introduced in Definition 2.3
- p_0 : the balance of a node without incident Maker or Breaker-edges; introduced in Definition 2.3
- $\deg^*(v)$: the *balanced Breaker-degree* of v; introduced in Definition 2.5
- $d(v)$: the *deficit* of v, exponent in the potential function; introduced in Definition 2.5
- μ : base in the potential function; introduced in Definition 2.5

- $\mathrm{pot}(v)$: the *potential* of v, in part 2 of the strategy Breaker always claims edges $\{u, v\}$ maximizing $\mathrm{pot}(u) + \mathrm{pot}(v)$; introduced in Definition 2.5
- POT_t : the *total potential* of a turn t; introduced in Definition 2.5
- $f(t)$: number of *free edges* claimed by Breaker in turn t; introduced in Section 2.2.3
- $I_t(v)$: potential increase of v in turn t
- $D_t(v)$: potential decrease of v in turn t
- $D_t^{\mathrm{free}}(v)$: potential decrease of v in turn t caused by free edges
- $D_t^{\mathrm{heads}}(v)$: potential decrease of v in turn t caused by closing edges with v as head
- $D_t^{\mathrm{tails}}(v)$: potential decrease of v in turn t caused by closing edges with v as tail
- $D_t^0(v)$: potential decrease of v in turn t caused by claiming the last unclaimed edge of v
- $D_t^-(v) = \min\{I_t(v), D_t^{\mathrm{heads}}(v)\}$; it holds $D_t^-(v) + D_t^+(v) = D_t^{\mathrm{heads}}(v)$
- $D_v^+(v) = \max\{D_t^{\mathrm{heads}}(v) - I_t(v), 0\}$; it holds $D_t^-(v) + D_t^+(v) = D_t^{\mathrm{heads}}(v)$
- η : a constant with $0 < \eta < 1 - \mu p_0$; introduced in Section 2.3.3
- Δ_t : main part of the total potential change in turn t with $\Delta_t + r_t = \mathrm{POT}_t - \mathrm{POT}_{t-1}$; introduced in Definition 2.15
- r_t : rest part of the total potential change in turn t, with $\Delta_t + r_t = \mathrm{POT}_t - \mathrm{POT}_{t-1}$; introduced in Definition 2.15
- γ : a strictly positive constant; introduced in Section 2.3.4
- ϵ : a strictly positive constant; introduced in Section 2.3.4
- c : a strictly positive value bounded by a constant; introduced in Section 2.3.4
- $t_i, i = 0, 1, 2, 3$: certain turns considered in Section 2.3.4
- $t^* = \min(t_1, t_2, t_3)$; introduced in Section 2.3.4

2.6 A proof of Beck's theorem

In this subsection we prove Beck's theorem [7]. Although the version presented in [7] is slightly more general, the ideas for the proof are basically the same.

Theorem 2.1 (Beck's theorem)**.** *Let U be a finite universe, $\mathcal{W} \subseteq \mathcal{P}(U)$ and consider the Maker-Breaker game played on the hypergraph $(U, \mathcal{W})$. If*

$$\sum_{A \in \mathcal{W}} (1+q)^{-|A|} < \frac{1}{1+q},$$

then Breaker has a winning strategy for the corresponding Maker-Breaker game.

Proof. We start by defining the *potential* of a game situation: For two disjoint sets $M, B \subseteq U$ define $\mathcal{W}_B := \{A \in \mathcal{W} | A \cap B = \emptyset\}$ and

$$\varphi(M, B) := \sum_{A \in \mathcal{W}_B} (1+q)^{-|A \setminus M|}.$$

The disjoint sets M and B represent the elements already chosen by Maker and Breaker, respectively. The set $\mathcal{W}_B$ contains all winning sets that are still relevant for the game, because none of their elements already belongs to Breaker. For every $A \in \mathcal{W}_B$ the term $(1+q)^{-|A \setminus M|}$ can be thought of as the "value" of A for Maker. With every element from A claimed by Maker, this value increases exponentially, such that a set completely claimed by Maker has a value of 1. We also define the potential of a single element: For $u \in U$ let

$$\varphi(M, B, u) := \sum_{\substack{A \in \mathcal{W}_B \\ u \in A}} (1+q)^{-|A \setminus M|}.$$

This definition turns out to be quite useful when computing the potential change caused by a single element: If Breaker claims the element u, the total potential will decrease by $\varphi(M, B, u)$, because all winning sets that contain u no longer contribute to the potential. This directly implies that for all disjoint $M, B \subseteq U$ and $u, v \in U$ it holds

$$\varphi(M, B \cup \{u\}, v) \leq \varphi(M, B, v). \tag{2.10}$$

Denote by m_i the element claimed by Maker in the i-th turn and by $b_i^{(1)}, \ldots, b_i^{(q)}$ the elements claimed by Breaker in this turn. Moreover, we define

$$M_i := \{m_1, \ldots, m_i\}$$

as the set of elements that Maker owns after turn i and

$$B_i := \{b_1^{(1)}, \ldots, b_1^{(q)}, \ldots, b_i^{(1)}, \ldots, b_i^{(q)}\}$$

as the set of Breaker's elements after this turn. Finally, for $j \in \{0, \ldots, q\}$ let $B_{i,j} := B_i \cup \{b_{i+1}^{(1)}, \ldots, b_{i+1}^{(j)}\}$ and define $\psi(i) := \varphi(M_i, B_{i-1})$ as the potential right after Maker chose his i-th element. Breaker's strategy works as follows:

Strategy 4. *For $i \in \mathbb{N}, j \in [q]$ and M_i and $B_{i-1,j-1}$ already fixed, choose $b_i^{(j)}$ such that*

$$\varphi(M_i, B_{i-1,j-1}, b_i^{(j)}) \geq \varphi(M_i, B_{i-1,j-1}, u) \quad \text{for all } u \in U.$$

We show that if Breaker plays according to this strategy, he will achieve

$$\psi(i+1) \le \psi(i) \quad \text{for every turn } i. \tag{2.11}$$

Fix some i. We have

$$\begin{aligned}
\varphi(M_{i+1}, B_i) &= \sum_{A \in \mathcal{W}_{B_i}} (1+q)^{-|A \setminus M_{i+1}|} \\
&= \sum_{\substack{A \in \mathcal{W}_{B_i} \\ m_{i+1} \in A}} (1+q)^{-|A \setminus M_i|+1} + \sum_{\substack{A \in \mathcal{W}_{B_i} \\ m_{i+1} \notin A}} (1+q)^{-|A \setminus M_i|} \\
&= \sum_{A \in \mathcal{W}_{B_i}} (1+q)^{-|A \setminus M_i|} + q \sum_{\substack{A \in \mathcal{W}_{B_i} \\ m_{i+1} \in A}} (1+q)^{-|A \setminus M_i|} \\
&= \varphi(M_i, B_i) + q \cdot \varphi(M_i, B_i, m_{i+1})
\end{aligned}$$

and

$$\begin{aligned}
&\varphi(M_i, B_i) \\
=&\varphi(M_i, B_{i-1}) + \varphi(M_i, B_i) - \varphi(M_i, B_{i-1}) \\
=&\varphi(M_i, B_{i-1}) + \sum_{j=1}^{q} \left(\varphi(M_i, B_{i-1,j}) - \varphi(M_i, B_{i-1,j-1})\right) \\
=&\varphi(M_i, B_{i-1}) + \sum_{j=1}^{q} \left(\sum_{A \in \mathcal{W}_{B_{i-1,j}}} (1+q)^{|A \setminus M_i|} - \sum_{A \in \mathcal{W}_{B_{i-1,j-1}}} (1+q)^{|A \setminus M_i|} \right) \\
=&\varphi(M_i, B_{i-1}) - \sum_{j=1}^{q} \left(\sum_{\substack{A \in \mathcal{W}_{B_{i-1,j-1}} \\ b_i^{(j)} \in A}} (1+q)^{|A \setminus M_i|} \right) \\
=&\varphi(M_i, B_{i-1}) - \sum_{j=1}^{q} \varphi(M_i, B_{i-1,j-1}, b_i^{(j)}),
\end{aligned}$$

so we get

$$\begin{aligned}
\psi(i+1) - \psi(i) &= \varphi(M_{i+1}, B_i) - \varphi(M_i, B_{i-1}) \\
&= q \cdot \varphi(M_i, B_i, m_{i+1}) - \sum_{j=1}^{q} \varphi(M_i, B_{i-1,j-1}, b_i^{(j)}).
\end{aligned}$$

Thus, to show (2.11), it suffices to prove that

$$q \cdot \varphi(M_i, B_i, m_{i+1}) \le \sum_{j=1}^{q} \varphi(M_i, B_{i-1,j-1}, b_i^{(j)}). \tag{2.12}$$

For fixed $j \in [q-1]$, because of the choice of $b_i^{(j)}$ we have

$$\varphi(M_i, B_{i-1,j-1}, b_i^{(j)}) \geq \varphi(M_i, B_{i-1,j-1}, b_i^{(j+1)}) \overset{(2.10)}{\geq} \varphi(M_i, B_{i-1,j}, b_i^{(j+1)})$$

and iterative application of this inequality yields

$$\varphi(M_i, B_{i-1,j-1}, b_i^{(j)}) \geq \varphi(M_i, B_{i-1,q-1}, b_i^{(q)}). \tag{2.13}$$

Because of the choice of $b_i^{(q)}$ it holds

$$\varphi(M_i, B_{i-1,q-1}, b_i^{(q)}) \geq \varphi(M_i, B_{i-1,q-1}, m_{i+1}) \overset{(2.10)}{\geq} \varphi(M_i, B_i, m_{i+1}), \tag{2.14}$$

so for all $j \in [q]$ we get

$$\varphi(M_i, B_{i-1,j-1}, b_i^{(j)}) \overset{(2.13)}{\geq} \varphi(M_i, B_{i-1,q-1}, b_i^{(q)}) \overset{(2.14)}{\geq} \varphi(M_i, B_i, m_{i+1}). \tag{2.15}$$

This implies

$$\sum_{j=1}^{q} \varphi(M_i, B_{i-1,j-1}, b_i^{(j)}) \overset{(2.15)}{\geq} \sum_{j=1}^{q} \varphi(M_i, B_i, m_{i+1}) = q \cdot \varphi(M_i, B_i, m_{i+1})$$

and thus completes the proof of (2.12) and (2.11).

Now assume that Breaker plays according to Strategy 4 and Maker wins the game. Let t^* be the turn in which Maker wins. Then there exists some $A^* \in \mathcal{W}$ with $A^* \subseteq M_{t^*}$. Because M_{t^*} and B_{t^*-1} are disjoint, we get

$$\psi(t^*) = \varphi(M_{t^*}, B_{t^*-1}) = \sum_{A \in \mathcal{W}_{B_{t^*-1}}} (1+q)^{-|A \setminus M_{t^*}|} \geq (1+q)^{-|A^* \setminus M_{t^*}|} = 1.$$

On the other hand, by our assumption,

$$\psi(1) = \varphi(M_1, \emptyset) = \sum_{A \in \mathcal{W}} (1+q)^{-|A \setminus \{m_1\}|} \leq (1+q) \sum_{A \in \mathcal{W}} (1+q)^{-|A|} < 1 \leq \psi(t^*),$$

in contradiction to (2.11). □

Chapter 3

The Mastermind Game

3.1 Introduction

This Chapter is based on a paper previously published in 2017 [16]. Section 3.6 is based on the paper [14].

Mastermind is a famous board game for two players invented by Mordecai Meirowitz in 1970. The first player, called *Codemaker*, makes up a secret code consisting of four pegs in a row. Each code peg has one of six possible colors. The second player, called *Codebreaker*, tries to guess this secret code in as few turns as possible. In each turn he asks a *question*, also consisting of four code pegs in a row. He then receives an *answer* from the Codemaker in form of a number of black and white answer pegs: a black peg for each peg correct in color and position and a white peg for each peg correct in color but at the wrong position. With this information the Codebreaker asks the next question until he receives four black pegs as answer, meaning that the recent question matches the secret code. Besides its success as board game, the Mastermind-Problem has gained a lot of combinatorial interest. In 1976, Donald Knuth [28] was the first one to present an algorithm for the Codebreaker that needs at most five turns to detect the secret code. This worst-case-algorithm was complemented by an average-case-strategy presented by Kenji Koyama and Tony Lai in 1993 [29] that needs 4.34 turns in average, provided that the secret code is chosen uniformly at random. They also proved that their strategy is average-optimal (whereas in the worst case it needs 6 turns and therefore is beaten by Knuth's algorithm).

3.1.1 Different versions of Mastermind

From the combinatorial point of view, the major interest is to investigate the case of p pegs in a row with c possible colors for arbitrary $p, c \in \mathbb{N}$. This problem of *general* Mastermind has been studied extensively during the last decades. The search for asymptotically optimal strategies for increasing p (and c) turns out to be a real challenge, not least because the space of possible secrets has a size of c^p. Even for high performance computers this number quickly leads to huge computation times when it

comes to analyze and test certain strategies.

This fact is emphasized by Jeff Stuckman and Guo-Qiang Zhang [34], who showed that it is NP-hard for the Codebreaker to check for a given game situation, whether there are still possible secrets left or the Codemaker gave an incorrect answer.

There are quite a few variants of this classic game that have also been considered in combinatorial works in the last decades.

- In the pencil and paper variant *bulls and cows* that Mastermind originates from, neither the secret code nor the asked questions are allowed to contain one color more than once. This variant is also called the *AB-Game*. In the *semi AB-Game*, double colors are forbidden in the secret code but may be used in questions.
- The special case of AB-Game played with $c = p$ colors is also called *permutation Mastermind*, because the secret code as well as the questions can be understood as permutations of the set $\{1, \ldots, p\}$.
- In the *black-peg* version Codemaker leaves out the white pegs, so the game becomes harder to solve for Codebreaker. Most works in combinatorics study the black-peg version of the game, because it is much easier to analyze.
- *Static Mastermind* is a combinatorial detection problem rather than a recreational game: The Codebreaker has to ask all of his questions *at once*. After receiving the corresponding answers, he must know the secret code. Non-static variants are also referred to as *adaptive* variants.

The generalized version of Mastermind has been investigated in [21] and [13]. In the latter a strategy with $\mathcal{O}(n \log \log n)$ questions is presented, which is also adaptable to the Black-Peg variant. The best strategy known for Permutation Mastermind for $p = c = n$ needs $\mathcal{O}(n \log n)$ questions and is presented in [14].

3.1.2 Our contribution

The main result of this chapter is a Codebreaker strategy for static permutation Mastermind with $p = c =: n$ pegs and colors that uses at most $\mathcal{O}(p^{1.525} \log(p))$ questions. For the proof, we introduce some new concepts. First, we define the term *separation*. Let S_n be the set of permutations of the set $\{1, 2, \ldots, n\}$. We say that a question Q *separates* two possible secret codes (secrets) $X_1, X_2 \in S_n$ if Q yields different answers for them. A set of questions, called *strategy*, is *feasible* if every pair of possible secrets is separated by at least one question of the set.

We show that there is a set of $\mathcal{O}(n^{1.525})$ questions such that every pair of possible secrets with Hamming distance of at most $\sqrt{n}$ is separated by at least one question. For a prime n, we construct a set of $\mathcal{O}(n^{1.5})$ questions for that matter. If n is not a prime, the problem gets more complicated. Here we start with a fairly simple feasible $(2n^2/3)$-strategy. We then modify this strategy to get a set of $\mathcal{O}(n^{1.525})$ questions that for a secret gives us the placement of the last $n^{0.525}$ colors and the colors of the last $n^{0.525}$ pegs. A result of Baker et al. [4] for the difference between consecutive primes

reveals that for sufficiently large n there is a prime $p(n) \in [n - n^{0.525}, n]$, so we can use the mentioned $\mathcal{O}(p(n)^{1.5})$ questions to get the information of the first $p(n)$ colors and pegs. Altogether for this part we use $\mathcal{O}(n^{1.525})$ questions.

For pairs of possible secrets with Hamming distance of at least $\sqrt{n}$ there are considerably more separating questions, so here we use a different approach. We transfer the problem to a vertex cover problem in a suitable hypergraph. We show that for a high Hamming distance, the edges of this hypergraph are sufficiently large, so one can find a vertex cover of size $\mathcal{O}(n^{1.5} \log n)$.

In Section 3.5 we complement our main result by a lower bound of $\Omega(n \log(n))$ questions. This is proved with the help of information theoretical arguments that are adapted from Doerr et al. [13].

Finally, in Section 3.6 we leave the field of static Mastermind and establish a lower bound of c questions for the adaptive semi AB-Game. To accomplish this, we transfer the worst case situation in the Mastermind game to a variant in which Codemaker is allowed to change the secret code during the game and present an appropriate Codemaker strategy.

For a better understanding, in Table 3.1 we give a short overview over recent upper and lower bounds for several Mastermind variants.

	Adaptive	Static
Classic	$\Omega(n)$	$\Omega(n \log n)$ [13]
AB-Game	$\Omega(n)$	$\Omega(n \log n)$

(a) Lower bounds.

	Adaptive	Static
Classic	$\mathcal{O}(n \log \log n)$ [13]	$\mathcal{O}(n \log n)$ [13]
AB-Game	$\mathcal{O}(n \log n)$ [14]	$\mathcal{O}(n^{1.525})$

(b) Upper bounds.

Table 3.1: Best known asymptotic bounds for different Mastermind variants with $p = c = n$. Bounds colored blue are proved in this chapter.

3.2 Preliminaries

3.2.1 The Rencontres number

To estimate the size of certain sets of questions, we will make use of the so-called *Rencontres number* that provides an exact formula for the number of permutations with a given number of fixpoints.

Definition 3.1. *For $k \in \{0, \dots, n\}$ the* Rencontres number $D_{n,k}$ *is defined as*

$$D_{n,k} := |\{Q \in S_n | Q \text{ has exactly } k \text{ fixpoints}\}|.$$

We need the following result from [32]. For completeness, we also present a combinatorial proof.

Lemma 3.2. *For every $n \in \mathbb{N}$ and $k \in \{0, \dots, n\}$ it holds*

$$D_{n,k} = \frac{n!}{k!} \sum_{i=0}^{n-k} \frac{(-1)^i}{i!}.$$

Proof. First of all, note that for all $k \in \{0, \dots, n\}$ we have $D_{n,k} = \binom{n}{k} D_{n-k,0}$: To count all permutations with exactly k fixpoints, we can first choose the fixpoints (which gives $\binom{n}{k}$ possibilities) and for every chosen set of points we have $D_{n-k,0}$ permutations that have exactly this set as set of fixpoints. Hence, to prove the lemma, it suffices to prove that for every $n \in \mathbb{N}$ it holds $D_{n,0} = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$, because then for all $k \in \{0, \dots, n\}$

$$D_{n,k} = \binom{n}{k} D_{n-k,0} = \binom{n}{k} (n-k)! \sum_{i=0}^{n-k} \frac{(-1)^i}{i!} = \frac{n!}{k!} \sum_{i=0}^{n-k} \frac{(-1)^i}{i!}.$$

We will use the fact that

$$\frac{n!}{i!} = \sum_{k=i}^{n} \binom{k}{i} D_{n,k}. \tag{3.1}$$

This can be seen by a simple counting argument. Suppose we want to count all permutations with at least i fixpoints. We have $\binom{n}{i}$ choices for i fixpoints and $(n-i)!$ possibilities to complete the permutation. This gives a total of $\binom{n}{i}(n-i)! = \frac{n!}{i!}$ permutations, but we counted several permutations more than once. To be more precise, for every $k \geq i$ a permutation with k fixpoints is counted $\binom{k}{i}$ times, giving the formula (3.1). It follows that

$$\begin{aligned} n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} &= \sum_{i=0}^{n} (-1)^i \frac{n!}{i!} \\ &\overset{(3.1)}{=} \sum_{i=0}^{n} (-1)^i \sum_{k=i}^{n} \binom{k}{i} D_{n,k} \\ &= \sum_{k=0}^{n} D_{n,k} \sum_{i=0}^{k} (-1)^i \binom{k}{i} \end{aligned}$$

and due to the binomial theorem we have $\sum_{i=0}^{k} (-1)^i \binom{k}{i} = (1-1)^k = 0$ for all $k > 0$, so finally we get

$$n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} = D_{n,0} \sum_{i=0}^{0} (-1)^i \binom{0}{i} = D_{n,0}$$

and the proof is complete. □

Corollary 3.3. *For all $k \leq n-2$ it holds $\frac{1}{3}\frac{n!}{k!} \leq D_{n,k} \leq \frac{1}{2}\frac{n!}{k!}$.*

Proof. Because of Lemma 3.2, it suffices to show that for all $N \geq 2$

$$\frac{1}{3} \leq \sum_{i=0}^{N} \frac{(-1)^i}{i!} \leq \frac{1}{2}. \tag{3.2}$$

This can be seen via induction over N. For $N = 2, 3$ we have $\sum_{i=0}^{2} \frac{(-1)^i}{i!} = \frac{1}{2}$ and $\sum_{i=0}^{3} \frac{(-1)^i}{i!} = \frac{1}{6}$. Now, let $N \geq 4$. If N is odd, we get

$$\sum_{i=0}^{N} \frac{(-1)^i}{i!} = \sum_{i=0}^{N-2} \frac{(-1)^i}{i!} + \frac{N-1}{(N-1)!} - \frac{N}{N!} \geq \sum_{i=0}^{N-2} \frac{(-1)^i}{i!}$$

and, on the other hand,

$$\sum_{i=0}^{N} \frac{(-1)^i}{i!} = \sum_{i=0}^{N-1} \frac{(-1)^i}{i!} - \frac{N}{N!} \leq \sum_{i=0}^{N-1} \frac{(-1)^i}{i!}.$$

By applying the induction hypothesis we are done. An analog proof works for even N. □

3.2.2 Questions and strategies

For $n \in \mathbb{N}$ let $[n] := \{1, \ldots, n\}$. For $r \in \mathbb{R}$ we define $[r] := \{1, \ldots, \lceil r \rceil\}$. Except for Section 3.6 we will only consider static permutation Mastermind with $p = c =: n$ pegs and colors, so every question as well as the secret code are permutations on $[n]$. For a question $Q \in S_n$ and a secret code $X \in S_n$ let

$$\mathrm{B}(Q, X) := |\{a \in [n] | Q(a) = X(a)\}|$$

be the number of black pegs that Codebreaker receives as answer to the question Q. For possible secrets X_1, X_2 we say that a question Q *separates* X_1 and X_2, if $\mathrm{B}(Q, X_1) \neq \mathrm{B}(Q, X_2)$. The *Hamming distance* $\Delta(X_1, X_2)$ of X_1 and X_2 is defined as

$$\Delta(X_1, X_2) = |\{a \in [n] : X_1(a) \neq X_2(a)\}|.$$

For $r \in \mathbb{N}$, an *r-strategy* is a set $T = \{Q_1, \ldots, Q_r\}$ of r questions. T is called *feasible* if for every pair $(X_1, X_2) \in (S_n)^2$ with $X_1 \neq X_2$ there exists $Q \in T$ that separates X_1 and X_2 (see Figure 3.1). Note that the feasible strategies are exactly the strategies that allow Codebreaker to determine every secret code: If there exist two distinct possible secret codes X_1 and X_2 such that none of the questions from T separates X_1 and X_2, then Codebreaker isn't able to distinguish X_1 from X_2, because in either case X_1 or X_2 being the secret code, Codebreaker receives exactly the same answers. On the other hand, if T is a feasible strategy, the answers to T determine the secret code, because a different choice for the secret leads to at least one different answer.

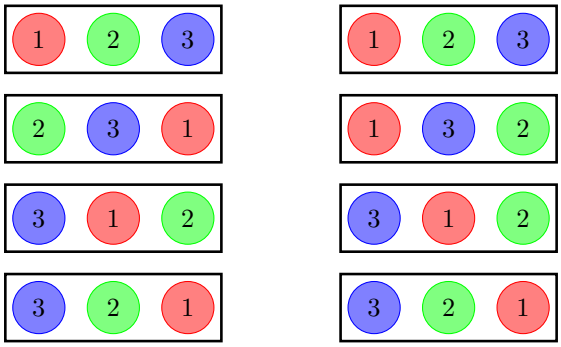

Figure 3.1: Two strategies for static permutation Mastermind with $n = 3$. The left strategy is infeasible, because the possible secrets $(2, 1, 3)$ and $(1, 3, 2)$ are not separated. The right strategy is feasible.

3.3 A feasible $\mathcal{O}(n^2)$-strategy

We start by presenting a technique that allows us to determine certain colors or positions. This technique will be used when constructing the strategy for our main result in Section 3.4, but also can be applied directly to obtain a quite simple strategy with $\mathcal{O}(n^2)$ questions, as done in Theorem 3.10.

Definition 3.4. *For $n \in \mathbb{N}_{\geq 3}$ define the following questions by starting with the identity function and only changing the mapping of two or three elements: Let $i, j, k \in [n]$ be pairwise distinct.*

$$\tau_{i,j} : [n] \longrightarrow [n], x \mapsto \begin{cases} j, & \text{if } x = i, \\ i, & \text{if } x = j, \\ x, & \text{otherwise.} \end{cases}$$

$$\sigma_{i,j,k} : [n] \longrightarrow [n], x \mapsto \begin{cases} j, & \text{if } x = i, \\ k, & \text{if } x = j, \\ i, & \text{if } x = k, \\ x, & \text{otherwise.} \end{cases}$$

Let I denote the identity function on $[n]$.

Note that

$$\sigma_{i,j,k} = \sigma_{j,k,i} = \sigma_{k,i,j}. \tag{3.3}$$

We will also use that $\tau_{i,j}^{-1} = \tau_{i,j}$ and $\sigma_{i,j,k}^{-1} = \sigma_{j,i,k}$ and $\sigma_{i,j,k} = \tau_{j,k} \circ \tau_{i,k}$.

When changing the mapping of two elements of a question, the difference of the answers is at most 2, so there are five cases to consider. We denote the exclusive disjunction of two events A and B by $A \oplus B := (A \wedge \neg B) \vee (\neg A \wedge B)$. For permutations $X_1, X_2 \in S_n$, by $X_1 \circ X_2$ we denote the usual composition of X_1 and X_2.

Observation 3.5. *Let $n \in \mathbb{N}_{\geq 3}$ and $i, j \in [n]$ be distinct. Let Q, X be permutations on $[n]$ and let $Q^{i,j} := \tau_{Q(i),Q(j)} \circ Q$.*

(i) $\mathrm{B}\left(Q^{i,j}, X\right) = \mathrm{B}(Q, X) + 2 \iff (Q(i) = X(j)) \wedge (Q(j) = X(i))$

(ii) $\mathrm{B}\left(Q^{i,j}, X\right) = \mathrm{B}(Q, X) + 1 \iff (Q(i) = X(j)) \oplus (Q(j) = X(i))$

(iii) $\mathrm{B}\left(Q^{i,j}, X\right) = \mathrm{B}(Q, X) + 0 \iff Q(i), Q(j) \notin \{X(i), X(j)\}$

(iv) $\mathrm{B}\left(Q^{i,j}, X\right) = \mathrm{B}(Q, X) - 1 \iff (Q(i) = X(i)) \oplus (Q(j) = X(j))$

(v) $\mathrm{B}\left(Q^{i,j}, X\right) = \mathrm{B}(Q, X) - 2 \iff (Q(i) = X(i)) \wedge (Q(j) = X(j))$

Proof. Let

$$b_1 := |\{a \in \{i, j\} | Q(a) = X(a)\}|$$

and

$$b_2 := |\{a \in \{i, j\} | \exists a' \in \{i, j\} \setminus \{a\} : Q(a) = X(a')\}|.$$

Hence, $b_2 = 0$ is equivalent to $X(i) \neq Q(j)$ and $X(j) \neq Q(i)$, whereas $b_2 = 2$ is equivalent to $X(i) = Q(j)$ and $X(j) = Q(i)$. Because Q and X are permutations, $b_1 > 0$ already implies $b_2 = 0$ and $b_2 > 0$ implies $b_1 = 0$. Straightforward calculation gives that

$$\mathrm{B}\left(Q^{i,j}, X\right) = |\{a \in [n] | Q^{i,j}(a) = X(a)\}| = |\{a \in [n] | Q(a) = X(a)\}| - b_1 + b_2.$$

Thus, $\mathrm{B}\left(Q^{i,j}, X\right) - \mathrm{B}\left(Q, X\right) = b_2 - b_1$. The following equivalences complete the proof.

$$\begin{aligned}
\text{For (i): } & b_2 - b_1 = 2 \Leftrightarrow b_2 = 2 \text{ and } b_1 = 0 \\
\text{For (ii): } & b_2 - b_1 = 1 \Leftrightarrow b_2 = 1 \text{ and } b_1 = 0 \\
\text{For (iii): } & b_2 - b_1 = 0 \Leftrightarrow b_2 = 0 \text{ and } b_1 = 0 \\
\text{For (iv): } & b_2 - b_1 = -1 \Leftrightarrow b_2 = 0 \text{ and } b_1 = 1 \\
\text{For (v): } & b_2 - b_1 = -2 \Leftrightarrow b_2 = 0 \text{ and } b_1 = 2
\end{aligned}$$

□

We will show that the questions introduced in Definition 3.4 suffice to construct a feasible strategy. The next lemmas provide some criteria to determine for given i, j whether peg i has color j.

Lemma 3.6. *Let $n \in \mathbb{N}$ and $i \in [n]$. Let X be a possible secret on $[n]$. Then, $X(i) = i$ if and only if $\mathrm{B}(\tau_{i,j}, X) < \mathrm{B}(I, X)$ for all $j \in [n] \backslash \{i\}$.*

Proof. "⇒": Let $X(i) = i$ and $j \in [n] \setminus \{i\}$. We apply Observation 3.5 with $Q = I$ and $Q^{i,j} = \tau_{i,j}$. Because $X(i) = i$, we are in case (iv) or (v) of Observation 3.5, so we have $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(Q^{i,j}, X) < \mathrm{B}(Q, X) = \mathrm{B}(I, X)$.

"⇐": Let $\mathrm{B}(\tau_{i,j}, X) < \mathrm{B}(I, X)$ for all $j \in [n] \backslash \{i\}$. Then with Observation 3.5 (iv),(v) we get $X(i) = i$ or $X(j) = j$ for all $j \in [n] \backslash \{i\}$. But in the second case the only color left for peg i is color i, so $X(i) = i$. □

The next two lemmas provide criteria under which for a secret X and $i, j \in [n]$ it holds $X(i) = j$. The proofs are sophisticated applications of Observation 3.5.

Lemma 3.7. *Let $n \in \mathbb{N}_{\geq 3}$ and $i, j, k \in [n]$ be pairwise distinct. Let X be a possible secret on $[n]$. Then, $X(i) = j$ if and only if one of the following conditions holds:*

(i) $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(I, X) + 2$

(ii) $\mathrm{B}(\sigma_{i,j,k}, X) = \mathrm{B}(\tau_{i,k}, X) + 2$

(iii) $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(I, X) + 1$ *and* $\mathrm{B}(\sigma_{i,j,k}, X) = \mathrm{B}(\tau_{i,k}, X) + 1$

Proof. "⇒": Let $X(i) = j$ and let (i) and (ii) not be fulfilled. We show that (iii) is fulfilled. For the first equation we apply Observation 3.5 with $Q = I$ and $Q^{i,j} = \tau_{i,j}$. Because $X(i) = j = Q(j)$, only cases (i) or (ii) of Observation 3.5 can be fulfilled and because $\mathrm{B}(Q^{i,j}, X) = \mathrm{B}(\tau_{i,j}, X) \neq \mathrm{B}(I, X) + 2 = \mathrm{B}(Q, X) + 2$ by our assumption, only case (ii) of Observation 3.5 is left and we get $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(Q^{i,j}, X) = \mathrm{B}(Q, X) + 1 = \mathrm{B}(I, X) + 1$.

The second equation follows analogously by applying Observation 3.5 with $Q = \tau_{i,k}$ and $Q^{i,j} = \tau_{k,j} \circ \tau_{i,k} = \sigma_{i,j,k}$.

"⇐": We show for each of the conditions (i),(ii) and (iii) that they imply $X(i) = j$.

(i). Let $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(I, X) + 2$. We apply Observation 3.5 (i) with $Q = I$ and $Q^{i,j} = \tau_{i,j}$ and get $X(i) = Q(j) = j$.

(ii). Let $\mathrm{B}(\sigma_{i,j,k}, X) = \mathrm{B}(\tau_{i,k}, X) + 2$. We apply Observation 3.5 (i) with $Q = \tau_{i,k}$ and $Q^{i,j} = \tau_{k,j} \circ \tau_{i,k} = \sigma_{i,j,k}$ and get $X(i) = Q(j) = j$.

(iii). Let $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(I, X) + 1$ and $\mathrm{B}(\sigma_{i,j,k}, X) = \mathrm{B}(\tau_{i,k}, X) + 1$. We apply Observation 3.5 (ii) with $Q = I$ and $Q^{i,j} = \tau_{i,j}$ and get that either $X(j) = Q(i) = i$ or $X(i) = Q(j) = j$, so

$$\text{either } X(j) = i \text{ or } X(i) = j. \tag{3.4}$$

Further we apply Observation 3.5 (ii) with $Q = \tau_{i,k}$ and $Q^{i,j} = \tau_{k,j} \circ \tau_{i,k} = \sigma_{i,j,k}$ and get that either $X(j) = Q(i) = k$ or $X(i) = Q(j) = j$, so

$$\text{either } X(j) = k \text{ or } X(i) = j. \tag{3.5}$$

Now assume for a moment that $X(i) \neq j$. Then, (3.4) and (3.5) imply that $i = X(j) = k$, a contradiction. □

In the following lemma we show that the same result can be achieved with the question $\sigma_{j,i,k}$ instead of the question $\sigma_{i,j,k}$. The proof is very similar to the proof of Lemma 3.7.

Lemma 3.8. *Let $n \in \mathbb{N}_{\geq 3}$ and $i, j, k \in [n]$ be distinct. Let X be a possible secret on $[n]$. Then, $X(i) = j$ if and only if one of the following conditions holds:*

(i) $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(I, X) + 2$,

(ii) $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(\sigma_{j,i,k}, X) + 2$,

(iii) $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(\sigma_{j,i,k}, X) + 1$ *and* $\mathrm{B}(\tau_{i,k}, X) \geq \mathrm{B}(I, X)$.

Proof. "⇒": Let $X(i) = j$ and let (i) and (ii) not be fulfilled. We show that (iii) is fulfilled. First, we apply Observation 3.5 with $Q = \sigma_{j,i,k}$ and $Q^{i,k} = \tau_{j,k} \circ \sigma_{j,i,k} = \tau_{i,j}$. Because $X(i) = j = Q(k)$, only cases (i) or (ii) of Observation 3.5 can be fulfilled and because $\mathrm{B}(Q^{i,k}, X) = \mathrm{B}(\tau_{i,j}, X) \neq \mathrm{B}(\sigma_{j,i,k}, X)+2 = \mathrm{B}(Q, X)+2$ by our assumption, only case (ii) of Observation 3.5 is left. So we get $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(Q^{i,k}, X) = \mathrm{B}(Q, X) + 1 = \mathrm{B}(\sigma_{j,i,k}, X) + 1$. Since we are in case (ii) of Observation 3.5, we also know that either $X(k) = Q(i) = k$ or $X(i) = Q(k) = j$, so by our assumption we have $X(k) \neq k$. We will use this to prove that $\mathrm{B}(\tau_{i,k}, X) \geq \mathrm{B}(I, X)$. We apply Observation 3.5 with $Q = I$ and $Q^{i,k} = \tau_{i,k}$. Because $X(k) \neq k = Q(k)$ we have to be in case (i),(ii) or (iii) of Observation 3.5. All cases imply $\mathrm{B}(\tau_{i,k}, X) \geq \mathrm{B}(I, X)$.

"⇐": We show for each of the conditions (i),(ii) and (iii) that they imply $X(i) = j$.

(i). The condition is the same as Lemma 3.7 (i).

(ii). Let $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(\sigma_{j,i,k}, X) + 2$. By Observation 3.5 (i) with $Q = \sigma_{j,i,k}$ and $Q^{i,k} = \tau_{j,k} \circ \sigma_{j,i,k} = \tau_{i,j}$ we get $X(i) = Q(k) = j$.

(iii). Let $\mathrm{B}(\tau_{i,j}, X) = \mathrm{B}(\sigma_{j,i,k}, X) + 1$ and $\mathrm{B}(\tau_{i,k}, X) \geq \mathrm{B}(I, X)$. First we apply Observation 3.5 (ii) with $Q = \sigma_{j,i,k}$ and $Q^{i,k} = \tau_{i,j}$ and get that either $X(i) = Q(k) = j$ or $X(k) = Q(i) = k$, so it is left to prove that $X(k) \neq k$. To see this, we apply Observation 3.5 with $Q = I$ and $Q^{i,k} = \tau_{i,k}$. Because $\mathrm{B}(Q^{i,k}, X) = \mathrm{B}(\tau_{i,k}, X) \geq \mathrm{B}(I, X) = \mathrm{B}(Q, X)$, we are in case (i),(ii) or (iii) of Observation 3.5. All cases imply $X(k) \neq Q(k) = k$. □

Example 1. *We explain the intuition behind the proof of Lemma 3.8 by an example. Suppose* $n = 6$ *and* $X \in S_6$ *is a secret. We want to find out whether peg* 2 *has color* 3*, that is,* $X(2) = 3$*. For this we use the answers to the four questions* $I, \tau_{2,3}, \sigma_{3,2,5}$ *and* $\tau_{2,5}$ *as depicted in Figure 3.3. Note that Lemma 3.8 requires some question* $\sigma_{3,2,k}$ *for*

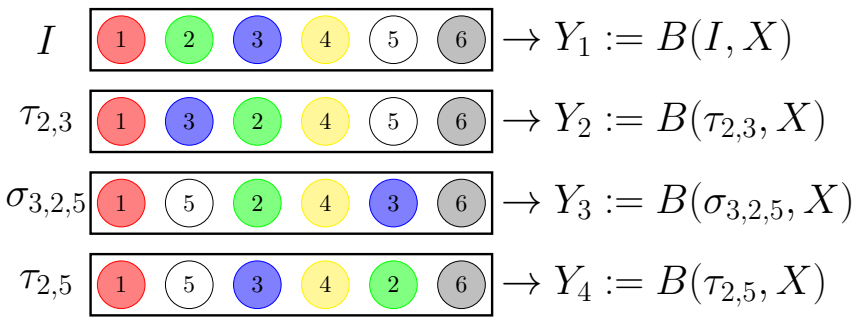

Figure 3.2: These four questions are sufficient for finding out whether peg 2 has color 3.

some $k \in \{1, 4, 5, 6\}$ *and not necessarily the question* $\sigma_{3,2,5}$*, so in general we might have to replace the third question and change the fourth question accordingly. We denote the answers to these four questions by* $Y_1, \ldots, Y_4$.

If $Y_2 - Y_1 \leq 0$*, it is easily seen that* $X(2) \neq 3$*: The second question* $\tau_{2,3}$ *emerges from the first question* I *by only swapping the colors* 2 *and* 3*. This implies that if one of*

the colors is swapped to its correct position, the total number of correctly placed colors has to increase.

If $Y_2 - Y_1 = 2$ *we know that* $X(2) = 3$ *((i) in Lemma 3.8). So the only problematic case is* $Y_2 - Y_1 = 1$. *In this case there are two possible* disjoint *sub-cases to consider:*

$$\text{either Case A: } X(2) = 3 \qquad \text{or Case B: } X(3) = 2$$

We use Y_3 *to further specify the cases A and B. Note that* $\sigma_{3,2,5} = \tau_{3,5} \circ \tau_{2,3}$.

If $Y_3 - Y_2 \geq 0$, *as above this directly implies that* $X(2) \neq 3$. *If* $Y_3 - Y_2 = -2$, *we know that* $X(2) = 3$ *((ii) in Lemma 3.8). So again, there is just one problematic sub-case, namely* $Y_3 - Y_2 = -1$. *Then, either* $X(2) = 3$ *(so we are in Case A) or* $X(5) = 5$. *Since the latter case excludes Case A, consequently we are in Case B. So the two possible cases left are*

- *Case A:* $X(2) = 3$ *and* $X(5) \neq 5$.
- *Case B:* $X(3) = 2$ *and* $X(5) = 5$.

Finally, with the help of Y_4 *we are able to decide in which case we are: If* $Y_4 - Y_1 \geq 0$, *we can deduce that* $X(5) \neq 5$, *because again the 4-th question* $\tau_{2,5}$ *emerges from the first question I by swapping two colors. Hence, we are in Case A and we are done ((iii) in Lemma 3.8). If* $Y_4 - Y_1 < 0$, *we know that either* $X(2) = 2$ *or* $X(5) = 5$. *Peg 2 cannot have color 2, because either* $X(3) = 2$ *or* $X(2) = 3$. *Hence,* $X(5) = 5$ *and we are in Case B, so we are done.*

Next, we introduce a strategy that enables us to find out the positions of certain fixed colors as well as the colors of certain fixed positions.

Lemma 3.9. *Let* $n \in \mathbb{N}_{\geq 3}$ *and* $t \in [n]$. *Define*

$$\begin{aligned} T_\tau &:= \{\tau_{i,j} | i \in \{t+1, \ldots, n\}, j \in [n], i \neq j\} \\ T_\sigma &:= \{\sigma_{i,j,1} | i \in \{t+1, \ldots, n\}, j \in \{2, \ldots, n\}, i \neq j\} \\ T &:= \{I\} \cup T_\tau \cup T_\sigma. \end{aligned}$$

Then for all $X_1, X_2 \in S_n$ *the following holds: If no question from* T *separates* X_1 *and* X_2, *then*

$$X_1(i) = X_2(i) \quad \text{for all } i \in \{t+1, \ldots, n\}$$

and

$$X_1^{-1}(j) = X_2^{-1}(j) \quad \text{for all } j \in \{t+1, \ldots, n\}.$$

Proof. Let X_1 and X_2 be possible secrets, such that no question from T separates X_1 and X_2. For the first property, let $i \in \{t+1, \ldots, n\}$ and $j := X_1(i)$. If $j = i$, by Lemma 3.6 we have $\mathrm{B}(\tau_{i,j}, X_1) < \mathrm{B}(I, X_1)$ for all $j \in [n] \setminus \{i\}$. Because T does not separate X_1 and X_2, also $\mathrm{B}(\tau_{i,j}, X_2) < \mathrm{B}(I, X_2)$ for all $j \in [n] \setminus \{i\}$ and by applying Lemma 3.6 once more, we get $X_2(i) = i$.

Now let $j \neq i$. First we show that there exists $k \neq i, j$ with $\sigma_{i,j,k} \in T$ or $\sigma_{j,i,k} \in T$. For $j \neq 1$, we set $k := 1$ and get $\sigma_{i,j,k} = \sigma_{i,j,1} \in T$. For $j = 1$, choose $k \in \{2, \ldots, n\} \setminus \{i\}$ arbitrarily. It follows that

$$\sigma_{j,i,k} \overset{(3.3)}{=} \sigma_{i,k,j} = \sigma_{i,k,1} \in T.$$

We distinguish two cases: If $\sigma_{i,j,k} \in T$ for some k, one of the conditions (i)-(iii) in Lemma 3.7 has to be fulfilled for i, j, k and X_1. Because all the permutations $I, \tau_{i,j}, \tau_{i,k}$ and $\sigma_{i,j,k}$ are contained in T and T does not separate X_1 and X_2, the same condition holds for X_2 and hence $X_2(i) = j$. If $\sigma_{j,i,k} \in T$ for some k, we can apply Lemma 3.8 with analog arguments and also get $X_2(i) = j$.

For the second property, let $j \in \{t+1, \ldots, n\}$ and let $i := X_1^{-1}(j)$, so that $X(i) = j$. The case $i = j$ was already handled, so let $i \neq j$. As above, we find $k \neq i, j$ with $\sigma_{i,j,k} \in T$ or $\sigma_{j,i,k} \in T$ (just swap the roles of i and j there) and thereby obtain $X_2^{-1}(j) = i$. □

Theorem 3.10. *For every $n \in \mathbb{N}$ there exists a feasible $\frac{3}{2}n^2$-strategy for static permutation Mastermind.*

Proof. For $n \leq 2$ one arbitrary question suffices, so let $n \geq 3$. We apply Lemma 3.9 with $t = 1$: The corresponding strategy T is feasible, because for every pair of possible secrets (X_1, X_2) with $X_1 \neq X_2$ there exists $i \in \{2, \ldots, n\}$ with $X_1(i) \neq X_2(i)$, hence T separates X_1 and X_2. The number of questions in T is $|T| = 1 + |T_\tau| + |T_\sigma| = 1 + \frac{n(n-1)}{2} + (n-1)(n-2) < \frac{3}{2}n^2$. □

3.4 A feasible $\mathcal{O}(n^{1.525})$-strategy

For improving the upper bound of $\mathcal{O}(n^2)$ questions, we will classify the pairs of possible secrets into two types: pairs with a low Hamming distance and pairs with a high Hamming distance. For each type we present a strategy that separates all pairs of this kind. By combining the questions of both strategies, we finally construct a feasible strategy with $\mathcal{O}(n^{1.525})$ questions.

3.4.1 Possible secrets with low Hamming distance

In this subsection we explain how to separate pairs of possible secrets with low Hamming distance, i.e., a Hamming distance at most $\sqrt{n}$.

Definition 3.11. *For $m, t \in \mathbb{N}$ we denote by* $\mathrm{rem}_t(m)$ *the* remainder *of the Euclidean division of m by t, i.e., the unique integer $r \in \{0, \ldots, n-1\}$ such that there exists $q \in \mathbb{Z}$ with $m = q \cdot t + r$.*

We need some well-known properties of the remainder.

Lemma 3.12. *Let $t, k, l \in \mathbb{N}$ and $m \in \mathbb{Z}$.*

(i) $\mathrm{rem}_t(k) = \mathrm{rem}_t(l) \Longrightarrow \mathrm{rem}_t(k+m) = \mathrm{rem}_t(l+m)$.

(ii) *Let $s, s' \in [t-1]$ with $s \neq s'$. If t and k are co-prime, it holds*

$$\mathrm{rem}_t(s \cdot k + m) \neq \mathrm{rem}_t(s' \cdot k + m).$$

(iii) $\mathrm{rem}_t(k + \mathrm{rem}_t(l)) = \mathrm{rem}_t(k + l)$.

Proof. (i). Let $r := \mathrm{rem}_t(k) = \mathrm{rem}_t(l)$. Then there exist $q, q' \in \mathbb{Z}$ such that $k = q \cdot t + r$ and $l = q' \cdot t + r$. Moreover, there exist $q'' \in \mathbb{Z}$ and $r'' \in \{0, \ldots, t-1\}$ with $m = q'' \cdot t + r''$. We get $k + m = (q + q'')t + r + r''$ and $l + m = (q' + q'')t + r + r''$, so

$$\mathrm{rem}_t(k + m) = \mathrm{rem}_t(r + r') = \mathrm{rem}_t(l + m).$$

(ii). We prove the claim for $m = 0$, the general case then follows with (i). Assume that $\mathrm{rem}_t(s \cdot k) = \mathrm{rem}_t(s' \cdot k) =: r$. Then there exist $q, q' \in \mathbb{Z}$ with $s \cdot k = q \cdot t + r$ and $s' \cdot k = q' \cdot t + r$. This implies $(s - s')k = (q - q')t$. Because $-t + 1 < (s - s') < t - 1$ and $(s - s') \neq 0$, we know that t does not divide $(s - s')$, so t and k can't be co-prime.

(iii). The definition of the remainder directly implies that $\mathrm{rem}_t(l) = \mathrm{rem}_t(\mathrm{rem}_t(l))$. We apply (i) with $\mathrm{rem}_t(l)$ instead of k and k instead of m and are done. □

Definition 3.13. *Let $n \in \mathbb{N}$, $t \leq n$ be a prime, $k \in [t-1]$ and $l \in \{0, 1, \ldots, t-1\}$. Define the question $P(n, t, k, l) : [n] \longrightarrow [n]$ as*

$$P(n, t, k, l)(a) := \begin{cases} \mathrm{rem}_t(k \cdot a + l) + 1, & \text{if } a \leq t, \\ a, & \text{if } a > t. \end{cases}$$

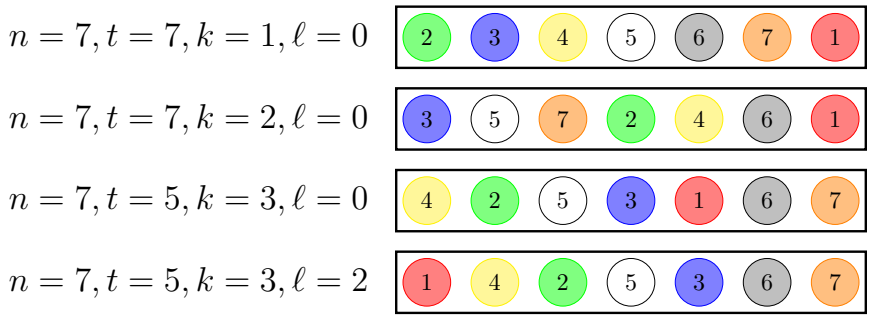

Figure 3.3: Some examples for questions $P(n, t, k, \ell)$.

Lemma 3.14. *For n, t, k, l as above, $P(n, t, k, l)$ is a permutation.*

Proof. We show that $P(n, t, k, l)$ is injective. Let $a, a' \in [t]$ with $a \neq a'$. We have $P(n, t, k, l)(a) = \mathrm{rem}_t(k \cdot a + l) + 1 \leq t$ and the same holds for a', so it remains to prove that $P(n, t, k, l)(a) \neq P(n, t, k, l)(a')$. Because $k < t$ and t is a prime, k and t are co-prime. Hence, by Lemma 3.12 (ii), we get

$$P(n, t, k, l)(a) = \mathrm{rem}_t(k \cdot a + l) + 1 \neq \mathrm{rem}_t(k \cdot a' + l) + 1 = P(n, t, k, l)(a'),$$

so $P(n, t, k, l)$ is injective. Because $P(n, t, k, l)$ is a mapping between finite sets, it is also bijective. □

The questions of the type $P(n,t,k,l)$ turn out to be very useful when separating pairs of secrets with low Hamming distance. The following two lemmas show how this separation works.

Lemma 3.15. *Let $n \in \mathbb{N}$ and $X_1, X_2 \in S_n$ be possible secrets with $h := \Delta(X_1, X_2)$. Let $A := \{a_1, \dots, a_h\}$ denote the set of pegs on which X_1 and X_2 have different colors. Let $Q \in S_n$ be a question with $Q(a_1) = X_1(a_1)$ and $Q(a) \neq X_2(a)$ for all $a \in A$. Then Q separates X_1 and X_2.*

Proof. By definition,

$$\begin{aligned}\mathrm{B}(Q,X_1) - \mathrm{B}(Q,X_2) &= |\{a \in [n] | Q(a) = X_1(a)\}| - |\{a \in [n] | Q(a) = X_2(a)\}| \\ &= |\{a \in A | Q(a) = X_1(a)\}| - \underbrace{|\{a \in A | Q(a) = X_2(a)\}|}_{=0} \\ &= |\{a \in A | Q(a) = X_1(a)\}| \overset{a_1 \in A}{\geq} 1.\end{aligned}$$

Hence, $\mathrm{B}(Q,X_1) \neq \mathrm{B}(Q,X_2)$ and thus Q separates X_1 and X_2. □

Lemma 3.16. *Let $n \in \mathbb{N}$, $t \in \{\lceil \sqrt{n} \rceil, \dots, n\}$ be a prime and $X_1, X_2 \in S_n$ be possible secrets with $2 \leq h := \Delta(X_1, X_2) \leq \sqrt{n}$. If $X_1^{-1}(b) = X_2^{-1}(b)$ for every $b \in \{t+1, \dots, n\}$ and there is a peg $a \in [t]$ with $X_1(a) \neq X_2(a)$, then there exist $k \in [\lceil \sqrt{n} \rceil]$ and $l \in [t-1] \cup \{0\}$ such that $P(n,t,k,l)$ separates X_1 and X_2.*

Proof. Let $a_1, \dots, a_h$ be the pegs with $X_1(a_i) \neq X_2(a_i)$ and w.l.o.g. let $a_1 \in [t]$. For $i \in [h]$ let $b_i := X_1(a_i)$. Note that $b_i \in [t]$ for all $i \in [h]$, because otherwise $a_i = X_1^{-1}(b_i) = X_2^{-1}(b_i) = X_2^{-1}(X_1(a_i))$ in contradiction to $X_1(a_i) \neq X_2(a_i)$. For every $k \in [\sqrt{n}]$ let $l(k) := \mathrm{rem}_t(b_1 - 1 - k \cdot a_1)$ let $P_k := P(n,t,k,l(k))$. We show that there exists $k \in [\sqrt{n}]$ such that P_k fulfills the conditions of Lemma 3.15. For every $a \in [t]$ we get

$$\begin{aligned}P_k(a) &= \mathrm{rem}_t(k \cdot a + l(k)) + 1 \\ &= \mathrm{rem}_t(k \cdot a + \mathrm{rem}_t(b_1 - 1 - k \cdot a_1)) + 1 \\ &= \mathrm{rem}_t(k \cdot a + b_1 - 1 - k \cdot a_1) + 1 && \text{(Lemma 3.12 (iii))} \\ &= \mathrm{rem}_t(k \cdot (a - a_1) + b_1 - 1) + 1.\end{aligned}$$

Further, because t is a prime, for every $a \in [t] \setminus \{a_1\}$ the integers t and $a - a_1$ are co-prime. We apply Lemma 3.12 (ii) and get for all $k' \neq k$ and all $2 \leq i \leq h$

$$P_k(a_i) = \mathrm{rem}_t(k \cdot (a_i - a_1) + b_1 - 1) + 1 \neq \mathrm{rem}_t(k' \cdot (a_i - a_1) + b_1 - 1) + 1 = P_{k'}(a_i).$$

Hence, for every $i \in \{2, \dots, h\}$ there exists at most one $k \in [\sqrt{n}]$ with $P_k(a_i) = b_i$. Because $h \leq \lfloor \sqrt{n} \rfloor$, we conclude by the pigeonhole principle that there is at least one $k^* \in [\sqrt{n}]$ with $P_{k^*}(a_i) \neq b_i$ for all $2 \leq i \leq h$. Moreover we have

$$P_{k^*}(a_1) = \mathrm{rem}_t(k^* \cdot (a_1 - a_1) + b_1 - 1) + 1 = \mathrm{rem}_t(b_1 - 1) + 1 = b_1,$$

so P_{k^*} fulfills the conditions of Lemma 3.15 and hence separates X_1 and X_2. □

With the questions from Definition 3.4 and 3.13 we can construct a strategy that separates all pairs of possible secrets with low Hamming distance.

Lemma 3.17. *Let $n \in \mathbb{N}$ be sufficiently large. Let $t \in [n]$ be the largest prime with $t \leq n$ and let T_1 be the corresponding strategy from Lemma 3.9. Moreover, let $T_2 := \{P(n,t,k,l) | k \in [\sqrt{n}], l \in \{0,\dots,t-1\}\}$. Then, the strategy $T := T_1 \cup T_2$ has $\mathcal{O}\left(\max\{\sqrt{n}\cdot t, n\cdot(n-t)\}\right)$ questions and every pair $X_1, X_2 \in S_n$ with $2 \leq \Delta(X_1,X_2) \leq \sqrt{n}$ is separated by at least one question from T.*

Proof. We have

$$\begin{aligned}|T| \leq |T_1| + |T_2| &= 1 + \tfrac{(n-t)(n-1)}{2} + (n-t)(n-2) + \left\lceil \sqrt{n} \right\rceil t \\ &= \mathcal{O}\left(\max\{\sqrt{n}\cdot t, n\cdot(n-t)\}\right).\end{aligned}$$

For the second property let X_1, X_2 be a pair of possible secrets with $2 \leq \Delta(X_1,X_2) \leq \sqrt{n}$. If there is an $i \in \{t+1,\dots,n\}$ with $X_1(i) \neq X_2(i)$ or $X_1^{-1}(i) \neq X_2^{-1}(i)$, by Lemma 3.9 at least one question from T separates X_1 and X_2. Otherwise, there exists a color $a \in [t]$ with $X_1(a) \neq X_2(a)$, because $X_1 \neq X_2$. Hence, X_1 and X_2 fulfill the properties of Lemma 3.16 and at least one question from T_2 separates X_1 and X_2. □

For further specifying the bound in Lemma 3.17 we need an upper bound for the difference of consecutive primes. For the next theorem we use the following result of Baker et al.

Lemma 3.18 (Theorem 1 in [4])**.** *There exists $x_0 \in \mathbb{N}$ such that for all $x \geq x_0$ the interval $[x - x^{0.525}, x]$ contains at least one prime number.*

Theorem 3.19. *Let $n \in \mathbb{N}$ be sufficiently large.*

a) There exists a strategy T with $\mathcal{O}(n^{1.525})$ questions such that every pair $(X_1,X_2) \in S_n^2$ with $2 \leq \Delta(X_1,X_2) \leq \sqrt{n}$ is separated by at least one question from T.

b) If n is a prime, T has $\mathcal{O}(n^{1.5})$ questions.

Proof. Strategy T from Lemma 3.17 contains $\mathcal{O}\Big(\max\left\{\sqrt{n}\cdot t, n(n-t)\right\}\Big)$ questions, where t is the largest prime with $t \leq n$. If n is a prime, we have $n - t = 0$, so there are $\mathcal{O}\left(n^{1.5}\right)$ questions. In general, $\sqrt{n}\cdot t \leq n^{1.5}$ and $n\cdot(n-t) \leq n^{1.525}$ due to Lemma 3.18. □

3.4.2 Possible secrets with high Hamming distance

We have yet to separate pairs of possible secrets with a Hamming distance of $h \geq \sqrt{n}$. We reformulate this case as a vertex cover problem in hypergraphs.

A *hypergraph* is a pair $\mathcal{H} = (V, \mathcal{E})$, where V is a finite set and $\mathcal{E}$ is a set of subsets of V. We call elements of V vertices and the elements of $\mathcal{E}$ edges. A *vertex cover* is a subset $U \subseteq V$ such that every edge $E \in \mathcal{E}$ contains at least one vertex of U. For a detailed description see, e.g., [33].

We start by showing that for every pair there is a relatively large number of separating questions. Let $n \in \mathbb{N}$. We define the hypergraph $\mathcal{H} = (V, \mathcal{E})$ as follows:

- $V := S_n$ is the set of all possible questions.
- For every pair of possible secrets X_1, X_2 with $\Delta(X_1, X_2) \geq \sqrt{n}$, we create an edge $E_{X_1,X_2} := \{Q \in S_n | \mathrm{B}(Q, X_1) \neq \mathrm{B}(Q, X_2)\}$ consisting of all questions Q separating X_1 and X_2.
- Let $\mathcal{E} := \{E_{X_1,X_2} | X_1, X_2 \in S_n, \Delta(X_1, X_2) \geq \sqrt{n}\}$.

Note that every vertex cover T of $\mathcal{H}$ is a set of questions such that for every pair of secrets X_1, X_2 with $\Delta(X_1, X_2) \geq \sqrt{n}$ there exists at least one question in T that separates X_1 and X_2. Hence, T is a strategy that separates all pairs with high Hamming distance. So our aim in this subsection is to find a small vertex cover of $\mathcal{H}$.

Intuitively it seems quite obvious that a pair of secrets with a high Hamming distance has more questions that separate this pair than a pair with low Hamming distance. Transferred to the vertex cover problem this means that for pairs with high Hamming distance, the constructed edges are relatively big. We will prove this intuition with the next two lemmas.

Lemma 3.20. *Let $X \in S_n$. Define $A := \{Q \in S_n | \Delta(Q, X) = n\}$ and for any peg $a \in [n]$ and any color $b \in [n]$ let $B_{a,b} := \{Q \in S_n | Q(a) = b\}$. Then,*

(i) $|A \cap B_{a,b}| = \frac{1}{n-1} \cdot |A|$ *for any* $a \in [n], b \in [n] \setminus \{X(a)\}$

(ii) $|A \cap B_{a,b} \cap B_{a^*,b^*}| \leq \frac{1}{(n-1)(n-3)} \cdot |A|$ *for any* $a, a^* \in [n], b, b^* \in [n]$ *with* $a \neq a^*, b \neq b^*$.

Proof. (i): We start with proving

$$|A \cap B_{a,b_1}| = |A \cap B_{a,b_2}| \text{ for all } a \in [n], b_1, b_2 \in [n] \setminus \{X(a)\}. \tag{3.6}$$

Let $a \in [n]$ and $b_1, b_2 \in [n] \setminus \{X(a)\}$. If $b_1 = b_2$, there is nothing to show, so let us assume $b_1 \neq b_2$. Let $D := \{Y \in A \cap B_{a,b_1} | Y^{-1}(b_2) \neq X^{-1}(b_1)\}$, $E := \{Y \in A \cap B_{a,b_1} | Y^{-1}(b_2) = X^{-1}(b_1)\}$ and consider the function $\varphi : A \cap B_{a,b_1} \to S_n$ defined by

$$\varphi(Y) = \begin{cases} \tau_{b_1,b_2} \circ Y & \text{on } D \\ \sigma_{b_1,b_2,Y \circ X^{-1}(b_2)} \circ Y & \text{on } E \end{cases}.$$

We show that φ is injective and $\varphi(A \cap B_{a,b_1}) \subseteq A \cap B_{a,b_2}$. This implies $|A \cap B_{a,b_1}| \leq |A \cap B_{a,b_2}|$ and because b_1 and b_2 have been chosen arbitrarily from $[n] \setminus \{X(a)\}$, we also get $|A \cap B_{a,b_2}| \leq |A \cap B_{a,b_1}|$, implying (3.6). Clearly, $\varphi|_D$ and $\varphi|_E$ are injective functions. In the following we show $\varphi(D) \cap \varphi(E) = \emptyset$. Let $Q \in \varphi(D)$, then $Q = \tau_{b_1,b_2} \circ Y$ for some $Y \in D$ and hence

$$Q^{-1}(b_1) = Y^{-1} \circ (\tau_{b_1,b_2})^{-1}(b_1) = Y^{-1} \circ \tau_{b_1,b_2}(b_1) = Y^{-1}(b_2) \neq X^{-1}(b_2),$$

where the last statement follows from $\Delta(Y, X) = n$, as $Y \in A$. On the other hand, for $Q' \in \varphi(E)$ we have $Q' = \sigma_{b_1,b_2,Y' \circ X^{-1}(b_2)} \circ Y'$ for some $Y' \in E$, so

$$\begin{aligned}(Q')^{-1}(b_1) &= (Y')^{-1} \circ \left(\sigma_{b_1,b_2,Y' \circ X_1^{-1}(b_2)}\right)^{-1}(b_1) \\ &= (Y')^{-1} \circ \sigma_{b_2,b_1,Y' \circ X_1^{-1}(b_2)}(b_1) \\ &= (Y')^{-1} \circ Y' \circ X^{-1}(b_2) \\ &= X^{-1}(b_2).\end{aligned}$$

Hence, $Q \neq Q'$ and therefore $\varphi(D) \cap \varphi(E) = \emptyset$, so φ is injective.

Next we show $\varphi(A \cap B_{a,b_1}) \subseteq A \cap B_{a,b_2}$ by showing $\varphi(D) \subseteq A \cap B_{a,b_2}$ and $\varphi(E) \subseteq A \cap B_{a,b_2}$.

"$\varphi(D) \subseteq A \cap B_{a,b_2}$": Let $Q \in \varphi(D)$, then $Q = \tau_{b_1,b_2} \circ Y$ for some $Y \in D$. For any $a' \in [n] \setminus \{Y^{-1}(b_1), Y^{-1}(b_2)\}$ we have $Q(a') = Y(a') \neq X(a')$ (because $Y \in A$). Moreover, we have

$$\begin{aligned}Q\left(Y^{-1}(b_1)\right) &= \tau_{b_1,b_2}(b_1) \\ &= b_2 \\ &\neq X(a) && (b_2 \in [n] \setminus \{X(a)\}) \\ &= X\left(Y^{-1}(b_1)\right) && (Y \in B_{a,b_1})\end{aligned}$$

and

$$\begin{aligned}Q\left(Y^{-1}(b_2)\right) &= \tau_{b_1,b_2}(b_2) \\ &= b_1 \\ &= X\left(X^{-1}(b_1)\right) \\ &\neq X\left(Y^{-1}(b_2)\right). && (Y \in D)\end{aligned}$$

Hence, $Q \in A$. We already showed that $Q(a) = Q\left(Y^{-1}(b_1)\right) = b_2$, so $Q \in B_{a,b_2}$.

"$\varphi(E) \subseteq A \cap B_{a,b_2}$": Let $Q \in \varphi(E)$. Then, $Q = \sigma_{b_1,b_2,Y \circ X^{-1}(b_2)} \circ Y$ for some $Y \in E$. For any $a' \in [n] \setminus \{Y^{-1}(b_1), Y^{-1}(b_2), X^{-1}(b_2)\}$ we have $Q(a') = Y(a') \neq X(a')$, because $Y \in A$. For the three remaining pegs we have

$$\begin{aligned}Q\left(Y^{-1}(b_1)\right) &= \sigma_{b_1,b_2,Y \circ X^{-1}(b_2)}(b_1) \\ &= b_2 \\ &\neq X(a) && (b_2 \in [n] \setminus \{X(a)\}) \\ &= X\left(Y^{-1}(b_1)\right), && (Y \in B_{a,b_1})\end{aligned}$$

$$\begin{aligned} Q\left(Y^{-1}(b_2)\right) &= \sigma_{b_1,b_2,Y\circ X^{-1}(b_2)}(b_2) \\ &= Y \circ X^{-1}(b_2) \\ &\neq Y(a) && (b_2 \in [n]\backslash\{X(a)\}) \\ &= b_1 && (Y \in B_{a,b_1}) \\ &= X\left(Y^{-1}(b_2)\right), && (Y \in E) \end{aligned}$$

$$\begin{aligned} Q\left(X^{-1}(b_2)\right) &\neq Q(a) && (b_2 \in [n]\backslash\{X(a)\}) \\ &= Q \circ Y^{-1}(b_1) && (Y \in B_{a,b_1}) \\ &= \sigma_{b_1,b_2,Y\circ X^{-1}(b_2)}(b_1) \\ &= b_2 \\ &= X\left(X^{-1}(b_2)\right). \end{aligned}$$

Hence, $Q \in A$. With $Q(a) = Q\left(Y^{-1}(b_1)\right) = \sigma_{b_1,b_2,Y\circ X^{-1}(b_2)}(b_1) = b_2$ we have that $Q \in B_{a,b_2}$. Altogether, $\varphi(A \cap B_{a,b_1}) \subseteq A \cap B_{a,b_2}$, so we proved (3.6).

Now let $b \in [n] \setminus \{X(a)\}$. Since the sets $B_{a,b'}$ for $b' \in [n]$ form a partition of S_n and $B_{a,X(a)} \cap A = \emptyset$, we can write A as disjoint union

$$A = \bigcup_{b' \in [n]} (A \cap B_{a,b'}) = \bigcup_{b' \in [n]\backslash\{X(a)\}} (A \cap B_{a,b'}),$$

implying that

$$|A| = \sum_{b' \in [n]\backslash\{X(a)\}} |A \cap B_{a,b'}| = (n-1) \cdot |A \cap B_{a,b}|$$

and we are done.

(ii): The proof is similar to the proof of (i). Note that the claim is true if $b = X(a)$ resp. $b^* = X(a^*)$, because then $|A \cap B_{a,b}| = 0$ resp. $|A \cap B_{a^*,b^*}| = 0$. So we may assume $b \neq X(a)$ and $b^* \neq X(a^*)$.

We first show that for all $a, a^* \in [n]$ with $a \neq a^*$ and $b^* \in [n], b_1 \in [n]\backslash\{b^*, X(a)\}, b_2 \in [n] \setminus \{b^*, X(a), X(a^*)\}$ we have

$$|A \cap B_{a,b_1} \cap B_{a^*,b^*}| \leq |A \cap B_{a,b_2} \cap B_{a^*,b^*}| \tag{3.7}$$

and if additionally $b_1 \neq X(a^*)$, we get

$$|A \cap B_{a,b_1} \cap B_{a^*,b^*}| = |A \cap B_{a,b_2} \cap B_{a^*,b^*}|. \tag{3.8}$$

Let $a, a^* \in [n]$ with $a \neq a^*$ and $b^* \in [n], b_1 \in [n] \setminus \{b^*, X(a)\}, b_2 \in [n] \setminus \{b^*, X(a), X(a^*)\}$. If $b_1 = b_2$, there is nothing to show, so we may assume $b_1 \neq b_2$. Define the sets D, E and the function φ as in the proof of (i) and consider the function $\psi := \varphi|_{A \cap B_{a,b_1} \cap B_{a^*,b^*}}$.

Due to (i), ψ is injective and we also have $\psi(A \cap B_{a,b_1} \cap B_{a^*,b^*}) \subseteq A \cap B_{a,b_2}$. We show that $\psi(A \cap B_{a,b_1} \cap B_{a^*,b^*}) \subseteq B_{a^*,b^*}$ to complete the proof of (3.7). Again, we split the proof into two parts.

For $Q \in \psi(D \cap B_{a^*,b^*})$ there exists some $Y \in D \cap B_{a^*,b^*}$ with $Q = \tau_{b_1,b_2} \circ Y$. Since $Y \in B_{a^*,b^*}$, we have $Y(a^*) = b^* \notin \{b_1, b_2\}$. This implies that $a^* \notin \{Y^{-1}(b_1), Y^{-1}(b_2)\}$, hence $Q(a^*) = Y(a^*) = b^*$ and therefore $Q \in B_{a^*,b^*}$.

For $Q \in \psi(E \cap B_{a^*,b^*})$ there exists some $Y \in E \cap B_{a^*,b^*}$ with $Q = \sigma_{b_1,b_2,Y\circ X^{-1}(b_2)} \circ Y$. Since $Y \in B_{a^*,b^*}$, we have $Y(a^*) = b^* \notin \{b_1, b_2\}$. Moreover, $Y(a^*) \neq Y \circ X^{-1}(b_2)$, because otherwise $a^* = X^{-1}(b_2)$ and therefore $X(a^*) = b_2$, in contradiction to the choice of b_2. Hence, $Q(a^*) = Y(a^*) = b^*$ and therefore $Q \in B_{a^*,b^*}$. Because $(D \cap B_{a^*,b^*}) \cup (E \cap B_{a^*,b^*}) = A \cap B_{a,b_1} \cap B_{a^*,b^*}$, the proof of (3.7) is complete.
If we additionally have $b_1 \neq X(a^*)$, we can apply (3.7) with swapped roles of b_1 and b_2 and additionally obtain that $|A \cap B_{a,b_1} \cap B_{a^*,b^*}| \geq |A \cap B_{a,b_2} \cap B_{a^*,b^*}|$, directly implying (3.8).

Now, let $b \in [n] \setminus \{b^*, X(a), X(a^*)\}$. Since the sets $B_{a,b'}$ with $b' \in [n]$ form a partition of S_n, we get

$$A \cap B_{a^*,b^*} = \bigcup_{b' \in [n]} (A \cap B_{a,b'} \cap B_{a^*,b^*}) \supseteq \bigcup_{b' \in [n] \setminus \{b^*, X(a), X(a^*)\}} (A \cap B_{a,b'} \cap B_{a^*,b^*}).$$

Because these unions are disjoint, we have

$$|A \cap B_{a^*,b^*}| \geq \sum_{b' \in [n] \setminus \{b^*, X(a), X(a^*)\}} |A \cap B_{a,b'} \cap B_{a^*,b^*}| \overset{(3.8)}{=} (n-3) \cdot |A \cap B_{a,b} \cap B_{a^*,b^*}|$$

and hence,

$$|A \cap B_{a,b} \cap B_{a^*,b^*}| \leq |A \cap B_{a^*,b^*}| \cdot \frac{1}{n-3} \overset{(i)}{=} |A| \cdot \frac{1}{(n-1)(n-3)}. \tag{3.9}$$

Since we assumed $b \neq X(a)$, the only remaining case is $b = X(a^*)$. Choose an arbitrary $b' \in [n] \setminus \{b^*, X(a), X(a^*)\}$. We have

$$|A \cap B_{a,b} \cap B_{a^*,b^*}| \overset{(3.7)}{\leq} |A \cap B_{a,b'} \cap B_{a^*,b^*}| \overset{(3.9)}{\leq} |A| \cdot \tfrac{1}{(n-1)(n-3)}.$$

□

Next, we want to lower bound the edge size for our hypergraph $\mathcal{H}$. For this we need the following proposition on the Rencontres number.

Proposition 3.21. *Let $n \in \mathbb{N}, k \in \{0, \ldots, n\}$ and let $X \in S_n$ be a permutation. Then, the number of all permutations Q with $\mathrm{B}(Q, X) = k$ is equal to $D_{n,k}$.*

Proof. Let $M_{X,k}$ denote the set of all permutations Q with $\mathrm{B}(Q, X) = k$. Let F_k denote the set of permutations with k fixpoints. By definition, $D_{n,k} = |F_k|$, so it suffices to show that $|F_k| = |M_{X,k}|$. To see this, we show that $X(F_k) = M_{X,k}$: Let $Q \in X(F_k)$, so $Q = X \circ Y$ for some $Y \in F_k$. But then for every $a \in [n]$ we have $Q(a) = X(a) \Leftrightarrow Y(a) = a$, hence $\mathrm{B}(Q, X)$ is exactly the number of fixpoints of Y and we are done. □

Lemma 3.22. *Let $n \geq 6$. Let $X_1, X_2 \in S_n$ with $\Delta(X_1, X_2) \geq \sqrt{n}$. Then, for the edge H_{X_1,X_2} of the hypergraph $\mathcal{H}$, it holds $|H_{X_1,X_2}| \geq n! \cdot \frac{1}{18\sqrt{n}}$.*

Proof. Let $h := \Delta(X_1, X_2)$ and $a_1, \ldots, a_h$ be the colors with $X_1(a_i) \neq X_2(a_i)$ for $1 \leq i \leq h$. Let $A := \{Q \in S_n | \Delta(Q, X_1) = n\}$. For $i \in [h]$ let $B_i := \{Q \in S_n | Q(a_i) = X_2(a_i)\}$ and let $B := \bigcup_{i=1}^{h} B_i$. Note that for $Q \in A \cap B$ we have $Q(a_i) = X_2(a_i)$ for some $i \in [h]$, thus $\Delta(Q, X_2) < n = \Delta(Q, X_1)$. Hence, Q separates X_1 and X_2 and therefore $(A \cap B) \subseteq H_{X_1,X_2}$. Moreover, with Proposition 3.21 we get $|A| = D_{n,0}$ and by Corollary 3.3 we get $D_{n,0} \geq \frac{n!}{3}$ for $n \geq 2$. Finally, for $n \geq 6$ we get

$$
\begin{aligned}
|H_{X_1,X_2}| \geq |A \cap B| &= \left| A \cap \bigcup_{i=1}^{h} B_i \right| = \left| \bigcup_{i=1}^{h} (A \cap B_i) \right| \\
&\geq \sum_{i=1}^{h} |A \cap B_i| - \sum_{i<j\in[h]} |A \cap B_i \cap B_j| && \text{(Bonferroni ineq. [10])} \\
&\geq \sum_{i=1}^{h} \frac{1}{n-1}|A| - \sum_{i<j\in[h]} \frac{1}{(n-1)(n-3)}|A| && \text{(Lemma 3.20 (i),(ii))} \\
&= |A| \left(\frac{h}{n-1} - \binom{h}{2} \frac{1}{(n-1)(n-3)} \right) \\
&\geq \frac{n!}{3} \cdot \frac{h}{n-1} \cdot \left(1 - \frac{h-1}{2(n-3)} \right) \\
&\geq \frac{n!}{3} \cdot \frac{h}{n-1} \cdot \left(1 - \frac{(n-3)+2}{2(n-3)} \right) && (h \leq n) \\
&= \frac{n!}{3} \cdot \frac{h}{n-1} \cdot \left(\frac{1}{2} - \frac{1}{n-3} \right) \\
&\geq n! \cdot \frac{h}{18n} && (n \geq 6) \\
&\geq n! \cdot \frac{1}{18\sqrt{n}}. && (h \geq \sqrt{n})
\end{aligned}
$$

□

This lower bound for the edge size of the hypergraph $\mathcal{H}$ can be used to obtain a lower bound for the maximum vertex degree.

Lemma 3.23. *Let $n \geq 6$. For every subset $\emptyset \neq \mathcal{F} \subseteq \mathcal{E}$, there is a vertex $Q \in V$ with $|\{H \in \mathcal{F} : Q \in H\}| \geq \frac{1}{18\sqrt{n}} \cdot |\mathcal{F}|$.*

Proof. Let $\emptyset \neq \mathcal{F} \subseteq \mathcal{E}$. Assume that such a vertex Q doesn't exist. Then for all $Q \in V$ it holds $|\{H \in \mathcal{F} : Q \in H\}| < |\mathcal{F}| \cdot \frac{1}{18\sqrt{n}}$ and with Lemma 3.22 we get

$$
|\mathcal{F}| \cdot n! \cdot \frac{1}{18\sqrt{n}} \leq \sum_{H \in \mathcal{F}} |H| = \sum_{Q \in V} |\{H \in \mathcal{F} : Q \in H\}| < n! \cdot |\mathcal{F}| \cdot \frac{1}{18\sqrt{n}},
$$

a contradiction. □

We now construct a vertex cover of $\mathcal{H}$ by iteratively picking vertices with maximum degree and then deleting all covered edges. In the following theorem we prove that such a vertex cover is of size $\mathcal{O}(n^{1.5} \cdot \ln(n))$.

Theorem 3.24. *There exists a set of $\mathcal{O}(n^{1.5} \cdot \ln(n))$ questions such that every pair $X_1, X_2 \in S_n$ with $\Delta(X_1, X_2) \geq \sqrt{n}$ is separated by at least one question.*

Proof. W.l.o.g. let $n \geq 6$. By construction of $\mathcal{H}$ it suffices to prove that there exists a vertex cover of $\mathcal{H}$ with $\mathcal{O}(n^{1.5} \cdot \ln(n))$ vertices. With Lemma 3.23, for every subset $\emptyset \neq \mathcal{F} \subseteq \mathcal{E}$ there is a vertex $Q \in V$ with $|\{H \in \mathcal{F} : Q \in H\}| \geq \frac{1}{18\sqrt{n}} \cdot |\mathcal{F}|$. Hence, for every subset $\emptyset \neq \mathcal{F} \subseteq \mathcal{E}$ we can pick a vertex $Q \in V$ that leaves at most $\left(1 - \frac{1}{18\sqrt{n}}\right) \cdot |\mathcal{F}|$ edges uncovered. Now we can start with the empty set $T = \emptyset$, and iteratively add a vertex to T that covers at least a fraction of $\frac{1}{18\sqrt{n}}$ of all former uncovered edges. After t steps the fraction of uncovered edges is at most $\left(1 - \frac{1}{18\sqrt{n}}\right)^t$. With $t := 36 \ln(n) \cdot n^{1.5}$, the fraction of uncovered edges after t steps is at most

$$\begin{aligned}\left(1 - \frac{1}{18\sqrt{n}}\right)^{36 \ln(n) \cdot n^{1.5}} &= \left(1 - \frac{1}{18\sqrt{n}}\right)^{18\sqrt{n} \cdot (2 \ln(n) \cdot n)} \\ &\leq e^{-2 \ln(n) \cdot n} \\ &= n^{-2n} \leq (n!)^{-2}.\end{aligned}$$

Since $|\mathcal{E}| < (n!)^2$, after t iteration steps the total number of uncovered edges is at most $|\mathcal{E}|(n!)^{-2} < 1$, so T is a vertex cover of $\mathcal{H}$. Hence, $\mathcal{O}(n^{1.5} \cdot \ln(n))$ questions suffice to separate every pair $X_1, X_2 \in S_n$ with $\Delta(X_1, X_2) \geq \sqrt{n}$. □

Finally, we can prove our main result.

Theorem 3.25. *For every $n \in \mathbb{N}$ there exists a feasible $\mathcal{O}(n^{1.525})$-strategy for static permutation Mastermind with n colors and pegs.*

Proof. According to Theorem 3.19 there is a strategy T_{low} with $|T_{\text{low}}| = \mathcal{O}(n^{1.525})$ that separates every pair of possible secrets with Hamming distance at most $\sqrt{n}$. By Theorem 3.24, there exists a strategy T_{high} with $|T_{\text{high}}| = \mathcal{O}(n^{1.5}\ log(n))$ that separates all pairs of possible secrets with Hamming distance at least $\sqrt{n}$. So the strategy $T := T_{\text{low}} \cup T_{\text{high}}$ is a feasible strategy with $\mathcal{O}(n^{1.525})$ questions. □

3.5 A lower bound

In this section we present a lower bound of $\Omega(n \cdot \log n)$ questions for static permutation Mastermind. The technique is based on information theory and adopted from [13].

Theorem 3.26. *Every feasible strategy for static permutation Mastermind with n colors and pegs has $\Omega(n \log n)$ questions.*

We only consider deterministic Codemaker strategies. Nevertheless, the proof can be expanded to randomized strategies as done in [13]. Note that in the following we use the logarithm to the base 2 and denote it by "log".

3.5.1 Proof of the lower bound

For proving the lower bound, we introduce a few notions and results from information theory.

Definition 3.27. *Let D be a finite set and let $\mathbb{P}$ a probability measure on D. Let $X : D \to \mathbb{R}$ be a random variable. The* entropy *of X is defined as*

$$H(X) := \sum_{\substack{x \in D \\ \mathbb{P}[X=x]>0}} \mathbb{P}[X = x] \log\left(\frac{1}{\mathbb{P}[X = x]}\right).$$

Intuitively speaking, the entropy is a measure on how much information X will reveal in expectation.

We need the following well-known properties of entropy:

Lemma 3.28. *Let D be a finite set and $\mathbb{P}$ a probability measure on D. Let $X, Y : D \to \mathbb{R}$ be random variables.*

(i) $H((X, Y)) \leq H(X) + H(Y)$.

(ii) If $X = f(Y)$ for some function $f : \mathbb{R} \to \mathbb{R}$, then $H(X) \leq H(Y)$.

Proof of Theorem 3.26. Consider a possible secret $X \in S_n$ chosen uniformly at random So $D = S_n$ and $\mathbb{P}$ is the uniform distribution on D. Hence, $H(X) = \log(|D|) = \log(n!)$. Let $T := \{Q_1, \ldots, Q_s\}$ be a feasible s-strategy. For $i \in [s]$ let $Y_i := \mathrm{B}(Q_i, X)$ be the answer to the i-th question. Because our strategy is feasible, the sequence $Y = (Y_1, \ldots, Y_s)$ determines X and hence we have $H(Y) \geq H(X)$ by Lemma 3.28 (ii). On the other hand, $H(Y) = H(Y_1, \ldots, Y_s) \leq \sum_{i=1}^{s} H(Y_i)$ by Lemma 3.28 (i). We recall the definition of the Rencontres number $D_{n,k}$ in Definition 3.1. For every $i \in [s]$ and every $k \in \{0, \ldots, n\}$ we have $\mathbb{P}(Y_i = k) = \frac{D_{n,k}}{n!}$, because due to Proposition 3.21 there are $D_{n,k}$ permutations $\tilde{X}$ with $\mathrm{B}(Y_i, \tilde{X}) = k$. Hence, $H(Y_i) = \sum_{k=0}^{n} \frac{D_{n,k}}{n!} \log\left(\frac{n!}{D_{n,k}}\right)$. Because

$D_{n,n} = 1$ and $D_{n,n-1} = 0$, for any $i \in [s]$ and $n \geq 4$ we get

$$\begin{aligned}
H(Y_i) &= \sum_{k=0}^{n} \frac{D_{n,k}}{n!} \log\left(\frac{n!}{D_{n,k}}\right) \\
&= \frac{\log(n!)}{n!} + \sum_{k=0}^{n-2} \frac{D_{n,k}}{n!} \log\left(\frac{n!}{D_{n,k}}\right) \\
&\leq \frac{\log(n!)}{n!} + \frac{1}{2}\sum_{k=0}^{n-2} \frac{\log(3k!)}{k!} && \text{(Corollary 3.3)} \\
&= \frac{\log(n!)}{n!} + \frac{1}{2}\sum_{k=0}^{n-2} \frac{\log(3)}{k!} + \frac{1}{2}\sum_{k=2}^{n-2} \frac{\log(k!)}{k!} \\
&\leq \frac{n\log(n)}{n!} + \frac{\log(3)}{2}e + \frac{1}{2}\sum_{k=2}^{n-2} \frac{\log(k!)}{k!} \\
&\leq \frac{e}{5} + \frac{4e}{5} + \frac{1}{2}\sum_{k=2}^{n-2} \frac{\log(k!)}{k!} && (n \geq 4) \\
&\leq e + \frac{1}{2}\sum_{k=2}^{n-2} \frac{k\log(k)}{k(k-1)(k-2)!} \\
&\leq e + \frac{1}{2}\sum_{k=2}^{n-2} \frac{1}{(k-2)!} \\
&\leq \frac{3}{2}e.
\end{aligned}$$

Altogether we have $\log(n!) = H(X) \leq H(Y) \leq \frac{3se}{2}$, hence $s \geq 2\log(n!)/3e = \Omega(n \cdot \log n)$. □

3.6 A lower bound for the adaptive semi AB-Game

In this section we leave the field of static Mastermind and present a lower bound for the number of questions in the adaptive semi AB-Game. Recall that in the semi AB-Game the secret code has no repetition, but arbitrary questions are allowed. When talking about lower bounds in adaptive games, we mean the number of questions that Codebreaker has to ask in the worst case, before he receives p black pegs.

Information theoretical lower bounds as presented in Section 3.6 do not apply for adaptive games, since the entropy of a single answer can't be estimated that easily. In the static game the given answer Y_j to a question Q_j can be considered independent of the question, whereas in the adaptive version for all $j > 1$ Codebreaker can adapt all earlier answers when formulating question Q_j, thus the question Q_j may not be independent of Y_j. Nevertheless, one can still use the trivial upper bound $H(Y_j) \leq \log(p)$ to obtain a lower bound of $\Omega(n)$ questions. In this section we will use a combinatorial approach to

obtain a lower bound. In each iteration, the worst case for the Codebreaker is simulated by allowing the Codemaker to replace his secret code with a different permutation from the remaining feasible search space. We consider the adaptive black-peg semi AB-Game with p pegs and $c \geq p$ colors and present a rather simple strategy for Codemaker, assuring that Codebreaker has to ask a minimum of c questions before he can end the game.

Note that the lower bounds established in this section especially hold true for the black-peg AB-Game, since the Codebreaker will not be able to detect a secret code with less attempts, if the set of allowed queries is restricted to the corresponding subset.

3.6.1 The case $p = c$

For $k \in \mathbb{N}$ we denote the k-th query of the Codebreaker with Q_k, the corresponding answer with Y_k and the k-th secret code adaption of the Codemaker with X_k. The remaining feasible search space R_k consists of all permutations that agree with the first k pairs of queries and answers:

$$\begin{aligned} &R_0 := S_n, \\ &R_k := \{X \in S_n \mid \mathrm{B}(X, Q_j) = Y_j \text{ for all } j \in [k]\}, \text{ for } k > 0. \end{aligned}$$

The strategy of the Codemaker is to reply every query Q_k, $k \in \mathbb{N}$, with the smallest possible number

$$Y_k := \min_{X \in R_{k-1}} \mathrm{B}(X, Q_k),$$

choosing his new secret code $X_k \in R_{k-1}$ such that $\mathrm{B}(X_k, Q_k) = Y_k$. We obtain our lower bound on the necessary number of queries by proving the following Lemma.

Lemma 3.29. *If Codemaker plays according to the above strategy, for all $k < p$ it holds $Y_k \leq k$.*

In particular, none of the first $p-1$ queries will be answered with p. Thus, the secret code cannot be identified with less than p queries.

Proof. Assuming that our claim is wrong, we fix the smallest number $k \in [p-1]$ with $Y_k > k$. Let

$$D := \{b \in [c] \mid {Q_k}^{-1}(b) = {X_k}^{-1}(b)\}$$

be the set of colors that are correctly placed in the current query with respect to the current secret code. For every $a \in [p]$, let $C_a \subseteq [p]$ be the set of all colors that do not occur at position a in any of the first k queries, i.e.,

$$C_a := \{b \in [c] \mid b \neq Q_\ell(a) \text{ for all } \ell \in [k]\}.$$

The intersections $C_a \cap D$, $a \in [p]$ are not empty since $|D| = Y_k \geq k+1$, but at most k of all $c = p$ colors are missing in C_a. This fact will enable us to determine a new feasible secret code $X \in R_{k-1}$ such that $\mathrm{B}(X, Q_j) = Y_j$ for all $j \in [k-1]$

but $\mathrm{B}(X, Q_k) < Y_k$, a contradiction to the minimality of Y_k. The new secret code X is constructed from X_k by changing the colors of certain pegs that coincide with Q_k, choosing the new color at a given position a from $C_a \cap D$. The precise procedure is outlined as Algorithm 1. Starting with any position a_1 where X_k and Q_k have the same color, we choose a color $b_1 \in C_{a_1} \cap D$. Since $b_1 \in D$, there must be another position a_2 such that $X_k(a_2) = b_1 = Q_k(a_2)$. Thus, for $s > 1$, we can iteratively determine positions a_s where X_k and Q_k have the same color, b_{s-1}, and choose a new color $b_s \in C_{a_s} \cap D$ (while loop, lines 5–9). The iteration stops if the chosen color b_s corresponds with a color that appears in X_k at some position a_t, $t < s$, that has been considered before. Let $B := \{b_1, \ldots, b_s\}$ denote the set of all colors chosen this way and let $B^* := \{b_t, b_{t+1}, \ldots, b_s\}$. Note that $2 \leq |B^*| \leq |B| \leq |D| \leq n$, since the iteration has at least two steps and by construction $B^* \subseteq B \subseteq D$.

Let $A^* := \{a_t, a_{t+1}, \ldots, a_s\} = \{a \in [n] \mid Q_k(a) \in B^*\}$. We now construct the new secret X from X_k by recoloring position a_j with color b_j for all $t \leq j \leq s$ (lines 11–12). Because the set of old colors $\{X_k(a) \mid a \in A^*\}$ is equal to the set of new colors B^*, the

Algorithm 1: Secret code adaption, $p = c$

```
1  s := 1;
2  B := ∅;
3  Choose position a_1 ∈ [n] with X_k(a_1) = Q_k(a_1);
4  Choose color b_1 ∈ C_{i_1} ∩ D;
5  while b_s ∉ B do
6  |  B := B ∪ {X_k(a_s)};
7  |  s := s + 1;
8  |  a_s := (X_k)^{-1}(b_{s-1});
9  |  Choose color b_s ∈ C_{a_s} ∩ D;
10 Find the unique t < s with X_k(a_t) = b_s;
11 X := X_k;
12 for ℓ := t to s do X(a_ℓ) := b_ℓ;
```

new secret code X is still a permutation. First note that for all $a \in A^*$ and all $\ell \in [k]$,

$$X(a) \neq Q_\ell \quad \text{and} \quad X_k(a) = Q_k(a). \tag{3.10}$$

Let $a \in A^*$ and $\ell \in [k]$. Then, $a = a_i$ for some $t \leq i \leq s$ and by construction of X we have $X(a) = X(a_i) = b_i$, where $b_i \in C_{a_i} \cap D$. Because $b_i \in C_{a_i}$, we have $b_i \neq Q_\ell(a_i)$ and because $b_i \in D$, we have $X_k(a) = b_i = Q_k(a)$.

We show that

(i) $X \in R_k$

(ii) $\mathrm{B}(X, Q_k) < Y_k$

This completes the proof, because (i) combined with (ii) contradicts the fact that by choice of Y_k we have $\mathrm{B}(X, Q_k) \geq Y_k$ for all $X \in R_k$.

For the proof of (i) we use induction over i to show that for all $i \in \{0, \dots k-1\}$ we have. For $i = 0$ we have $R_0 = S_n$ and because X is a permutation, we are done.

Now let $X \in R_i$ for some $i < k-1$. To show that $X \in R_i + 1$, it suffices to prove $\mathrm{B}(X, Q_{i+1}) = Y_{i+1}$. Note that $\mathrm{B}(X, Q_j) \geq Y_{i+1}$ because of the choice of Y_{i+1}. On the other hand,

$$\begin{aligned}
\mathrm{B}(X, Q_{i+1}) &= |\{a \in [p] \mid X(a) = Q_{i+1}(a)\}| \\
&= |\{a \in A^* \mid X(a) = Q_{i+1}(a)\}| + |\{a \in [p] \setminus A^* \mid X(a) = Q_{i+1}(a)\}| \\
&\overset{(3.10)}{=} |\{a \in [p] \setminus A^* \mid X(a) = Q_{i+1}(a)\}| \\
&= |\{a \in [p] \setminus A^* \mid X_k(a) = Q_{i+1}(a)\}| \\
&\leq |\{a \in [p] \mid X_k(a) = Q_{i+1}(a)\}| \\
&= \mathrm{B}(X_k, Q_{i+1}) = Y_{i+1}
\end{aligned}$$

and the proof of (i) is complete.

(ii). We have

$$\begin{aligned}
\mathrm{B}(X, Q_k) &= |\{a \in [p] \mid X(a) = Q_k(a)\}| \\
&\overset{(3.10)}{=} |\{a \in [p] \setminus A^* \mid X(a) = Q_k(a)\}| \\
&= |\{a \in [p] \setminus A^* \mid X_k(a) = Q_k(a)\}| \\
&= \mathrm{B}(X_k, Q_k) - |\{a \in A^* \mid X_k(a) = Q_k(a)\}| \\
&\overset{(3.10)}{=} \mathrm{B}(X_k, Q_k) - |A^*| \\
&= \mathrm{B}(X_k, Q_k) - |B^*| < \mathrm{B}(X_k, Q_k).
\end{aligned}$$

□

3.6.2 More colors than positions

Considering the case $c \geq p$, we adapt the Codemaker strategy from the former subsection, i.e., in each turn k, the Codemaker chooses the new secret code X_k such that the answer is the smallest possible answer Y_k. We easily obtain a lower bound of c queries by the following:

Lemma 3.30. *If Codemaker plays according to the above strategy, for all $k < c$ it holds $Y_k < p$.*

Note that this lemma especially works for the case $p = c$ and although in this case it is weaker than Lemma 3.29, it leads to the same lower bound.

Proof. Assume for a moment that there exists an $k < c$ with $Y_k = p$. Like before, let

$$C_a := \{b \in [c] \mid b \neq Q_\ell(a) \text{ for all } \ell \in [k]\}.$$

Note that we don't need a set D as defined in the proof of Lemma 3.29 since we assumed $Y_k = p$, hence $Q_k = X_k$. Instead, we define the set

$$B_0 := \{b \in [c] \mid X_k(a) \neq b \text{ for all } a \in [p]\}$$

of all colors that don't occur in the secret code X_k As Algorithm 1, we will replace certain peg colors of X_k by elements of the corresponding C_i. The detailed procedure is described in Algorithm 2.

Algorithm 2: Secret code adaption, $k > n$

```
s := 1;
a_1 := 1;
B := B_0;
Choose color b_1 ∈ C_1;
while b_s ∉ B do
    B := B ∪ {X_k(a_s)};
    s := s + 1;
    a_s := (X_k)^{-1}(b_{s-1});
    Choose color b_s ∈ C_{a_s};
if b_s ∉ A_0 then
    Find the unique t < s with X_k(a_t) = b_s;
else t := 1;
X := X_k;
for ℓ := t to s do X(a_ℓ) := b_ℓ;
```

We start with peg $a_1 = 1$ and choose a color $b_1 \in C_{a_1} = C_1$. If $b_1 \notin B_0$, there is a unique peg a_2 with $X_k(a_2) = b_1$. Just as in Algorithm 1, we iteratively choose pairs (a_i, b_i) until a pair occurs for the second time or we have $b_i \in B_0$ for some i. In the first case, the algorithm works identically to Algorithm 1 and we are done. So assume that the iteration stops because $b_i \in B_0$ for some i. Again, we construct X by starting with X_k and then replacing the color $X_k(a_\ell)$ by the color b_ℓ for any $\ell \leq s$. The set of chosen colors $\{b_\ell \mid \ell \leq s\}$ is equal to the set of colors $\{X_k(a_\ell) \mid \ell \leq s\}$ except for b_s, which only appears in the first set and $X_k(a_\ell)$, which only appears in the second. Since $b_s \in B_0$, we know that X has no color occurring twice.

Analogously to the analysis of Algorithm 1 one can use the fact that all colors b_i are chosen from C_{a_i} to show that $X \in R_k$ with $\mathrm{B}(X, Q_k) < Y_k$, in contradiction to the minimality of Y_k. □

3.7 Open questions

For the static permutation Mastermind on n colors and pegs, we present a strategy using $\mathcal{O}(n^{1.525})$ questions and a lower bound of $\Omega(n \log(n))$ questions, leaving quite a big gap.

Besides the challenge of reducing this gap, it would be interesting to know, whether our techniques and results from Sections 3.4 and 3.5 can be transferred to the AB-Game with $c > p$. Open gaps also exist on the adaptive side, being of size $\Theta(\log(n))$ for the AB-Game and $\Theta(\log\log(n))$ for the classic variant.

Chapter 4

The Vertex Destruction Game

4.1 Introduction

This chapter is based on a previously unpublished paper [17]. In the previous chapters we considered different games played by two opponents. In real-world situations there are often far more players involved in a problem and each of them wants to maximize his individual profit.

4.1.1 The network model

The well-known graph network model introduced by Jackson and Wolinsky [20] in 1996 is often used to represent such a multi player problem in a combinatorial way. The players are represented by the vertices of a graph and their relationships are represented by its edges. In this chapter we investigate on the problem of network formation, i.e. the development of such a network over time. This kind of model was introduced to computer science by Fabrikant et al. [15] in 2003. Consider n players in a given network graph. Every player obtains a certain profit (or cost) depending on his position in the network and he has some possibilities to change his position. Now suppose that all players are egoistic in the sense that they always will change their position in the graph if this leads to an increase of their personal profit. In this work we consider Nash equilibria, i.e., networks in which none of the players can increase his profit by changing his position. These kind of stable networks are also called *swap equilibria*.

The choice of the cost function substantially affects the interpretation and behavior of the network model. A common choice are centrality criteria, for example if the cost function is defined as the sum of the distances to all other players or similar [1, 3, 11, 20, 22]. On the other hand, robustness aspects of the network have been addressed: In 2010, Kliemann [24] introduced the so-called *destruction model*, where certain edges are deleted from the network and the players try to stay connected to as many other players as possible. Since then, several aspects of this model were studied, like the price of anarchy in Nash equilibria [25, 26, 27]. The concept of *swap equilibria* (SE) was introduced by Alon et al. [2] in 2010. They restricted the possibilities of the players to

simple edge swaps, i.e., the removal of an incident edge combined with the creation of a new incident edge. In 2017, Kliemann et al. [23] first considered the destruction of vertices: In the *vertex destruction model*, a so-called vertex destroyer picks one vertex according to some probability distribution which then is destroyed, i.e., all of its incident edges are deleted. The cost of a single vertex is the expected number of other vertices it loses connection to after this deletion. They considered a *uniform destroyer*, who always destroys one vertex chosen uniformly at random and an *extreme destroyer*, who tries to cause maximal damage to the network by destroying a vertex of maximal separation, a so-called *max-sep vertex*. For the latter, Kliemann et al. proved a lower bound of $\Omega(n^{3/2})$ for the social cost of SE by presenting a corresponding star-like graph. Moreover they showed that for $n \geq 8$, every tree that is a SE has at least two max-sep vertices.

4.1.2 Our contribution

All results in this chapter are for the extreme vertex destroyer. We prove two open conjectures of Kliemann et al. [23] and thereby generalize their result: On one hand we show (Theorem 4.9) that a tree on more than 5 vertices that is a SE, has *exactly* one max-sep vertex. On the other hand, we prove (Theorem 4.21) that the only SE graphs with exactly one max-sep vertex are short paths. Combining these two results, every SE graph that is a tree *or* has only one max-sep vertex is a path of length at most 4.

From the network formation point of view this means that for all networks with more than 5 players, a network without a cycle will never come to a stable state: At any time there is at least one player who can improve his position by a swap. On the other hand, networks in which the vertex that will be destroyed is already determined are never stable, because either the player who will be isolated can prevent this or there is some other player that can improve his own situation by 'helping' the max-sep player.

4.2 Preliminaries

We introduce the model of extreme vertex destruction and some important terminology. We start with some notation. For a graph $G = (V, E)$ and a set of vertices $H \subseteq V$ we frequently identify H with the subgraph G/H of G induces on H, i.e., $G/H = \left(H, E \cap \binom{H}{2}\right)$. We simply write H instead of G/H if the context is clear. For $v \in V$, with $H + v$ we denote the subgraph of G induced on the vertex set $H \cup \{v\}$. For two paths P, Q in G we denote their concatenation by (P, Q) and analogously, (P, v) denotes the concatenation of the vertex v to the path P.

4.3 Extreme Vertex Destroyer and Preliminaries

We start with some notation. For a graph $G = (V, E)$ and a set of vertices $H \subseteq V$ we frequently identify H with the subgraph G/H of G induces on H, i.e., $G/H = \left(H, E \cap \binom{H}{2}\right)$. We simply write H instead of G/H if the context is clear. For $v \in V$,

with $H + v$ we denote the subgraph of G induced on the vertex set $H \cup \{v\}$. For two paths P, Q in G we denote their concatenation by (P, Q) and analogously, (P, v) denotes the concatenation of the vertex v to the path P.

Next, We introduce the model of extreme vertex destruction and some important terminology. Let $n \in \mathbb{N}_{\geq 3}$ and denote by $\mathcal{G}_n$ the set of all *connected* graphs on n vertices. For $G \in \mathcal{G}_n$, let $G - \{a, b\}$ denote the graph that is obtained from G by removing the edge $\{a, b\}$.

Definition 4.1 (Swap)**.** *Let $G = (V, E) \in \mathcal{G}_n$ be a connected graph and $s = (a, b, c)$ a triple of vertices of G such that $\{a, b\} \in E$ and $\{a, c\} \notin E$. Denote by G^s the graph that is obtained from G by removing $\{a, b\}$ and inserting $\{a, c\}$. If G^s is still connected, we call s a* swap.

Definition 4.2 (Cost function and swap equilibria)**.** *A* cost function $\mathcal{C}$ *assigns to each pair of a graph $G \in \mathcal{G}_n$ and vertex $v \in V$ a cost $\mathcal{C}(G, v) \in \mathbb{R}$. (The cost function considered in this paper is introduced in Definition 4.4)*

The social cost *of G is defined as*

$$\mathrm{SC}(G) = \sum_{v \in V} \mathcal{C}(G, v).$$

We call G a swap equilibrium *(SE) if $\mathcal{C}(G, a) \leq \mathcal{C}(G^s, a)$ for all swaps $s = (a, b, c)$ and $\mathcal{C}(G, a) \leq \mathcal{C}(G - \{a, b\}, a)$ for all $\{a, b\} \in E$ such that $G - \{a, b\}$ is still connected.*

Thus, in a SE a vertex cannot improve its cost by swapping one of its incident edges or by simply removing one of its incident edges. As mentioned above, we will study a cost function that expresses robustness aspects of the graph against a probabilistic adversary (*vertex destroyer*).

Definition 4.3 (vertex destroyer)**.** *A* vertex destroyer $\mathcal{D}$ *is a map that associates with each $G \in \mathcal{G}_n$ a probability measure $\mathcal{D}(G, \cdot)$ on the vertices of G, that is $\mathcal{D}(G, v) \in [0, 1]$ for each $v \in V$, and $\sum_{v \in V} \mathcal{D}(G, v) = 1$.*

The vertex destroyer is used to randomly choose a certain vertex which then will be destroyed, i.e., all of its incident edges will be deleted. We use the vertex destroyer to define a robustness-related cost function.

Definition 4.4 (Relevance and separation)**.** *For $u, v \in V$, define*

$$\mathcal{R}_u(v) := \{w \in V | u \text{ lies on every } v\text{-}w\text{-path in G}\}.$$

The relevance *of $u \in V$ for $v \in V$ is defined as*

$$\mathrm{rel}_{G,u}(v) := \mathrm{rel}_u(v) := |\mathcal{R}_u(v)|.$$

Given a vertex destroyer $\mathcal{D}$, we define the cost *for player v in G as*

$$\mathcal{C}(G, v) := \sum_{u \in V} \mathrm{rel}_u(v) \mathcal{D}(G, u).$$

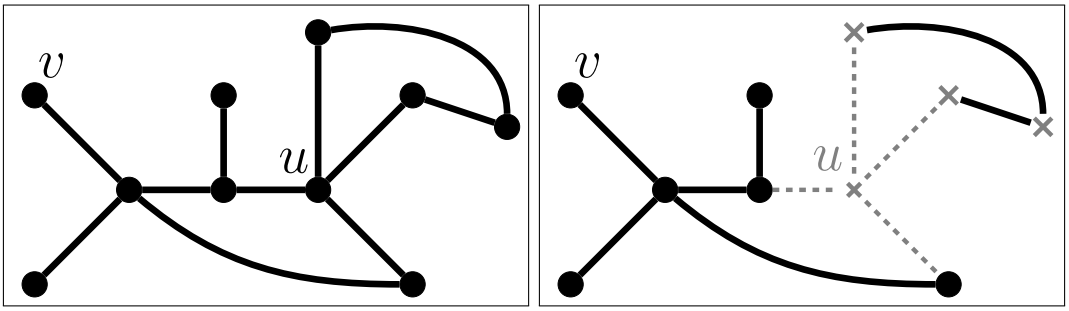

Figure 4.1: The relevance $\mathrm{rel}_u(v)$ of u for v is the number of vertices that v loses connection to if u is destroyed. In this example, $\mathrm{rel}_u(v) = 4$.

The separation *of $v \in V$ is defined as*

$$\mathrm{sep}_G(v) := \left| \bigcup_{u \in V} \{(u, w) | w \in \mathcal{R}_v(u)\} \right| = \sum_{u \in V} \mathrm{rel}_v(u).$$

Let us explain this terminology. The relevance $\mathrm{rel}_u(v)$ of u for v is the number of players that v will no longer be able to reach after all of u's incident edges have been removed (see Figure 4.1). Note that since v is in every v-w-path, we have $\mathrm{rel}_v(v) = n-1$. Hence, the defined cost function $\mathcal{C}$ is the expected number of vertices that v will no longer be able to reach after one vertex u has been picked randomly according to the probability distribution $\mathcal{D}(G, \cdot)$ and then all of u's incident edges have been removed. The *separation* $\mathrm{sep}_G(v)$ of a vertex $v \in V$ is the number of ordered player pairs (u, w) such that the removal of v will destroy all u-w-paths in G.

When the graph G is clear from context, we omit the G subscripts from the sep notation. For a swap s and vertices u, v we also write $\mathrm{sep}^s(u)$ instead of $\mathrm{sep}_{G^s}(u)$ and $\mathrm{rel}^s_u(v)$ instead of $\mathrm{rel}_{G^s,u}(v)$. Note that

$$\mathrm{SC}(G) = \sum_{v \in V} \mathcal{C}(G, v) = \sum_{v \in V} \sum_{u \in V} \mathrm{rel}_v(u) \mathcal{D}(G, u) = \sum_{v \in V} \mathrm{sep}_G(v)\, \mathcal{D}(G, v). \tag{4.1}$$

Many different destroyers are conceivable. We study a particular destroyer that maximizes the social cost of the network.

Definition 4.5. *A vertex v is called a* max-sep vertex *if $\mathrm{sep}(v) \geq \mathrm{sep}(u)$ for all $u \in V$. Let $\mathrm{MS}(G)$ be the set of all max-sep vertices in G. The* extreme vertex destroyer $\mathcal{D}_{\mathrm{ev}}$ *is defined by*

$$\mathcal{D}_{\mathrm{ev}}(G, v) = \begin{cases} 1/|\mathrm{MS}(G)| & \text{if } v \in \mathrm{MS}(G) \\ 0 & \text{else.} \end{cases}$$

Hence, the extreme vertex destroyer picks the vertex to destroy uniformly at random from the set of all max-sep vertices and thereby maximizes the social cost of the graph (see (4.1)). An example for the setting under an extreme vertex destroyer is given in Figure 4.2.

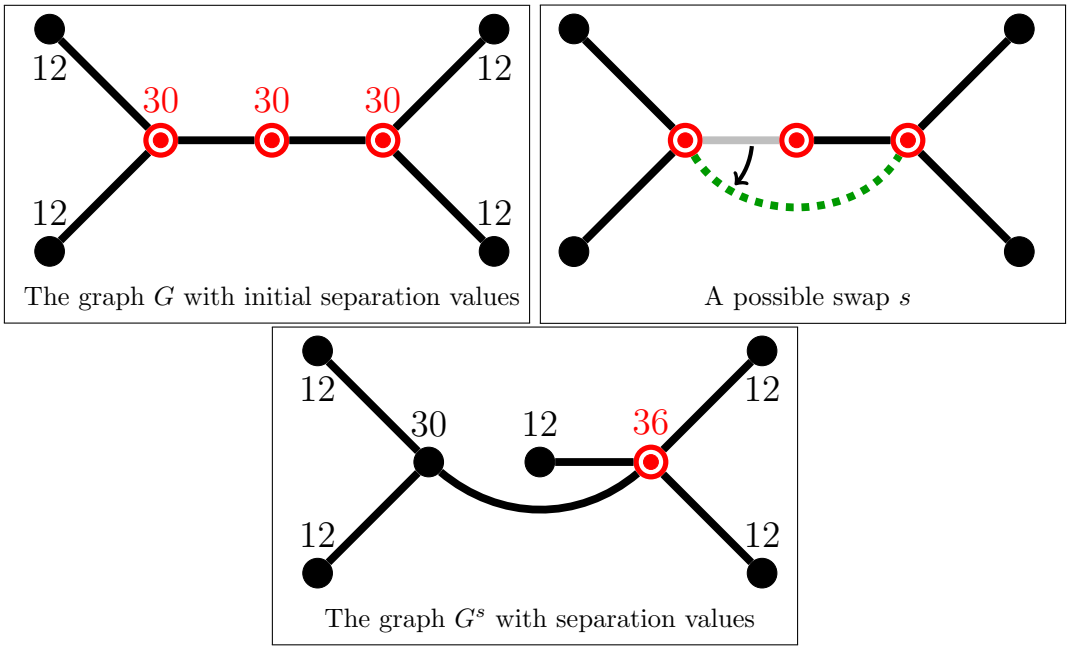

Figure 4.2: The graph G has three max-sep vertices (colored red). It is no SE, because the left max-sep vertex can perform swap s and decrease its cost from $\frac{13}{3}$ to 4.

Removing a vertex v from a connected graph G in the usual sense (that is, v and its incident edges are removed) splits the graph into $k \geq 1$ components, which we call $v\bar{}$flaps, and the set of which we denote by $\mathcal{F}(v)$.

Proposition 4.6. *Let $G = (V, E)$, $v \in V$ and $\mathcal{F}(v) = \{A_1, \ldots, A_k\}$ for some $k \in \mathbb{N}$. Then,*

(i) For every $A \in \mathcal{F}(v)$ and every $u \in A$ it holds $\mathrm{rel}_v(u) = n - |A|$.

(ii) $\mathrm{sep}_G(v) = n^2 - 1 - \sum_{i=1}^{k} |A_i|^2$.

Proof. By definition of the flaps, for every $A \in \mathcal{F}(v)$ and $u \in A$ we have $\mathcal{R}_v(u) = V \setminus A$,

so we get $\mathrm{rel}_v(u) = n - |A|$ and (i) is proved. Further, with $\mathrm{rel}_v(v) = n - 1$,

$$\begin{aligned}
\mathrm{sep}_G(v) &= \sum_{u \in V} \mathrm{rel}_v(u) \\
&= \mathrm{rel}_v(v) + \sum_{i=1}^{k} \sum_{u \in A_i} \mathrm{rel}_v(u) \\
&= n - 1 + \sum_{i=1}^{k} \sum_{u \in A_i} (n - |A_i|) \\
&= n - 1 + \sum_{i=1}^{k} |A_i|(n - |A_i|) \\
&= n^2 - 1 - \sum_{i=1}^{k} |A_i|^2.
\end{aligned}$$

□

Hence, the more 'balanced' the sizes of v's flaps are, the higher v's separation. This implies that a leaf of G always has minimum separation.

Remark 4.7. *Let $G = (V, E)$ and $v \in V$ with $|\mathcal{F}(v)| = 1$. Then,* $\mathrm{sep}(v) = 2(n-1)$. *This holds especially if v is a leaf of G.*

Proof. By Proposition 4.6 (ii) we have

$$\mathrm{sep}(v) = n^2 - 1 - (n-1)^2 = 2(n-1).$$

If v is a leaf, $\mathcal{F}(v) = \{V \setminus \{v\}\}$, so $|\mathcal{F}(v)| = 1$. □

As we will make frequent use of balancing arguments of flaps in our proofs, we formalize them in the next lemma.

Lemma 4.8. *(i) Let $k, \ell, N \in \mathbb{N}$ with $N \geq k \geq \ell$. For all $a_1, \ldots, a_k \in \mathbb{N}$ with $\sum_{i=1}^{k} a_i = N$, we have*

$$\sum_{i=1}^{k} a_i^2 \leq (N - \ell + 1)^2 + \ell - 1.$$

(ii) Let $k, N, c \in \mathbb{N}$. For all $a_1, \ldots, a_k \in \mathbb{N}$ with $\sum_{i=1}^{k} a_i = N$ and $a_i \leq c$ for all $i \in [k]$ it holds

$$\sum_{i=1}^{k} a_i^2 \leq c^2 + (N - c)^2.$$

(iii) Let $N, b_1, b_2 \in \mathbb{N}$ with $b_1 \geq N/2$ and $b_2 \geq (N - b_1)/2$. For all $a_1, a_2, a_3 \in \mathbb{N}$ with $a_1 \geq b_1$ and $a_2 \geq b_2$ and $a_1 + a_2 + a_3 = N$ it holds

$$\sum_{i=1}^{3} a_i^2 \geq b_1^2 + b_2^2 + (N - b_1 - b_2)^2.$$

Proof. (i). Let $a_1 \geq \ldots \geq a_k \in \mathbb{N}$ with $\sum_{i=1}^{k} a_i = N$ such that $\sum_{i=1}^{k} a_i^2$ is maximized. We first show that $a_1 = N - k + 1$ and $a_i = 1$ for all $i \geq 2$. Assume for a moment that $a_i \geq 2$ for some $i \geq 2$. Then, $a_2 \geq 2$. Define $a_1' := a_1 + 1$, $a_2' := a_2 - 1$ and $a_i' := a_i$ for all $i \geq 3$. Then, $a_1', \ldots, a_k' \in \mathbb{N}$ and $\sum_{i=1}^{k} a_i' = N$. We have

$$\sum_{i=1}^{k} (a_i')^2 = (a_1 + 1)^2 + (a_2 - 1)^2 + \sum_{i=3}^{k} a_i^2 = 2a_1 - 2a_2 + 2 + \sum_{i=1}^{k} a_i^2 > \sum_{i=1}^{k} a_i^2.$$

This is a contradiction to the choice of the a_i.

Hence, $a_1 = N - k + 1$ and $a_i = 1$ for all $i \geq 2$, implying

$$\begin{aligned}
\sum_{i=1}^{k} a_i^2 &= (N - k + 1)^2 + k - 1 \\
&= (N - \ell + 1)^2 + \ell - 1 + k^2 - \ell^2 + k - \ell + 2(N + 1)(\ell - k) \\
&= (N - \ell + 1)^2 + \ell - 1 + k^2 - \ell^2 + 2N(\ell - k) \\
&= (N - \ell + 1)^2 + \ell - 1 + (k + \ell)(k - \ell) + 2N(\ell - k) \\
&= (N - \ell + 1)^2 + \ell - 1 + (k - \ell)(\ell + k - 2N) \\
&\leq (N - \ell + 1)^2 + \ell - 1.
\end{aligned}$$

(ii). Let $a_1 \geq \ldots \geq a_k \in \mathbb{N}$ with $\sum_{i=1}^{k} a_i = N$ and $a_i \leq c$ for all $i \in [k]$ such that $\sum_{i=1}^{k} a_i^2$ is maximized.

Case 1: $c \geq N - k + 1$. Let $x := c - (N - k + 1)$, so $0 \leq x \leq c$. By (i) we get

$$\begin{aligned}
\sum_{i=1}^{k} a_i^2 &\leq (N - k + 1)^2 + k - 1 = (c - x)^2 + N + x - c \\
&= c^2 + N - c - 2cx + x^2 + x \leq c^2 + N - c \leq c^2 + (N - c)^2.
\end{aligned}$$

Case 2: $c < N - k + 1$. We show that $a_1 = c$: Assume that $a_1 \leq c - 1$. Note that $a_2 \geq 2$, because otherwise $\sum_{i=1}^{k} a_i = a_1 + k - 1 < N - 1$, in contradiction to the assumption. Define $a_1' := a_1 + 1$, $a_2' := a_2 - 1$ and $a_i' := a_i$ for all $i \geq 3$. Then, $a_1', \ldots, a_k' \in \mathbb{N}$ with $\sum_{i=1}^{k} a_i' = N$ and $a_i' \leq c$ for all $i \in [k]$. As in (i) we get $\sum_{i=1}^{k} (a_i')^2 > \sum_{i=1}^{k} a_i^2$, a contradiction. So we have $a_1 = c$, implying that

$$\sum_{i=1}^{k} a_i^2 = a_1^2 + \sum_{i=2}^{k} a_i^2 \leq a_1^2 + \left(\sum_{i=2}^{k} a_i \right)^2 = c^2 + (N - c)^2.$$

(iii). Let $a_1 \geq a_2 \geq a_3 \in \mathbb{N}$ with $a_1 + a_2 + a_3 = N$ and $a_1 \geq b_1, a_2 \geq b_2$, such that $\sum_{i=1}^{3} a_i^2$ is minimized. We show in two steps that $a_1 = b_1$ and $a_2 = b_2$. Then the assertion follows. Assume for a moment that $a_1 \geq b_1 + 1$. Because $b_1 + 1 \geq N/2 + 1$ we have $a_3 \leq N/2 - 1 \leq a_1 - 2$. Define $a_1' := a_1 - 1, a_2' := a_2$ and $a_3' := a_3 + 1$. Then a_1', a_2', a_3' fulfill all conditions and we get

$$\begin{aligned}\sum_{i=1}^{3}(a_i')^2 &= \sum_{i=1}^{3} a_i^2 + (a_1')^2 + (a_3')^2 - a_1^2 - a_3^2 \\ &= \sum_{i=1}^{3} a_i^2 + (a_1 - 1)^2 + (a_3 + 1)^2 - a_1^2 - a_3^2 \\ &= \sum_{i=1}^{3} a_i^2 - 2(a_1 - a_3 - 1) < \sum_{i=1}^{3} a_i^2,\end{aligned}$$

a contradiction. So $a_1 = b_1$ and we still have to show $a_2 = b_2$. Assume that $a_2 \geq b_2 + 1 \geq (N - a_1)/2 + 1$. Because $a_2 + a_3 = N - a_1$, we have $a_3 \leq (N - a_2)/2 - 1 \leq b_2 - 1$. Define $a_1' := a_1, a_2' := a_2 - 1$ and $a_3' := a_3 + 1$. Then a_1', a_2', a_3' fulfill all conditions and as in the first part we get

$$\sum_{i=1}^{3}(a_i')^2 < \sum_{i=1}^{3} a_i^2,$$

a contradiction. □

In the following two sections we prove our first two main results (Theorem 4.9 and Theorem 4.21), giving a characterization of SE graphs for the extreme destroyer under different conditions.

4.4 Characterization of SE trees

Intuitively, trees are not very robust graphs in the context of vertex destruction. Because there are no 2-connected subgraphs, many swaps lead to a restructuring of the whole graph. This intuition is confirmed by the following theorem, which we will prove in this section.

Theorem 4.9. *Let $G = (V, E)$ be an SE tree with at least two max-sep vertices. Then G is a path of length 3.*

We start with some basic auxiliary lemmas.

Lemma 4.10. *Let $G = (V, E)$ be a graph. Let $a, b, c \in V$ and consider the swap $s = (a, b, c)$. Then $\mathrm{sep}^s(a) = \mathrm{sep}(a)$, $\mathrm{sep}^s(b) \leq \mathrm{sep}(b)$ and $\mathrm{sep}^s(c) \geq \mathrm{sep}(c)$. If G is a tree, we get $<$ instead of $\leq$ and $>$ instead of $\geq$.*

Proof. For $v \in V$, denote by $\mathcal{F}^s(v)$ the set of v-flaps in the graph G^s. Due to Proposition 4.6 (ii) we have

$$\operatorname{sep}(v) - \operatorname{sep}^s(v) = \sum_{A \in \mathcal{F}^s(v)} |A|^2 - \sum_{A \in \mathcal{F}(v)} |A|^2. \tag{4.2}$$

For the first property, note that $\mathcal{F}^s(a) = \mathcal{F}(a)$, so $\operatorname{sep}(a) - \operatorname{sep}^s(a) = 0$.

For the second property let $A_a \in \mathcal{F}(b)$ be the b-flap that contains a and let $A_c \in \mathcal{F}(b)$ be the b-flap that contains c. Both, $A_a = A_c$ and $A_a \neq A_c$ are possible. We have $\mathcal{F}^s(b) = (\mathcal{F}(b) \setminus \{A_a, A_c\}) \cup \{A_a \cup A_c\}$. For $A_a = A_c$ we get $\mathcal{F}^s(b) = \mathcal{F}(b)$, so $\operatorname{sep}(b) - \operatorname{sep}^s(b) = 0$. Otherwise, A_a and A_c are disjoint, so (4.2) yields

$$\operatorname{sep}(b) - \operatorname{sep}^s(b) = |A_a \cup A_c|^2 - |A_a|^2 - |A_c|^2 > 0.$$

Note that if G is a tree, then also G^s is a tree. Hence, the only $a - c$-path in G^s is the edge $\{a, c\}$ and in G, every $a - c$-path contains the edge $\{a, b\}$ and therefore $A_a \neq A_c$.

For the third property let $A^s_a \in \mathcal{F}^s(c)$ be the c-flap that after the swap contains a and let $A^s_b \in \mathcal{F}^s(c)$ be the c-flap that after the swap contains b. Then, $\mathcal{F}(c) = (\mathcal{F}^s(c) \setminus \{A^s_a, A^s_b\}) \cup \{A^s_a \cup A^s_b\}$. For $A^s_a = A^s_b$ we get $\mathcal{F}^s(c) = \mathcal{F}(c)$, so $\operatorname{sep}(c) - \operatorname{sep}^s(c) = 0$. Otherwise, A^s_a and A^s_b are disjoint, so (4.2) yields

$$\operatorname{sep}(c) - \operatorname{sep}^s(c) = |A^s_a|^2 + |A^s_b|^2 - |A^s_a \cup A^s_b|^2 < 0.$$

Note that if G is a tree, we always have $A^s_a \neq A^s_b$. □

Lemma 4.11. *Let $G = (V, E)$ be a graph. Let $\ell \in \mathbb{N}$ and $v, w_1, \ldots, w_\ell \in V$. If for every $i, j \in [\ell]$ with $i \neq j$ there exists a v-w_i-path that does not contain w_j, then $\sum_{i=1}^{\ell} \operatorname{rel}_{w_i}(v) \leq n - 1$.*

Proof. We prove the claim by showing that for all $i \in [\ell]$ the sets $\mathcal{R}_{w_i}(v)$ are pairwise disjoint. Because $v \notin \mathcal{R}_{w_i}(v)$, this implies

$$\sum_{i=1}^{\ell} \operatorname{rel}_{w_i}(v) = \sum_{i=1}^{\ell} |\mathcal{R}_{w_i}(v)| = \Big| \bigcup_{i=1}^{\ell} \mathcal{R}_{w_i}(v) \Big| \leq |V \setminus \{v\}| \leq n - 1$$

and we are done. So let $i, j \in [\ell]$ with $i \neq j$ and $u \in \mathcal{R}_{w_i}(v)$. We show that $u \notin \mathcal{R}_{w_j}(v)$. Note that w_j and v lie in the same w_i-flap, because they are connected by a path that does not contain w_i. Because $u \in \mathcal{R}_{w_i}(v)$, u and v lie in different w_i-flaps, therefore u and w_j also lie in different w_i-flaps. Hence, there exists a w_i-u-path that does not contain w_j. By assumption of the lemma there also exists a v-w_i-path that does not contain w_j. This implies that v and u lie in the same w_j-flap, so $u \notin \mathcal{R}_{w_j}(v)$. □

Lemma 4.12. *Let $G = (V, E)$ be a graph and let $H = (V', E')$ be a connected subgraph of G. Let $a, b, c \in V'$, such that the swap $s := (a, b, c)$ keeps the vertices of H connected.*

(i) For every $v \in V \setminus V'$ it holds $\operatorname{sep}^s(v) = \operatorname{sep}(v)$.

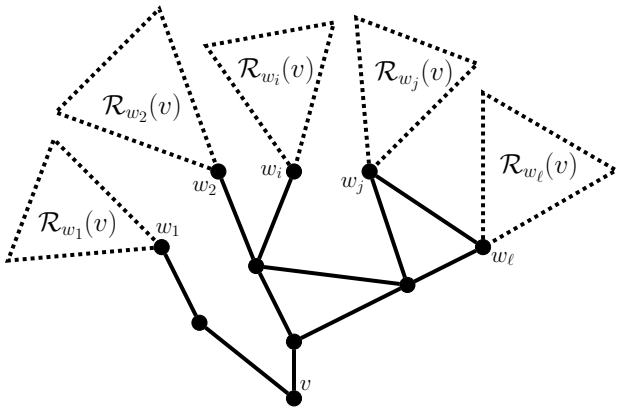

Figure 4.3: Situation in Lemma 4.11.

(ii) For every $v \in V \setminus V'$ and $w \in V'$ it holds $\mathrm{rel}_v^s(w) = \mathrm{rel}_v(w)$.

Proof. (i). Let $v \in V \setminus V'$ and let $A_1, \dots, A_\ell$ denote the v-flaps of G. Because H is connected and $v \notin V'$, one of these flaps contains H as subgraph. Let w.l.o.g. $H \subseteq A_1$. Because both edges $\{a, b\}$ and $\{a, c\}$ are located inside H and the swap s keeps H connected, A_1 is also a v-flap of G^s. All the other flaps do not change, so $\mathcal{F}(v) = \mathcal{F}^s(v)$ and $\mathrm{sep}^s(v) = \mathrm{sep}(v)$.

(ii) Let $v \in V \setminus V'$ and $w \in V'$. As above, let $\mathcal{F}(v) = \{A_1, \dots, A_\ell\}$ such that $H \subseteq A_1$. By definition, $\mathcal{R}_v(w) = \bigcup_{i=2}^{\ell} A_i$. Since $\mathcal{F}(v) = \mathcal{F}^s(v)$, the relevance of v for w doesn't change with the swap s, so $\mathrm{rel}_v^s(w) = \mathrm{rel}_v(w)$. □

Lemma 4.13. *Let $G = (V, E)$ be a graph and $v, w \in V$ with $v \neq w$. Let $A \in \mathcal{F}(v)$ be the v-flap with $w \in A$ and $B \in \mathcal{F}(w)$ be the w-flap with $v \in B$.*

(i) $A \cup B = V$.

(ii) For every $B' \in \mathcal{F}(w)$ with $v \notin B'$ we have $B' \subset A$.

(iii) If G is a tree and v and w are neighbors in G, then A and B form a partition of V.

Proof. (i). Let $u \in V \setminus A$ and let P be a u-w-path. Because u and w lie in different v-flaps, v has to lie on P. Hence, P contains a u-v-path that does not contain w. But then, v and u lie in the same w-flap, so $u \in B$.

(ii). Let $B' \in \mathcal{F}(w)$ with $v \notin B'$. Then $B' \cap B = \emptyset$, so by (i) we get $B' \subseteq A$. Since $w \in A \setminus B'$, we get $B' \subset A$.

(iii). Due to (i) we already know that $A \cup B = V$, so it suffices to show that $A \cap B = \emptyset$. Let $u \in A$. Since u and w are in the same v-flap and G is a tree, there is a unique w-u-path P with $v \notin P$. Hence, $\tilde{P} := (v, w) + P$ is the unique v-u-path in G. Because $w \in \tilde{P}$, v and u lie in different w-flaps, so $u \notin B$. □

If a vertex v separates two vertices a and b, intuitively the relevance of v for a has to be larger than the relevance of b for a. This intuition is formalized in the next proposition.

Proposition 4.14. *Let $G = (V, E)$ and $v, a, b \in V$, such that a and b lie in different v-Flaps. Then,* $\mathrm{rel}_v(a) > \mathrm{rel}_b(a)$.

Proof. Let $A \in \mathcal{F}(v)$ with $a \in A$ and let $B \in \mathcal{F}(b)$ with $a \in B$. Then, $v \in B$ and $b \notin A$. By Lemma 4.13 (ii) we get $A \subset B$, so $|A| < |B|$. With Proposition 4.6 (ii),

$$\mathrm{rel}_v(a) = n - |A| > n - |B| = \mathrm{rel}_b(a).$$

□

In the following we present some results for trees. An argument that is used repeatedly, is as follows: In a tree we always find a vertex that lies somewhere 'in the center' of the tree and therefore has a certain minimum separation. Consequently, every max-sep vertex in the tree has to have at least this separation, implying that its flaps cannot exceed a certain size.

Lemma 4.15. *For every tree $G = (V, E)$ there exists a vertex $v \in V$ with*

$$\mathrm{sep}(v) \geq \frac{n^2}{2} + n - 2.$$

Proof. Let $m := \min\limits_{v \in V} \max\limits_{A \in \mathcal{F}(v)} |A|$. Choose $v \in V$ that minimizes $\max\limits_{A \in \mathcal{F}(v)} |A|$ with corresponding flap $A \in \mathcal{F}(v)$, so $|A| = m$. We first show that $m \leq n/2$: Let w be the neighbor of v in A. Due to the choice of m it holds $m \leq \max\limits_{B \in \mathcal{F}(w)} |B|$. For every flap $B \in \mathcal{F}(w)$ with $v \notin B$, by Lemma 4.13 (ii) we have $B \subset A$. Consequently, $|B| < |A| = m$. Therefore, the w-flap $B_w \in \mathcal{F}(w)$ with $v \in B_w$ is of size $|B_w| \geq m$. Due to Lemma 4.13 (iii), A and B_w form a partition of V, so

$$n = |V| = |A| + |B_w| \geq m + m = 2m.$$

Thus, $m \leq n/2$. Because $m \in \mathbb{N}$, this implies $m \leq \lfloor n/2 \rfloor$. By Proposition 4.6 (ii) we have

$$\mathrm{sep}(v) = n^2 - 1 - \sum_{B \in \mathcal{F}(v)} |B|^2.$$

Applying Lemma 4.8 (ii) with $|B|, B \in \mathcal{F}(w)$, for the a_i's, $N = n - 1$ and $c = \lfloor n/2 \rfloor$ we get

$$n^2 - 1 - \sum_{B \in \mathcal{F}(v)} |B|^2 \geq n^2 - 1 - \left(\left\lfloor \frac{n}{2} \right\rfloor^2 + \left(n - 1 - \left\lfloor \frac{n}{2} \right\rfloor \right)^2 \right).$$

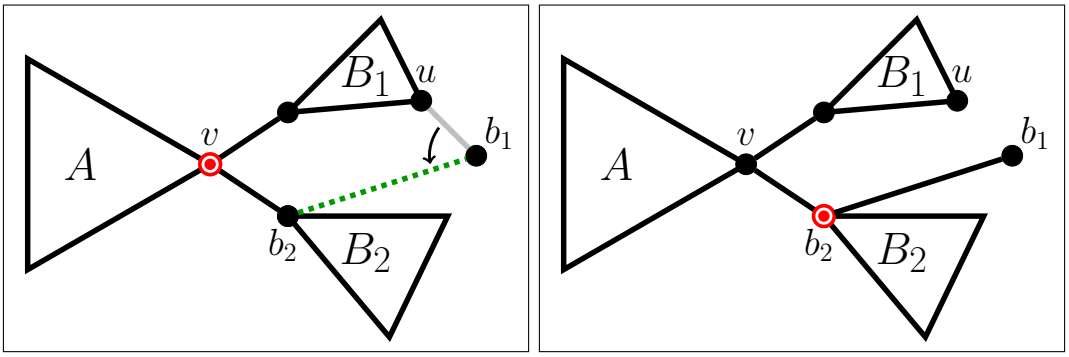

Figure 4.4: Swap $s = (b_1, u, b_2)$ from the proof of Lemma 4.17. If b_2 is no max-sep vertex after the swap, it is profitable for b_1.

If n is even, this implies

$$\operatorname{sep}(v) \geq \frac{n^2}{2} + n - 1$$

and for odd n we get

$$\operatorname{sep}(v) \geq \frac{n^2}{2} + n - \frac{3}{2}.$$

Hence, $\operatorname{sep}(v) \geq n^2/2 + n - 2$. □

Lemma 4.16. *Let $G = (V, E)$ be a tree and $v \in V$ a max-sep vertex of G. Then for every $A \in \mathcal{F}(v)$ it holds $|A| < \frac{n}{\sqrt{2}}$.*

Proof. For $n = 3$ every flap is of size at most $2 = \frac{2n}{3} \leq \frac{n}{\sqrt{2}}$, so let $n \geq 4$. Due to Lemma 4.15 there exists a vertex $w \in V$ with $\operatorname{sep}(w) \geq \frac{n^2}{2} + n - 2$. Let $\mathcal{F}(v) = \{A_1, \ldots, A_k\}$ for some $k \in \mathbb{N}$ and assume that $|A_j| \geq \frac{n}{\sqrt{2}}$ for some $j \in [k]$. Then, by Proposition 4.6 (ii),

$$\begin{aligned}\operatorname{sep}(v) &= n^2 - 1 - \sum_{i=1}^{k} |A_i|^2 \leq n^2 - 1 - |A_j|^2 \leq n^2 - 1 - \left(\frac{n}{\sqrt{2}}\right)^2 \\ &= \frac{n^2}{2} - 1 \overset{n \geq 4}{<} \frac{n^2}{2} + n - 2 \leq \operatorname{sep}(w),\end{aligned}$$

in contradiction to v being a max-sep vertex. □

Lemma 4.17. *Let $G = (V, E)$ be an SE tree with at least two max-sep vertices. Then for every max-sep vertex v and every $A \in \mathcal{F}(v)$ it holds $|A| < \frac{2n-1}{3}$.*

Proof. Let $v \in V$ be a max-sep vertex such that $\max_{A \in \mathcal{F}(v)} |A|$ is maximized in v with corresponding flap A. It suffices to prove that the claim holds for v. If $\deg(v) = 2$, we get

$$\operatorname{sep}(v) = n^2 - 1 - |A|^2 - (n - |A| - 1)^2 = 2n(|A| + 1) - 2(|A|^2 + |A| + 1).$$

On the other hand, by Lemma 4.15, we get $\text{sep}(v) \geq n^2/2 + n - 2$. A straightforward calculation shows that the inequality

$$2n(|A| + 1) - 2(|A|^2 + |A| + 1) \geq n^2/2 + n - 2$$

already implies $|A| \in [n/2 - 1, n/2]$, thus $|A| \leq (2n - 1)/3$.

So let $\deg(v) \geq 3$. Then there exist $B_1, B_2 \in \mathcal{F}(v) \setminus \{A\}$, such that $B_1 \neq B_2$ and $|B_1| \leq |B_2|$. Let b_1 be a leaf of B_1 with father u and b_2 be the neighbor of v in B_2.

We consider the swap $s = (b_1, u, b_2)$ (see Figure 4.4).

Before we proceed with the proof of the lemma, we prove the following claim:

$$b_2 \in \text{MS}(G^s). \tag{4.3}$$

Assume for a moment that (4.3) is not true. We first show that

$$\text{MS}(G^s) = \text{MS}(G) \setminus \{v\} \tag{4.4}$$

Denote by P the unique b_1-b_2-path in G. We first prove three auxiliary claims:

(i) $\text{sep}^s(w) = \text{sep}(w)$ for all $w \notin P$.

(ii) $\text{sep}^s(w) < \text{sep}(w)$ for all $w \in P \setminus \{b_1, b_2\}$.

(iii) The swap s doesn't change the maximum separation, i.e.,

$$\max_{w \in V} \text{sep}^s(w) = \max_{w \in V} \text{sep}(w).$$

(i). Note that the swap s keeps the vertices of P connected, so due to Lemma 4.12 (i) with $H = P$ we have $\text{sep}^s(w) = \text{sep}(w)$ for all $w \notin P$.

(ii). Let $w \in P \setminus \{b_1, b_2\}$ and $\mathcal{F}(w) = \{C_1, \ldots, C_k\}$. Since w lies on the unique b_1-b_2-path, b_1 and b_2 lie in different w-flaps, so w.l.o.g. let $b_1 \in C_1$ and $b_2 \in C_2$. We show that

$$C_1 \subseteq B_1 \text{ and } C_2 \supseteq B_2. \tag{4.5}$$

If $w = v$, we have $B_1 = C_1$ and $B_2 = C_2$, so let $w \neq v$. In this case, $w \in B_1$ and $v \notin C_1$, so Lemma 4.13 (ii) gives $C_1 \subset B_1$. Moreover, $v \in C_2$ and $w \notin B_2$, so Lemma 4.13 (ii) gives $B_2 \subset C_2$. (4.5) implies

$$|C_1| \leq |B_1| \leq |B_2| \leq |C_2|. \tag{4.6}$$

Finally, note that $\mathcal{F}^s(w) = \{C_1 \setminus \{b_1\}, C_2 \cup \{b_1\}, C_3, \ldots, C_k\}$. Hence, with Proposition 4.6,

$$\begin{aligned}
\text{sep}^s(w) &= n^2 - 1 - (|C_1| - 1)^2 - (|C_2| + 1)^2 - \sum_{i=3}^{k} |C_i|^2 \\
&= n^2 - 1 - \sum_{i=1}^{k} |C_i|^2 + |C_1|^2 + |C_2|^2 - (|C_1| - 1)^2 - (|C_2| + 1)^2 \\
&= \text{sep}(w) + 2(|C_1| - |C_2| - 1) \overset{(4.6)}{<} \text{sep}(w).
\end{aligned}$$

(iii). Note that $\mathrm{MS}(G)\setminus\{v\} \subseteq A$: Assume that there is a max-sep vertex w of G with $w \notin A \cup \{v\}$. Denote by W the w-flap that contains v. By Lemma 4.13 (ii), $A \subset W$. Thus, $|A| < |W|$, in contradiction to the choice of v and A. Moreover, $A \cap P = \emptyset$, because otherwise P would have to visit v at least twice. So for every $w \in \mathrm{MS}(G) \setminus \{v\}$ it holds $w \notin P$ and by (i) we get $\mathrm{sep}^s(w) = \mathrm{sep}(w)$. Because $|\mathrm{MS}(G)| \geq 2$, there exists $w' \in \mathrm{MS}(G) \setminus \{v\}$ and it follows that

$$\max_{w\in V} \mathrm{sep}^s(w) \geq \mathrm{sep}^s(w') = \mathrm{sep}(w') = \max_{w\in V} \mathrm{sep}(w).$$

Now let $w' \in \mathrm{MS}(G^s)$. By assumption, $w' \neq b_2$. If $w' \neq b_1$, by (i) and (ii) we get $\mathrm{sep}^s(w') \leq \mathrm{sep}(w)$. If $w' = b_1$, by Lemma 4.10 we have $\mathrm{sep}^s(w') = \mathrm{sep}(w)$. Thus, in any case $\mathrm{sep}^s(w') \leq \mathrm{sep}(w)$ and we get

$$\max_{w\in V} \mathrm{sep}^s(w) = \mathrm{sep}^s(w') \leq \mathrm{sep}(w') \leq \max_{w\in V} \mathrm{sep}(w).$$

and we finished the proof of (iii).

We have established (i),(ii) and (iii), and can complete the proof of (4.4):

Let $\mathrm{ms} := \max_{w\in V} \mathrm{sep}(w)$. Then, $\mathrm{MS}(G) = \{w \in V | \mathrm{sep}(w) = \mathrm{ms}\}$ and by (iii), $\mathrm{MS}(G^s) = \{w \in V | \mathrm{sep}^s(w) = \mathrm{ms}\}$

"$\mathrm{MS}(G) \setminus \{v\} \subseteq \mathrm{MS}(G^s)$": Let $w \in \mathrm{MS}(G) \setminus \{v\}$. As we showed in the proof of (iii), it holds $\mathrm{sep}^s(w) = \mathrm{sep}(w) = \mathrm{ms}$, so $w \in \mathrm{MS}(G^s)$.

"$\mathrm{MS}(G^s) \subseteq \mathrm{MS}(G) \setminus \{v\}$": Let $w \in \mathrm{MS}(G^s)$. By (i) and (ii) we know that $\mathrm{sep}^s(w) \leq \mathrm{sep}(w) \leq \mathrm{ms} = \mathrm{sep}^s(w)$. This implies $\mathrm{sep}(w) = \mathrm{ms}$, so $w \in \mathrm{MS}(G)$ and additionally $\mathrm{sep}(w) = \mathrm{sep}^s(w)$. Because $v \in P$, with (ii) we have $\mathrm{sep}(v) > \mathrm{sep}^s(v)$, so $w \neq v$ and the proof of (4.4) is complete.

We proceed to proof (4.3). We already showed that for every $w \in \mathrm{MS}(G^s)$ it holds $w \notin P$, so by Lemma 4.12 (ii) with $H = P$, we get $\mathrm{rel}^s_w(b_1) = \mathrm{rel}_w(b_1)$. Recall that $w \notin B$, so w and b_1 lie in different v-flaps. Hence, Proposition 4.14 gives $\mathrm{rel}_w(b_1) < \mathrm{rel}_v(b_1)$. This implies

$$\mathcal{C}(G^s, b_1) = \frac{1}{|\mathrm{MS}(G^s)|} \sum_{w\in\mathrm{MS}(G^s)} \mathrm{rel}^s_w(b_1) < \mathrm{rel}_v(b_1). \tag{4.7}$$

Moreover,

$$\begin{aligned}
\mathcal{C}(G,b_1) &= \frac{1}{|\mathrm{MS}(G)|}\sum_{w\in\mathrm{MS}(G)}\mathrm{rel}_w(b_1)\\
&= \frac{\mathrm{rel}_v(b_1)}{|\mathrm{MS}(G)|}+\frac{1}{|\mathrm{MS}(G)|}\sum_{w\in\mathrm{MS}(G^s)}\mathrm{rel}^s_w(b_1)\\
&= \frac{\mathrm{rel}_v(b_1)}{|\mathrm{MS}(G)|}+\frac{|\mathrm{MS}(G^s)|}{|\mathrm{MS}(G)|}\mathcal{C}(G^s,b_1)\\
&\overset{(4.4)}{=} \frac{\mathrm{rel}_v(b_1)}{|\mathrm{MS}(G)|}+\left(1-\frac{1}{|\mathrm{MS}(G)|}\right)\mathcal{C}(G^s,b_1)\\
&= \mathcal{C}(G^s,b_1)+\frac{(\mathrm{rel}_v(b_1)-\mathcal{C}(G^s,b_1))}{|\mathrm{MS}(G)|}\\
&\overset{(4.7)}{>} \mathcal{C}(G^s,b_1).
\end{aligned}$$

Thus, the swap s is profitable, in contradiction to G being an SE. Hence, b_2 is a max-sep vertex of G^s and (4.3) is proved.

In a last step, we complete the proof of the lemma. Let $C\in\mathcal{F}^s(b_2)$ be the b_2-flap of G^s that contains v. By Lemma 4.13 (iii), $C=V\setminus(B_2\cup\{b_1\})$, so $|C|=n-|B_2|-1$. We apply Lemma 4.16 to G^s and b_2 and get $|C|<\frac{n}{\sqrt{2}}$, implying that $|B_2|>n\left(1-\frac{1}{\sqrt{2}}\right)-1$. If $\deg(v)\geq 4$ there exists a flap $B_3\in\mathcal{F}(v)\setminus\{A,B_1,B_2\}$. W.l.o.g., B_1 and B_2 are chosen minimal, so we can assume $|B_1|\leq|B_2|\leq|B_3|$. Then, $|B_2|+|B_3|>(2-\sqrt{2})n-2>n/3$, so

$$|A|\leq n-|B_1|-|B_2|-|B_3|<\frac{2n}{3}-1<\frac{2n-1}{3}$$

and we are done. So let $\deg(v)=3$. By Proposition 4.6 (ii),

$$\mathrm{sep}(v)=n^2-1-|A|^2-|B_1|^2-|B_2|^2.$$

Now assume $|A|\geq\frac{2n-1}{3}$. We already showed that $|B_2|>n\left(1-\frac{1}{\sqrt{2}}\right)-1$. We apply Lemma 4.8 (iii) with $N=n-1, a_1=|A|, a_2=|B_2|, a_3=|B_1|, b_1=\frac{2n-1}{3}$ and $b_2=n\left(1-\frac{1}{\sqrt{2}}\right)-1$ and get

$$\begin{aligned}
\mathrm{sep}(v) &< n^2-1-\left(\frac{2n-1}{3}\right)^2-\left(n\left(1-\frac{1}{\sqrt{2}}\right)-1\right)^2-\left(n\left(\frac{1}{\sqrt{2}}-\frac{2}{3}\right)+\frac{1}{3}\right)^2\\
&= n^2\left(\frac{15\sqrt{2}-17}{9}\right)+n\left(\frac{26-12\sqrt{2}}{9}\right)-\frac{20}{9}\\
&< \frac{n^2}{2}-0.03n^2+n+0.004n-2\\
&< \frac{n^2}{2}+n-2.
\end{aligned}$$

Due to Lemma 4.15 there exists a vertex $w \in V$ with $\text{sep}(w) \geq \frac{n^2}{2}+n-2$, in contradiction to v being a max-sep vertex. □

In the following proofs we look at max-sep vertices that are decentralized in the sense that they do not lie on any path between two other max-sep vertices. We call them *boundary vertices*.

Definition 4.18. *Let $G = (V, E)$ be a graph. A vertex $v \in V$ is called* boundary vertex of G, *if v is a max-sep vertex and there exists $C_v \in \mathcal{F}(v)$ such that $w \in C_v$ for all max-sep vertices $w \neq v$. C_v is called the* core component of v.

Proposition 4.19. *Let $G = (V, E)$ be a graph and $v \in V$. If $A \in \mathcal{F}(v)$ contains a max-sep vertex, it also contains a boundary vertex.*

Proof. Via induction over number k of max-sep vertices in A.

For $k = 1$, A contains only one max-sep vertex, say w. Denote by B the w-flap that contains v. Due to Lemma 4.13 (i), we have $A \cup B = V$. Because A only contains the max-sep vertex w, all other max-sep vertices lie in B, so w is a boundary vertex.

For $k > 1$ choose an arbitrary max-sep vertex $w \in A$ and let B be the w-flap that contains v. If every max-sep vertex apart from w is contained in B, then w is a boundary vertex and we are done. Otherwise, there exists a w-flap $C \in \mathcal{F}(w) \setminus \{B\}$ containing at least one max-sep vertex. Because $v \notin C$, by Lemma 4.13 (ii) we get $C \subset A$. Because $w \in A \setminus C$, the flap C contains at most $k-1$ max-sep vertices. By applying the induction hypothesis to C, we obtain that C contains a boundary vertex. □

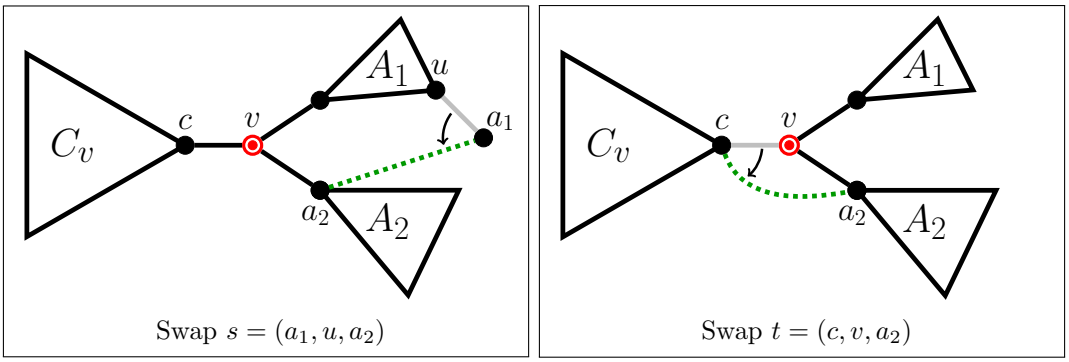

Figure 4.5: Swaps s and t from Lemma 4.20.

Lemma 4.20. *Let $G = (V, E)$ be an SE tree and $v \in V$ a boundary vertex of G with maximal core component C_v. Let c be the neighbor of v in C_v. If $\deg(v) \geq 3$, for every max-sep vertex $w \in V$ it holds $\text{rel}_w(c) = \text{rel}_v(c)$ and all max-sep vertices are boundary vertices.*

Proof. Let $\deg(v) \geq 3$. If G contains only one max-sep vertex, there is nothing to show, so let $|\text{MS}(G)| \geq 2$. Note that $|C_v| \geq 2$ because otherwise $C_v = \{c\}$ and c would be a leaf and no max-sep vertex.

We show that for every max-sep vertex $w \in V$ it holds $\mathrm{rel}_w(c) = \mathrm{rel}_v(c)$. Let $A_1, A_2 \in \mathcal{F}(v) \setminus \{C_v\}$ with $|A_1| \leq |A_2|$. Let a_1 be a leaf of A_1 with father u and a_2 be the neighbor of v in A_2 and consider the swap $s = (a_1, u, a_2)$. The situation is the same as in the proof of Lemma 4.17 with A_1, A_2 instead of B_1, B_2 and a_1, a_2 instead of b_1, b_2 (compare left pictures of Figure 4.4 and Figure 4.5). There, we proved (4.3). With the same arguments, $a_2 \in \mathrm{MS}(G^s)$, so

$$\mathrm{sep}^s(a_2) \geq \mathrm{sep}^s(x) \quad \text{for all } x \in V. \tag{4.8}$$

Now consider the swap $t = (c, v, a_2)$. We show that a_2 is the only max-sep vertex in G^t and start by proving that $\mathrm{sep}^t(a_2) > \mathrm{sep}^s(a_2)$. Let $A_v := \bigcup_{A \in \mathcal{F}(v) \setminus \{A_1, A_2, C_v\}} A$. By Proposition 4.6 (ii) we have

$$\mathrm{sep}^t(a_2) = n^2 - 1 - |C_v|^2 - (|A_1| + |A_v| + 1)^2 - \sum_{\substack{A \in \mathcal{F}(a_2) \\ v \notin A}} |A|^2$$

and

$$\mathrm{sep}^s(a_2) = n^2 - 1 - (|C_v| + |A_1| + |A_v|)^2 - 1 - \sum_{\substack{A \in \mathcal{F}(a_2) \\ v \notin A}} |A|^2,$$

so

$$\begin{aligned} \mathrm{sep}^t(a_2) - \mathrm{sep}^s(a_2) &= (|C_v| + |A_1| + |A_v|)^2 + 1 - |C_v|^2 - (|A_1| + |A_v| + 1)^2 \\ &= 2(|A_1| + |A_v|)(|C_v| - 1) > 0, \end{aligned}$$

where we used that $|C_v| \geq 2$.

It follows that

$$\mathrm{sep}^t(a_2) > \mathrm{sep}^s(a_2). \tag{4.9}$$

The swap t keeps the subgraph on $\{c, v, a_2\}$ connected, so by Lemma 4.12 (i) we get

$$\mathrm{sep}^t(x) = \mathrm{sep}(x) \quad \text{for all } x \in V \setminus \{c, v, a_2\}. \tag{4.10}$$

Applying Lemma 4.10 we also get $\mathrm{sep}^t(c) = \mathrm{sep}(c)$ and $\mathrm{sep}^t(v) < \mathrm{sep}(v)$ and together with (4.10) we have

$$\mathrm{sep}^t(x) \leq \mathrm{sep}(x) \quad \text{for all } x \in V \setminus \{a_2\}. \tag{4.11}$$

Now let $w \in \mathrm{MS}(G) \setminus \{v\}$, so $w \in C_v$. The swap s keeps the subgraph on $V \setminus C_v$ connected, hence Lemma 4.12 (i) gives

$$\mathrm{sep}^s(w) = \mathrm{sep}(w). \tag{4.12}$$

For every $x \in V \setminus \{a_2\}$ it follows that

$$\mathrm{sep}^t(x) \overset{(4.11)}{\leq} \mathrm{sep}(x) \overset{w \in \mathrm{MS}(G)}{\leq} \mathrm{sep}(w) \overset{(4.12)}{=} \mathrm{sep}^s(w) \overset{(4.8)}{\leq} \mathrm{sep}^s(a_2) \overset{(4.9)}{<} \mathrm{sep}^t(a_2).$$

Thus, a_2 is the only max-sep vertex in G^t. Hence, by Proposition 4.6 (i),

$$\mathcal{C}(G^t, c) = \mathrm{rel}^t_{a_2}(c) = n - |C_v| = \mathrm{rel}_v(c). \tag{4.13}$$

Next we prove that for every $w \in \mathrm{MS}(G)$ it holds

$$\mathrm{rel}_w(c) \geq \mathrm{rel}_v(c). \tag{4.14}$$

We distinguish three cases:

Case 1: $w = c$. Because c is not a leaf of G, we have $\mathrm{rel}_v(c) < n - 1$. Hence, $\mathrm{rel}_w(c) = \mathrm{rel}_c(c) = n - 1 > \mathrm{rel}_v(c)$.

Case 2: $w \neq c$ and w is a boundary vertex. Let C_w denote the core component of w. By choice of v we have $|C_w| \leq |C_v|$. For $w = v$ there is nothing to show, so let $w \neq v$. Because $v \in \mathrm{MS}(G)$, we have $v \in C_w$ and because c is a neighbor of v, this also implies $c \in C_w$. Hence, by Proposition 4.6 (i) we have $\mathrm{rel}_w(c) = n - |C_w| \geq n - |C_v| = \mathrm{rel}_v(c)$.

Case 3: w is no boundary vertex. Then, there exist at least two w-flaps that contain a max-sep vertex. Thus, there exists $A \in \mathcal{F}(w)$ with $c \notin A$ that contains a max-sep vertex. Proposition 4.19 ensures the existence of a boundary vertex $x \in A$. Because x and c lie in different w-flaps, Proposition 4.14 gives $\mathrm{rel}_w(c) > \mathrm{rel}_x(c)$. Applying Case 2 to the boundary vertex x, we get $\mathrm{rel}_x(c) \geq \mathrm{rel}_v(c)$, so altogether $\mathrm{rel}_w(c) > \mathrm{rel}_v(c)$.

Because G is an SE, the swap t cannot be profitable. Hence,

$$\begin{aligned}
0 &\geq \mathcal{C}(G, c) - \mathcal{C}(G^t, c) \\
&\overset{(4.13)}{=} \mathcal{C}(G, c) - \mathrm{rel}_v(c) \\
&= \frac{1}{|\mathrm{MS}(G)|} \left(\sum_{w \in \mathrm{MS}(G)} \mathrm{rel}_w(c) \right) - \mathrm{rel}_v(c) \\
&= \frac{1}{|\mathrm{MS}(G)|} \left(\sum_{w \in \mathrm{MS}(G)} \mathrm{rel}_w(c) - \mathrm{rel}_v(c) \right).
\end{aligned}$$

Due to (4.14) every single summand is non-negative. This implies $\mathrm{rel}_w(c) = \mathrm{rel}_v(c)$ for all $w \in \mathrm{MS}(G)$. Hence, the cases 1 and 3 in the proof above never occur. Since Case 2 is the only possible case left, we get that $c \notin \mathrm{MS}(G)$ and all max-sep vertices of G are boundary vertices. □

Proof of Theorem 4.9. By Proposition 4.19, G contains a boundary vertex. Let $v \in V$ be a boundary vertex of G with maximal core component C_v.

Case 1: $\deg(v) = 2$. Then $\mathcal{F}(v) = \{C_v, A\}$, where $A = V \setminus (C_v \cup \{v\})$. By Proposition 4.6 (ii), we get

$$\mathrm{sep}(v) = n^2 - 1 - |C_v|^2 - |A|^2 = n^2 - 1 - |C_v|^2 - (n - |C_v| - 1)^2. \tag{4.15}$$

Because v is a max-sep vertex, by Lemma 4.15 we know that $\mathrm{sep}(v) \geq n^2/2 + n - 2$. Combining this fact and (4.15), a short calculation shows that only two cases are possible:

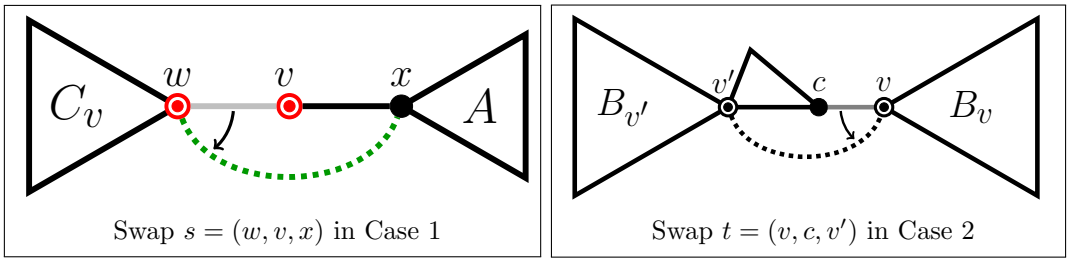

Figure 4.6: Swaps s and t in the proof of Theorem 4.9.

Case 1.a: n is odd and $|C_v| = |A|$.
Case 1.b: n is even and $|A| \in \{|C_v| - 1, |C_v| + 1\}$.

Due to Proposition 4.19 there exists a boundary vertex $w \in C_v$. Denote by C_w the core component of w. Because v is a max-sep vertex, we have $v \in C_w$. By Lemma 4.13 (ii), $A \subset C_w$, so by the choice of v it follows that $|C_v| \geq |C_w| \geq |A|+1$. Since Case 1.a and 1.b are the only possible cases, n must be even and $|C_v| = |C_w| = |A| + 1$. Therefore, $A = C_w \setminus \{v\}$, implying $C_w \cap C_v = \emptyset$. Let P be the unique v-w-path. From the definition of C_w and C_v it follows that $P \setminus \{v, w\} \subseteq C_w \cap C_v = \emptyset$, hence v and w are neighbors. Moreover, by definition of the core component, $\mathrm{MS}(G) \setminus \{v, w\} \subseteq C_w \cap C_v = \emptyset$, hence v and w are the only max-sep vertices in G.

Let x be the neighbor of v in A. If x is a leaf, then $A = \{x\}$ and $|C_v| = |A| + 1 = 2$, so G is a path of length 3, as claimed.

We assume that x is no leaf and derive a contradiction: Assume that $\deg(x) \geq 2$ and consider the swap $s = (w, v, x)$ (see Figure 4.6). We show that the swap s is profitable, in contradiction to G being an SE. Note that $\mathrm{sep}^s(w) = \mathrm{sep}(w)$ and $\mathrm{sep}^s(v) < \mathrm{sep}(v)$ by Lemma 4.10 and $\mathrm{sep}^s(y) = \mathrm{sep}(y)$ for all $y \in V \setminus \{w, v, x\}$ by Lemma 4.12 (i) with $H = \{w, v, x\}$. We show that $\mathrm{sep}^s(x) > \mathrm{sep}(w)$, implying that x is the only max-sep vertex after the swap s. $G^s - x$ consists of the connected components $C_v, \{v\}$ and $A_1, \dots A_\ell$ for some $\ell \geq 1$. Hence, for $A_x := \bigcup_{i=1}^{\ell} A_i$, by Proposition 4.6 (ii) we get

$$\begin{aligned}
\mathrm{sep}^s(x) &= n^2 - 1 - |C_v|^2 - 1 - \sum_{i=1}^{\ell} |A_i|^2 \\
&\geq n^2 - 1 - |C_v|^2 - 1 - \left(\sum_{i=1}^{\ell} |A_i| \right)^2 \\
&= n^2 - 1 - |C_v|^2 - 1 - (n - |C_v| - 2)^2 \\
&> n^2 - 1 - |C_v|^2 - (n - |C_v| - 1)^2 = \mathrm{sep}(v).
\end{aligned}$$

Thus, $\mathrm{MS}(G^s) = \{x\}$. Moreover, by Proposition 4.6 (i) we have $\mathrm{rel}_v(w) = n - |C_v| = \mathrm{rel}^s_x(w)$. Because w is not a leaf, we also have $\mathrm{rel}_w(w) > \mathrm{rel}_v(w)$, so the profit of the swap s is

$$\mathcal{C}(G, w) - \mathcal{C}(G^s, w) = \frac{1}{2}(\mathrm{rel}_v(w) + \mathrm{rel}_w(w)) - \mathrm{rel}^s_x(w) > \mathrm{rel}_v(w) - \mathrm{rel}_v(w) = 0.$$

Thus, s is profitable and this contradiction concludes Case 1.

Case 2: $\deg(v) \geq 3$. Let c be the neighbor of v in C_v. By Lemma 4.20, every max-sep vertex w is also a boundary vertex. For its core component C_w by Lemma 4.17 we have $|C_w| < \frac{2n-1}{3}$, implying that for $B_w := V \setminus C_w$ we have $|B_w| > \frac{n+1}{3}$.

For two boundary vertices w, w' with $w \neq w'$, by Lemma 4.13 (i) we have $C_w \cup C_{w'} = V$ and hence $B_w \cap B_{w'} = \emptyset$. Assume for a moment that there exist at least three boundary vertices w, w', w'' in G. Then

$$|B_w \cup B_{w'} \cup B_{w''}| = |B_w| + |B_{w'}| + |B_{w''}| > n + 1,$$

a contradiction. Thus, there exist only two boundary vertices and hence exactly two max-sep vertices in G. We denote them by v and v'. By Lemma 4.20, $\mathrm{rel}_{v'}(c) = \mathrm{rel}_v(c)$ and because c is no leaf in G, we have $\mathrm{rel}_v(c) < n - 1 = \mathrm{rel}_c(c)$. Because $\mathrm{rel}_{v'}(c) = \mathrm{rel}_v(c) < n - 1 = \mathrm{rel}_c(c)$, we have $v' \neq c$. Because c is the only neighbor of v in C_v, the vertex v' is not a neighbor of v. Consider the swap $t = (v, c, v')$ (Figure 4.6). With Lemma 4.10 we have $\mathrm{sep}^t(v') > \mathrm{sep}(v')$ and $\mathrm{sep}^t(v) = \mathrm{sep}(v)$ and with Lemma 4.12 (i) applied to $H = (V \setminus B_v) \cup \{v\}$ we get $\mathrm{sep}^t(x) = \mathrm{sep}(x)$ for all $x \in B_v \setminus \{v\}$. Thus, for every $b \in B_v$ it holds $\mathrm{sep}^t(b) = \mathrm{sep}(b) \leq \mathrm{sep}(v') < \mathrm{sep}^t(v')$, so $B_v \cap \mathrm{MS}(G^t) = \emptyset$, implying $\mathrm{MS}(G^t) \subseteq C_v$. Now let $w \in \mathrm{MS}(G^t)$. Then, $w \in C_v$. Let $D \in \mathcal{F}^t(w)$ denote the w-flap with $v \in D$ after the swap t. Because the swap t keeps the vertices from B_v connected, we have $B_v \subseteq D$ and with Proposition 4.6 (i) we get $\mathrm{rel}^t_w(v) = n - |D| \leq n - |B_v| < \frac{2n-1}{3}$. But then, the profit of the swap t is

$$\begin{aligned}
\mathcal{C}(G, v) - \mathcal{C}(G^t, v) &= \frac{1}{2}(\mathrm{rel}_{v'}(v) + \mathrm{rel}_v(v)) - \frac{1}{|\mathrm{MS}(G^t)|}\left(\sum_{w \in \mathrm{MS}(G^t)} \mathrm{rel}^t_w(v)\right) \\
&> \frac{1}{2}(\mathrm{rel}_{v'}(v) + \mathrm{rel}_v(v)) - \frac{2n-1}{3} \\
&= \frac{1}{2}(n - |C_{v'}| + n - 1) - \frac{2n-1}{3} \\
&= \frac{1}{2}(|B_{v'}| + n - 1) - \frac{2n-1}{3} \\
&> \frac{1}{2}\left(\frac{n+1}{3} + n - 1\right) - \frac{2n-1}{3} = 0.
\end{aligned}$$

The swap t is profitable, in contradiction to G being a SE. □

4.5 SE graphs with one max-sep vertex

In this section we prove the following theorem:

Theorem 4.21. *The only SE graphs with exactly one max-sep vertex are paths of length 2 or 4.*

Let us briefly present the main ideas. Two arguments are used most frequently: a vertex that lies on a *cycle* has the opportunity to swap one of its cycle-edges to enlarge

this cycle (Lemma 4.25). If after this swap the unique former max-sep vertex lies on the cycle, in many cases the swap is profitable.

The other argument concerns vertices that lie on small v-flaps, where v is the only max-sep vertex of the graph. If the flap is small enough, the neighbors of v in this flap can improve their situation by either expanding a cycle they lie on or by connecting to a neighbor that is more 'secure' that v.

With these and other arguments we are able to show that the max-sep vertex splits the graph G into only two connected components (Theorem 4.23) and that the smaller component is always cycle-free (Theorem 4.27). We proceed by proving that the whole graph has to be a tree (Theorem 4.29) and deduce that it is a small path (Theorem 4.21).

Lemma 4.22. *Let $G = (V, E)$, $v \in V$ and $A \in \mathcal{F}(v)$. Then A contains a vertex w with* $\operatorname{sep}(w) = 2(n-1)$.

Proof. Via induction over $|A|$. If $|A| = 1$, we have $A = \{w\}$ for some leaf w and by Remark 4.7 it follows $\operatorname{sep}(w) = 2(n-1)$.

Now let $|A| \geq 2$ and $a \in A$. If $|\mathcal{F}(a)| = 1$, by Remark 4.7, $\operatorname{sep}(a) = 2(n-1)$ and we are done, so let $|\mathcal{F}(a)| > 1$. Let $B \in \mathcal{F}(a)$ with $v \notin B$. Due to Lemma 4.13 (ii), we have $B \subset A$ and therefore $|B| < |A|$. By applying the induction hypothesis, B contains a vertex w with $\operatorname{sep}(w) = 2(n-1)$. □

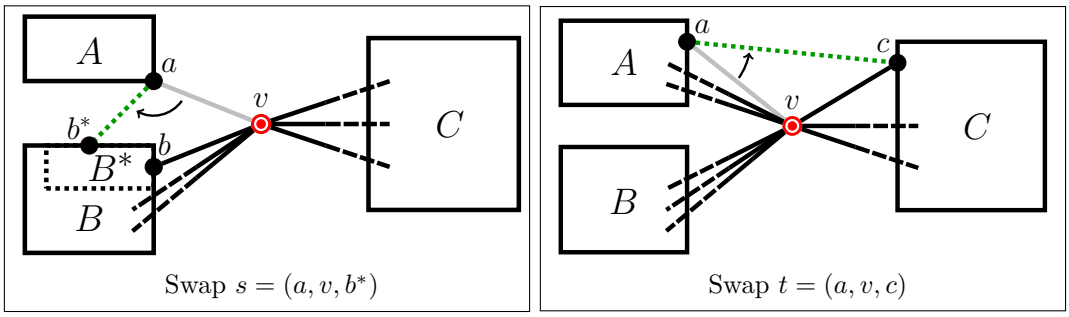

Figure 4.7: Swaps s and t in Theorem 4.23.

Theorem 4.23. *Let $G = (V, E)$ be an SE graph with exactly one max-sep vertex v. Then $|\mathcal{F}(v)| = 2$.*

Proof. First note that $|\mathcal{F}(v)| \neq 1$, because otherwise, due to Remark 4.7 $\operatorname{sep}(v) = 2(n-1)$, so v is not the only max-sep vertex.

Now assume that $|\mathcal{F}(v)| \geq 3$ and let $A, B, C \in \mathcal{F}(v)$ pairwise distinct with $|A| \leq |C|$ and $|B| \leq |C|$. Let $a_1, \ldots, a_k$ be the neighbors of v in A and $b_1, \ldots, b_\ell$ be the neighbors of v in B. Let $a \in \{a_1, \ldots, a_k\}$ with minimum separation and $b \in \{b_1, \ldots, b_\ell\}$ with minimum separation. Let c be a neighbor of v in C.

We are looking for a vertex $b^* \in B$ with $\operatorname{sep}(b^*) = 2(n-1)$. If $\operatorname{sep}(b) = 2(n-1)$, we simply set $b^* := b$. Otherwise, by Remark 4.7 we get $|\mathcal{F}(b)| \geq 2$. In this case,

there exists $B^* \in \mathcal{F}(b)$ with $v \notin B^*$. Due to Lemma 4.22 there exists $b^* \in B^*$ with $\text{sep}(b^*) = 2(n-1)$.

We consider the swaps $s = (a, v, b^*)$ and $t = (a, v, c)$ and prove five auxiliary claims:

(i) $\text{sep}^t(w) = \text{sep}(w)$ for every $w \in A \cup B$.

(ii) If $k = 1$, $\text{sep}^s(b) > \text{sep}(b)$.

(iii) $\text{sep}^s(b^*) \leq \text{sep}^s(v)$.

(iv) If $k = 1$, $a \in \text{MS}(G^s)$.

(v) If $k \geq 2$, $a \in \text{MS}(G^t)$.

(i). The swap t keeps the subgraph on the vertices $\{a, c, v\}$ connected. Hence, with Lemma 4.12 (i) for every w in $V \setminus \{a, c, v\}$ it holds $\text{sep}^t(w) = \text{sep}(w)$. Moreover, by Lemma 4.10 we get $\text{sep}^t(a) = \text{sep}(a)$. Because $A \cup B \subseteq V \setminus \{c, v\}$, the claim follows.

(ii). Let $k = 1$, so there is only one neighbor of v in A.

Case 1: $b = b^*$. In this case $\text{sep}(b) = 2(n-1)$ and $\mathcal{F}^s(b) = \{A, V \setminus (A \cup \{b\})\}$, hence $|\mathcal{F}^s(b)| > 1$ and by Remark 4.7 we get $\text{sep}^s(b) > 2(n-1) = \text{sep}(b)$.

Case 2: $b \neq b^*$. Let $\mathcal{F}(b) = \{R, B_1, \dots B_m\}$ such that $v \in R$. By Proposition 4.6 (ii),

$$\text{sep}(b) = n^2 - 1 - |R|^2 - \sum_{i=1}^{m} |B_i|^2.$$

Because b and b^* lie in the same v-flap, v and b^* have to lie in different b-flaps, hence $b^* \notin R$. W.l.o.g. let $b^* \in B_1$. Observe that $\mathcal{F}^s(b) = \{R \setminus A, B_1 \cup A, B_2, \dots, B_m\}$, so by Proposition 4.6 (ii),

$$\text{sep}^s(b) = n^2 - 1 - (|R| - |A|)^2 - (|B_1| + |A|)^2 - \sum_{i=2}^{m} |B_i|^2,$$

implying that

$$\text{sep}^s(b) - \text{sep}(b) = 2|R||A| - 2|B_1||A| - 2|A|^2 = 2|A|(|R| - |A| - |B_1|).$$

Thus, it suffices to show that $|R| - |A| - |B_1| > 0$.

Recall that R is the b-flap containing v. For every $i \in [m]$ the b-flap B_i doesn't contain v, so by Lemma 4.13 (ii), $B_i \subset B$. Moreover, since A and C are v-flaps not containing b, by Lemma 4.13 (ii) we get $A \subset R$ and $C \subset R$. A and C are disjoint, so $C \subseteq R \setminus A$ and

$$|R| - |A| = |R \setminus A| \geq |C| \geq |B| > |B_1|$$

and (ii) is proved.

(iii). We have $\mathcal{F}^s(b^*) = \{A, V \setminus (A \cup \{b^*\})\}$. Denote the v-Flaps of G by $\mathcal{F}(v) = \{A, B, C, D_1, \dots D_k\}$. Then, $\mathcal{F}^s(v) = \{A \cup B, C, D_1, \dots D_k\}$. Due to Proposition 4.6 (ii), we have

$$\text{sep}^s(b^*) = n^2 - 1 - |A|^2 - (n - 1 - |A|)^2$$

and

$$\begin{aligned}\operatorname{sep}^s(v) &= n^2 - 1 - |C|^2 - (|A| + |B|)^2 - \sum_{i=1}^{k} |D_i|^2 \\ &\geq n^2 - 1 - |C|^2 - \left((|A| + |B|)^2 + \sum_{i=1}^{k} |D_i| \right)^2 \\ &= n^2 - 1 - |C|^2 - (n - 1 - |C|)^2,\end{aligned}$$

implying that

$$\begin{aligned}\operatorname{sep}^s(v) - \operatorname{sep}^s(b^*) &= 2(|A|^2 - |C|^2 + (n-1)(|C| - |A|)) \\ &= 2(|C| - |A|)(n - 1 - |A| - |C|).\end{aligned}$$

Since $|C| \geq |A|$ and $n - 1 \geq n - |B| \geq |A| + |C|$, the proof of (iii) is complete.

(iv). Let $k = 1$ and assume that $a \notin \mathrm{MS}(G^s)$. We lead this assumption to a contradiction by showing that the swap s is profitable. First note that $\mathcal{F}^s(b^*) = \{A, V \setminus (A \cup \{b^*\})\}$, so by Proposition 4.6 (i) we get

$$\operatorname{rel}^s_{b^*}(a) = n - |A| = \operatorname{rel}_v(a). \tag{4.16}$$

Next, we show

$$\operatorname{rel}^s_w(a) < \operatorname{rel}_v(a) \quad \text{for all } w \in V \setminus \{a, b^*\}. \tag{4.17}$$

To see this, let $w \in V \setminus \{a, b^*\} = (A \setminus \{a\}) \cup (V \setminus (A \cup \{b^*\}))$. Let $D \in \mathcal{F}^s(w)$ be the w-flap that contains a after the swap s. Obviously, $b^* \in D$.

If $w \in A \setminus \{a\}$, then $V \setminus (A \cup \{b^*\}) \in \mathcal{F}^s(b^*)$ with $w \notin V \setminus (A \cup \{b^*\})$, so by Lemma 4.13 (ii) we get $V \setminus (A \cup \{b^*\}) \subset D$. Because $a, b^* \in D$, we have $D \supseteq (V \setminus A) \cup \{a\}$, implying $D \supseteq C \cup \{a\}$, so $|D| \geq |C| + 1 > |C| \geq |A|$ and by Proposition 4.6 (i) we get

$$\operatorname{rel}^s_w(a) = n - |D| < n - |A| = \operatorname{rel}_v(a).$$

Now let $w \in V \setminus (A \cup \{b^*\})$. Because $b^* \in D$ and $A \in \mathcal{F}^s(b^*)$ with $w \notin A$, by Lemma 4.13 (ii) we get $A \subset D$. Thus,

$$\operatorname{rel}^s_w(a) = n - |D| < n - |A| = \operatorname{rel}_v(a)$$

and the proof of (4.17) is complete.

Now we can estimate the profit of the swap s. We don't know, whether $b^* \in \mathrm{MS}(G^s)$ or not, but due to (iii) we know that $\mathrm{MS}(G^s) \setminus \{b^*\} \neq$. Since we assumed $\mathrm{MS}(G) = \{v\}$, we have $\mathcal{C}(G, a) = \operatorname{rel}_v(a)$ and get

$$\begin{aligned}\mathcal{C}(G, a) - \mathcal{C}(G^s, a) &= \operatorname{rel}_v(a) - \frac{1}{|\mathrm{MS}(G^s)|} \sum_{w \in \mathrm{MS}(G^s)} \operatorname{rel}^s_w(a) \\ &= \frac{1}{|\mathrm{MS}(G^s)|} \sum_{w \in \mathrm{MS}(G^s)} \operatorname{rel}_v(a) - \operatorname{rel}^s_w(a) \\ &\overset{(4.16)}{=} \frac{1}{|\mathrm{MS}(G^s)|} \sum_{w \in \mathrm{MS}(G^s) \setminus \{b^*\}} \operatorname{rel}_v(a) - \operatorname{rel}^s_w(a) \overset{(4.17)}{>} 0.\end{aligned}$$

Thus, the swap s is profitable, in contradiction to G being an SE.

(v). Let $k \geq 2$ and assume that $a \notin \mathrm{MS}(G^t)$. We show that the swap t is profitable. First, we prove

$$\mathrm{rel}_w^t(a) < n - |A| = \mathrm{rel}_v(a) \quad \text{for all } w \in V \setminus \{a\}. \tag{4.18}$$

So let $w \in V \setminus \{a\}$ and let $D \in \mathcal{F}^t(w)$ be the w-flap that contains a after the swap t.

If $w \in A \setminus \{a\}$, then C remains connected after the swap t, hence $C \cup \{a\} \subseteq D$ and $|D| > |C| \geq |A|$. By Proposition 4.6 (i) we get

$$\mathrm{rel}_w^t(a) = n - |D| < n - |A| = \mathrm{rel}_v(a).$$

Otherwise, $w \in V \setminus A$. In this case A remains connected after the swap t, hence $A \cup \{c\} \subseteq D$ and $|D| > |A|$. Again, by Proposition 4.6 (i) we get

$$\mathrm{rel}_w^t(a) = n - |D| < n - |A| = \mathrm{rel}_v(a).$$

For the profit of t it follows

$$\begin{aligned}\mathcal{C}(G,a) - \mathcal{C}(G^t,a) &= \mathrm{rel}_v(a) - \frac{1}{|\mathrm{MS}(G^t)|} \sum_{w \in \mathrm{MS}(G^t)} \mathrm{rel}_w^t(a) \\ &= \frac{1}{|\mathrm{MS}(G^t)|} \sum_{w \in \mathrm{MS}(G^t)} \mathrm{rel}_v(a) - \mathrm{rel}_w^t(a) \overset{(4.18)}{>} 0,\end{aligned}$$

a contradiction to G being an SE.

With (i)-(v) we are able to prove two further claims:

(C1) $\mathrm{sep}(a) \geq \mathrm{sep}(b)$.

(C2) $\mathrm{sep}(a) > \mathrm{sep}(b)$ if $|A| \leq |B|$.

(C1). Assume that $\mathrm{sep}(a) < \mathrm{sep}(b)$. For $k = 1$ we get

$$\mathrm{sep}^s(b) \overset{(ii)}{>} \mathrm{sep}(b) > \mathrm{sep}(a) = \mathrm{sep}^s(a),$$

where the last equation follows from Lemma 4.10. This is a contradiction to (iv). For $k \geq 2$ we have

$$\mathrm{sep}^t(b) \overset{(i)}{=} \mathrm{sep}(b) > \mathrm{sep}(a) = \mathrm{sep}^t(a),$$

where again the last equation follows from Lemma 4.10. This is a contradiction to (v).

(C2). Now let additionally $|A| \leq |B|$, so $|A| \leq |B| \leq |C|$, implying $|A| < |V|/3$. Assume that $\mathrm{sep}(a) = \mathrm{sep}(b)$. We show that the swap t is profitable. Note that $k \geq 2$, because otherwise by (ii) and Lemma 4.10 we get $\mathrm{sep}^s(b) > \mathrm{sep}(b) = \mathrm{sep}(a) = \mathrm{sep}^s(a)$, in contradiction to (iv). Hence, there exists a neighbor a' of v in A with $a' \neq a$. By choice of a we have $\mathrm{sep}(a') \geq \mathrm{sep}(a)$ and by assumption, $\mathrm{sep}(b) = \mathrm{sep}(a)$. Because $a, a', b \in A \cup B$, (i) implies $\mathrm{sep}^t(w) = \mathrm{sep}(w)$ for all $w \in \{a, a', b\}$. Thus,

$$\mathrm{sep}^t(a') = \mathrm{sep}(a') \geq \mathrm{sep}(a) = \mathrm{sep}^t(a)$$

and

$$\operatorname{sep}^t(b) = \operatorname{sep}(b) = \operatorname{sep}(a) = \operatorname{sep}^t(a).$$

With (v) we get $a, a', b \in \operatorname{MS}(G^t)$.

Let P_1 be an a-a'-path in A and let $P_2 := (a, c, v, b)$. Since P_1 doesn't contain b and P_2 doesn't contain a', we can apply Lemma 4.11 with $v = a, w_1 = a', w_2 = b$ and the paths P_1, P_2 and get

$$\operatorname{rel}^t_{a'}(a) + \operatorname{rel}^t_b(a) \leq n - 1. \tag{4.19}$$

Moreover, as shown in (4.18), for every $w \in V \setminus \{a\}$ it holds $\operatorname{rel}^t_w(a) \leq n - |A|$, so for $M := \operatorname{MS}(G^t) \setminus \{a, a', b\}$ we get

$$\begin{aligned}
\mathcal{C}(G^t, a) &= \frac{1}{|M|+3}\left(\operatorname{rel}^t_{a'}(a) + \operatorname{rel}^t_b(a) + \operatorname{rel}^t_a(a) + \sum_{w\in M} \operatorname{rel}^t_w(a)\right) \\
&= \frac{1}{|M|+3}\left(\operatorname{rel}^t_{a'}(a) + \operatorname{rel}^t_b(a) + n - 1 + \sum_{w\in M} \operatorname{rel}^t_w(a)\right) \\
&\overset{(4.19)}{\leq} \frac{1}{|M|+3}\left(2(n-1) + \sum_{w\in M} \operatorname{rel}^t_w(a)\right) \\
&< \frac{1}{|M|+3}\left(2(n-1) + |M|(n-|A|)\right) \\
&< \frac{1}{|M|+3}(|M|+3)(n-|A|) && (|A| < n/3) \\
&= n - |A|.
\end{aligned}$$

Recall that $\mathcal{C}(G, a) = \operatorname{rel}_v(a) = n - |A|$ by Proposition 4.6 (i), so $\mathcal{C}(G^t, a) < \mathcal{C}(G, a)$, in contradiction to G being an SE and the proof of (C2) is complete.

Finally, observe that (C1) and (C2) are contradicting statements: For symmetry reasons, (C1) also applies if we swap the roles of a and b, so we get $sep(a) = \operatorname{sep}(b)$. But this is a contradiction to (C2). Hence, the assumption $|\mathcal{F}(v)| \geq 3$ has to be wrong and we are done. □

In a next step, we want to show that at most one of the two flaps from Theorem 4.23 can contain a cycle. To this end we will introduce a certain kind of swap that can be performed by vertices on a cycle and is profitable in many cases. This is done in Lemma 4.25.

Definition 4.24. *Let C be a cycle in G and $w \in V$. A vertex $c \in C$ is called* connecting vertex *of C and w, if either $w \in C$ or there exists a c-w-path P with $P \cap C = \{c\}$. The path P is called* connecting path *of w and C. If $w \in C$, P is considered a path of length 0, only consisting of the vertex c.*

Lemma 4.25. *Let $G = (V, E), w \in V$ and let $C = (c_1, \ldots, c_k)$ be a cycle in G such that c_1 is a connecting vertex of C and w with the corresponding path $P = (p_1, \ldots, p_\ell)$, where $p_1 = c_1$ and $p_\ell = w$. Let $c_1 \neq w$ and $\{c_2, w\} \notin E$ and consider the swap $s = (c_2, c_1, w)$.*

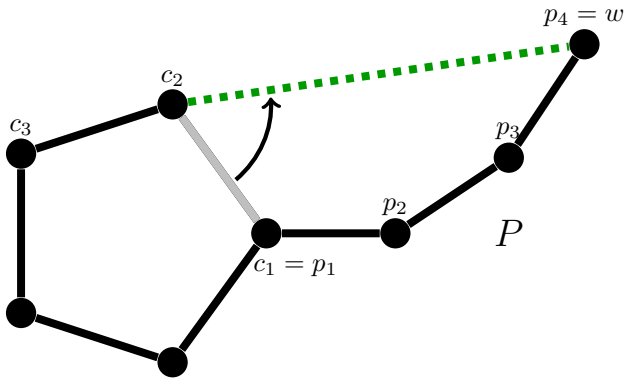

Figure 4.8: Example for swap s in Lemma 4.25.

(i) $\mathrm{sep}^s(v) \leq \mathrm{sep}(v)$ *for all* $v \in V$.

(ii) $\mathrm{rel}_v^s(c_2) \leq \mathrm{rel}_v(c_2)$ *for all* $v \in V$.

(iii) $\mathrm{sep}^s(v) = \mathrm{sep}(v)$ *for all* $v \in (V \setminus P) \cup \{w\}$.

Proof. We start by proving the following claim:

$$\text{For every } v \in V \text{ and every } A \in \mathcal{F}(v) \text{ there exists } B \in \mathcal{F}^s(v) \text{ with } A \subseteq B. \tag{4.20}$$

Let $v \in V, A \in \mathcal{F}(v)$ and $x \in A$. Let $B \in \mathcal{F}^s(v)$ with $x \in B$. We show that $A \subseteq B$. So let $a \in A$. Because B is a connected component of $G^s - v$, it suffices to show that there exists an x-a-path in G^s that does not contain v. Because $x, a \in A$, there exists an x-a-path Q in A and obviously $v \notin Q$. We may assume that Q uses the edge $\{c_1, c_2\}$, because otherwise Q is also a path in G^s and we are done. If we find a c_1-c_2-path Q' that doesn't contain v, we can use a part of this path to circumvent the edge $\{c_1, c_2\}$ in Q and the proof is complete.

Consider the two c_1-c_2-paths (P, c_2) and $(c_1, c_k, c_{k-1}, \ldots, c_3, c_2)$ in G^s. Since P is a connecting path of C and w, these paths only intersect at the vertices c_1 and c_2, so one of them doesn't contain the vertex v and we are done.

We proceed to the proofs of (i)-(iii).

(i). Let $v \in V$. By (4.20) we have $\sum_{A \in \mathcal{F}(v)} |A|^2 \leq \sum_{B \in \mathcal{F}^s(v)} |B|^2$, so with Proposition 4.6 (ii),

$$\mathrm{sep}^s(v) = n^2 - 1 - \sum_{B \in \mathcal{F}^s(v)} |B|^2 \leq n^2 - 1 - \sum_{A \in \mathcal{F}(v)} |A|^2 = \mathrm{sep}(v).$$

(ii). Let $v \in V$, let $A \in \mathcal{F}(v)$ be the v-flap with $c_2 \in A$ and let $B \in \mathcal{F}^s(v)$ be the v-flap with $c_2 \in B$ after the swap s. By (4.20), $A \subseteq B$, so by Proposition 4.6 (i),

$$\mathrm{rel}_v^s(c_2) = n - |B| \leq n - |A| = \mathrm{rel}_v(c_2).$$

(iii). Let $v \in (V \setminus P)$ and let H be the subgraph on the vertices $P \cup \{c_2\}$. Since H is still connected after the swap s, by Lemma 4.12 (i) we get $\text{sep}^s(v) = \text{sep}(v)$. It remains to show that $\text{sep}^s(w) = \text{sep}(w)$. By Lemma 4.10 we get $\text{sep}^s(w) \geq \text{sep}(w)$ and together with (i) the claim follows. □

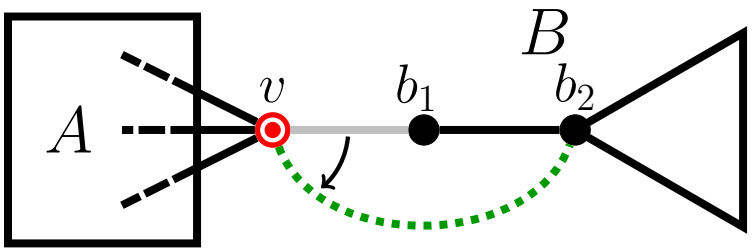

Figure 4.9: Swap s in Lemma 4.26.

Lemma 4.26. *Let $G = (V, E)$ be an SE graph with exactly one max-sep vertex v and $\mathcal{F}(v) = \{A, B\}$, such that $B + v$ is cycle-free. If $|B| \geq 3$, then $|A| > |B|$.*

Proof. Let $|B| \geq 3$ and assume for a moment that $|B| \geq |A|$. Since $B + v$ is cycle-free, there is a unique neighbor b_1 of v in B We start by showing:

$$\text{If } \deg(b_1) \geq 3, \text{ then } \text{sep}(b_1) \geq \text{sep}(v). \tag{4.21}$$

Let $d := \deg(b_1) \geq 3$. Then, $\mathcal{F}(b_1) = \{A \cup \{v\}, B_1, \ldots, B_{d-1}\}$ with $\sum_{i=1}^{d-1} |B_i| = |B| - 1$. We apply Lemma 4.8 (i) with $N = |B| - 1$, $k = d - 1$, $\ell = 2$ and $a_i = |B_i|$ for all $i \in [d-1]$ and get

$$\sum_{i=1}^{d-1} |B_i|^2 \leq (|B| - 2)^2 + 1. \tag{4.22}$$

Further, with Proposition 4.6 (ii):

$$\begin{aligned}
\text{sep}(b_1) &= n^2 - 1 - (|A| + 1)^2 - \sum_{i=1}^{d-1} |B_k|^2 \\
&\overset{(4.22)}{\geq} n^2 - 1 - (|A| + 1)^2 - (|B| - 2)^2 - 1 \\
&= n^2 - 1 - |A|^2 - |B^2| - 2|A| + 4|B| - 6 \\
&\geq n^2 - 1 - |A|^2 - |B^2| + 2|B| - 6 \\
&\geq n^2 - 1 - |A|^2 - |B^2| = \text{sep}(v),
\end{aligned}$$

where for the last two inequalities we used $|B| \geq |A|$ and $|B| \geq 3$.

We will now use (4.21) to come to a contradiction. Because $|B| \geq 3$, the vertex b_1 has at least one neighbor b_2 in B, so $\deg(b_1) \geq 2$. By (4.21), $\deg(b_1) \leq 2$, because v is the only max-sep vertex in G. Hence, $\deg(b_1) = 2$ and $|B| \geq 3$ implies $\deg(b_2) \geq 2$. We

consider the swap $s = (v, b_1, b_2)$ (see Figure 4.9) and show that it is profitable. Note that $\mathcal{F}^s(v) = \mathcal{F}(v) = \{A, B\}$. Moreover, in G^s, the vertex b_2 is the unique neighbor of v in B and B is still cycle free. We apply (4.21) with G^s instead of G and b_2 instead of b_1. Because the degree of b_2 in G^s is at least 3, we get $\text{sep}^s(b_2) \geq \text{sep}^s(v)$. Thus, $\text{MS}(G^s) \setminus \{v\} \neq \emptyset$. We show that

$$\text{rel}^s_w(v) < \text{rel}_v(v) \quad \text{for all } w \in \text{MS}(G^s) \setminus \{v\}. \tag{4.23}$$

Let $w \in \text{MS}(G^s) \setminus \{v\}$, so $w \in A \cup B$. Let $D \in \mathcal{F}^s(w)$ with $v \in D$. If $w \in A$, then $w \notin B$, so by Lemma 4.13 (ii) we have $B \subset D$ and by Proposition 4.6 (ii) we get

$$\text{rel}^s_w(v) = n - |D| \leq n - |B| < n - 1 = \text{rel}_v(v).$$

If $w \in B$, analogously we get $A \subset D$, so

$$\text{rel}^s_w(v) = n - |D| \leq n - |A| < n - 1 = \text{rel}_v(v)$$

and the proof of (4.23) is complete. We can now show that the swap s is profitable:

$$\begin{aligned} \mathcal{C}(G^s, v) &= \frac{1}{|\text{MS}(G^s)|} \sum_{w \in \text{MS}(G^s)} \text{rel}^s_w(v) \\ &\overset{(4.23)}{<} \frac{1}{|\text{MS}(G^s)|} \sum_{w \in \text{MS}(G^s)} \text{rel}_v(v) \\ &= \text{rel}_v(v) = \mathcal{C}(G, v), \end{aligned}$$

in contradiction to G being an SE. □

Theorem 4.27. *Let $G = (V, E)$ be an SE graph with exactly one max-sep vertex v and at least one cycle. Then $\mathcal{F}(v) = \{A, B\}$, such that $A + v$ contains a cycle, $B + v$ is cycle-free and $|A| > |B|$.*

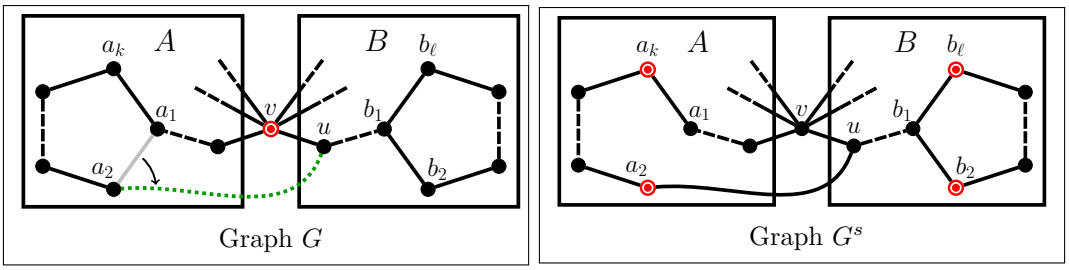

Figure 4.10: Situation before and after swap $s = (a_2, a_1, u)$ in the proof of Theorem 4.27 (i).

Proof. Due to Theorem 4.23, $G - v$ consists of exactly two connected components A and B. W.l.o.g. let $A + v$ contain a cycle C_A. We prove the theorem in two steps:

(i) $B + v$ is cycle-free.

(ii) $|A| > |B|$.

(i). Assume that $B + v$ contains a cycle C_B. Let $C_A = (a_1, \dots, a_k)$ such that a_1 is a connecting vertex of C_A and v and $C_B = (b_1, \dots, b_\ell)$ such that b_1 is a connecting vertex of C_B and v. Note that $v = a_1$ or $v = b_1$ is possible. Let u be a neighbor of v in B. Clearly, $\{a_2, u\} \notin E$. We consider the swap $s = (a_2, a_1, u)$ (see Figure 4.10) and show that this swap is profitable.

First we show

$$\mathrm{rel}^s_w(a_2) < \mathrm{rel}_v(a_2) \quad \text{for all } w \in V \setminus \{a_2\}. \tag{4.24}$$

We start by considering the case $w \in B$. Let $D \in \mathcal{F}^s(w)$ with $a_2 \in D$. Because $w \notin A \cup \{v\}$ and with the swap s we delete an edge in the cycle C_A, all vertices in $A \cup \{v\}$ are connected in $G^s - w$, hence $A \cup \{v\} \subseteq D$. This implies $|A| < |D|$, so Proposition 4.6 (i) gives

$$\mathrm{rel}^s_w(a_2) = n - |D| < n - |A| = \mathrm{rel}_v(a_2).$$

For the case $w = v$, note that $G^s - v$ is still connected, so

$$\mathrm{rel}^s_v(a_2) = n - |G^s - v| = 1 < n - |A| = \mathrm{rel}_v(a_2).$$

Finally, let $w \in A \setminus \{a_2\}$. Let $\mathcal{F}^s(w) = \{W_1, \dots, W_j\}$ with $u \in W_1$. Obviously, also $v \in W_1$ and $a_2 \in W_1$. Thus, for every $2 \le i \le j$, by Lemma 4.13 (ii) we have $W_i \subset A$. This implies $\bigcup_{i=2}^{j} W_i \subseteq A \setminus \{w\}$, so $d := |A| - \sum_{i=2}^{j} |W_i| > 0$. Since $|A| + |B| = n - 1$,

$$|W_1| = n - 1 - \sum_{i=2}^{j} |W_i| = |A| + |B| - \sum_{i=2}^{j} |W_i| = |B| + d, \tag{4.25}$$

so by Proposition 4.6 (ii) we have

$$\begin{aligned}
\mathrm{sep}^s(w) &= n^2 - 1 - |W_1|^2 - \sum_{i=2}^{j} |W_i|^2 \\
&\ge n^2 - 1 - |W_1|^2 - \left(\sum_{i=2}^{j} |W_i| \right)^2 \\
&\overset{(4.25)}{=} n^2 - 1 - (|B| + d)^2 - (|A| - d)^2 \\
&= n^2 - 1 - |A|^2 - |B|^2 + 2d(|A| - |B| - d) \\
&= \mathrm{sep}(v) + 2d(|A| - |B| - d).
\end{aligned}$$

Due to Lemma 4.25 (i) we have $\mathrm{sep}^s(w) \le \mathrm{sep}(w)$, yielding

$$2d(|A| - |B| - d) \le \mathrm{sep}^s(w) - \mathrm{sep}(v) \le \mathrm{sep}(w) - \mathrm{sep}(v) < 0, \tag{4.26}$$

where the last inequality holds, because v is the only max-sep vertex in G. Because $d > 0$, (4.26) implies

$$|B| > |A| - d = \sum_{i=2}^{j} |W_i| = n - 1 - |W_1|. \tag{4.27}$$

Finally, because $a_2 \in W_1$, with Proposition 4.6 (i) we get

$$\mathrm{rel}_w^s(a_2) = n - |W_1| \overset{(4.27)}{<} |B| + 1 = n - |A| = \mathrm{rel}_v(a_2).$$

Thus, the proof of (4.24) is complete.

From (4.24) it follows that $a_2 \in \mathrm{MS}(G^s)$, because otherwise

$$\mathcal{C}(G^s, a_2) = \frac{1}{|\mathrm{MS}(G^s)|} \sum_{w \in \mathrm{MS}(G^s)} \mathrm{rel}_w^s(a_2) \overset{(4.24)}{<} \mathrm{rel}_v(a_2) = \mathcal{C}(G, a_2)$$

and the swap s would be profitable, contradicting that G is an SE. By Lemma 4.10 we have $\mathrm{sep}^s(a_2) = \mathrm{sep}(a_2)$. Let P_A be a connecting path of C_A and v. Then, (P_A, u) is a connecting path of C_A and u with $P_A \cap B = \{u\}$ and with Lemma 4.25 (iii), for every $w \in B$ we have $\mathrm{sep}^s(w) = \mathrm{sep}(w)$. Hence,

$$\mathrm{sep}(a_2) = \mathrm{sep}^s(a_2) \geq \mathrm{sep}^s(w) = \mathrm{sep}(w) \quad \text{for every } w \in B. \tag{4.28}$$

Observe that a_k also is a cycle neighbor of a_1, so all arguments also apply to a_k instead of a_2 and we get

$$\mathrm{sep}(a_k) \geq \mathrm{sep}(w) \quad \text{for every } w \in B. \tag{4.29}$$

But there is still more useful symmetry: By our assumption, $B + v$ contains a cycle, hence A and B fulfill exactly the same conditions. interchanging A with B, C_A with C_B, a_2 with b_2 and a_k with b_ℓ we get that

$$\mathrm{sep}(b_2) \geq \mathrm{sep}(w) \quad \text{and} \quad \mathrm{sep}(b_\ell) \geq \mathrm{sep}(w) \quad \text{for every } w \in A. \tag{4.30}$$

Let $M := \{a_2, a_k, b_2, b_\ell\}$. By combining the results (4.28),(4.29) and (4.30), using $a_2, a_k \in A$ and $b_2, b_\ell \in B$ we get

$$\mathrm{sep}(x) = \mathrm{sep}(x') \geq \mathrm{sep}(w) \quad \text{for all } x, x' \in M \text{ and all } w \in A \cup B. \tag{4.31}$$

Now w.l.o.g. let $|A| \leq |B|$, because otherwise they could be interchanged. We turn back to the swap $s = (a_1, a_2, u)$. We prove that $M \subseteq \mathrm{MS}(G^s)$ by showing that $\mathrm{sep}^s(x) \geq \mathrm{sep}^s(w)$ for all $x \in M$ and $w \in V$. So let $x \in M$ and $w \in V$. If $w = v$, because $|\mathcal{F}^s(v)| = 1$, by Remark 4.7 we have $\mathrm{sep}^s(w) = \mathrm{sep}^s(v) = 2(n-1) \leq \mathrm{sep}^s x$. Thus, we may assume $w \in V \setminus \{v\} = A \cup B$. We already showed that $P_A \cap B = \emptyset$. Because $a_2, a_k \in C_k \setminus \{a_1\}$, we get $M \cap P_A = \emptyset$, so by Lemma 4.25 (iii), $\mathrm{sep}^s(x) = \mathrm{sep}(x)$. Moreover, by Lemma 4.25 (i), $\mathrm{sep}^s(w) \leq \mathrm{sep}(w)$, hence

$$\mathrm{sep}^s(x) = \mathrm{sep}(x) \overset{(4.31)}{\geq} \mathrm{sep}(w) \geq \mathrm{sep}^s(w)$$

and we proved that $M \subseteq \mathrm{MS}(G^s)$.

Our aim still is to show that the swap s is profitable. To this end, we will prove that

$$\mathrm{rel}^s_{a_k}(a_2) + \mathrm{rel}^s_{b_2}(a_2) + \mathrm{rel}^s_{b_\ell}(a_2) \leq n - 1. \tag{4.32}$$

We want to apply Lemma 4.11 to the graph G^s with $v = a_2$ and $w_1 = a_k, w_2 = b_2, w_3 = b_\ell$ and hence need to find suitable paths. We distinguish three cases:

Case 1: $u \notin \{b_2, b_\ell\}$. Recall that b_1 is a connecting vertex of C_B and v and let P be a corresponding b_1-v-path. By definition, $P \cap C_B = \{b_1\}$. Moreover, $P \subseteq B \cup \{v\}$, so $P \cap M = \emptyset$. The same holds for the reverse path $\bar{P}$. Let

$$Q := \begin{cases} (u, Q_2) & \text{if } \bar{P} = (Q_1, u, Q_2) \text{ for paths } Q_1, Q_2 \\ (u, \bar{P}) & \text{if } u \notin \bar{P}. \end{cases}$$

Note that Q is a u-b_1-path with $Q \cap M = \emptyset$, because $P \cap M = \emptyset, u \in B$ and by assumption, $w \neq b_2, b_\ell$, so $w \notin M$. Let $P_1 := (a_2, a_3, \ldots, a_k), P_2 := (a_2, Q, b_2)$ and $P_3 := (a_2, Q, b_\ell)$. P_1 is a a_2-a_k-path in G^s with $b_2, b_\ell \notin P_1$. P_2 is a a_2-b_2-path in G^s with $a_k, b_\ell \notin P_2$ and P_3 is a a_2-b_ℓ-path in G^s with $a_k, b_2 \notin P_3$. Hence we can apply Lemma 4.11 and obtain (4.32).

Case 2: $u = b_2$. Let $P_1 := (a_2, a_3, \ldots, a_k)$, $P_2 := (a_2, b_2)$ and $P_3 := (a_2, b_2, b_1, b_\ell)$. Again, P_1 is a a_2-a_k-path in G^s with $b_2, b_\ell \notin P_1$ and P_2 is a a_2-b_2-path in G^s with $a_k, b_\ell \notin P_2$. Moreover, P_3 is a a_2-b_ℓ-path in G^s with $a_k \notin P_3$.

In order to apply Lemma 4.11, we still need to prove the existence of a a_2-b_ℓ-path P_4 with $b_2 \notin P_4$. Let P_A be a connecting path of C_A and v and let P_B be a connecting path of C_B and v. Denote its reverse path by $\bar{P}_B$. Then, P_A is a a_1-v-path with $P_A \cap M = \emptyset$ and $\bar{P}_B$ is a v-b_1-path with $P_B \cap M = \emptyset$ and $P_A \cap P_B = \{v\}$. Thus, $P_4 := (a_2, a_3, \ldots, a_k, a_1, P_A, P_B, b_1, b_\ell)$ is a a_2-b_ℓ-path with $b_2 \notin P_4$. We apply Lemma 4.11 as above and obtain (4.32).

Case 3: $u = b_\ell$. This case is symmetric to Case 2. Thus, we can apply Lemma 4.11 to the graph G^s with $v = a_2$ and $w_1 = a_k, w_2 = b_2, w_3 = b_\ell$ and the paths (a_2, a_k), (a_2, Q, b_2) and (a_2, Q, b_ℓ) and get

$$\mathrm{rel}^s_{a_k}(a_2) + \mathrm{rel}^s_{b_2}(a_2) + \mathrm{rel}^s_{b_\ell}(a_2) \leq n - 1.$$

Thus, the proof of (4.32) is complete. Since $|A| \leq n/2$, (4.32) yields

$$\sum_{w \in M} \mathrm{rel}^s_w(a_2) \leq \mathrm{rel}^s_{a_2}(a_2) + n - 1 = 2(n-1) < 4(n - |A|) = 4 \cdot \mathrm{rel}_v(a_2). \tag{4.33}$$

Recalling (4.24), we also have

$$\mathrm{rel}^s_w(a_2) \leq \mathrm{rel}_v(a_2) \quad \text{for every } w \in V \setminus \{a_2\}, \tag{4.34}$$

so finally

$$\begin{aligned}
\mathcal{C}(G^s, a_2) &= \frac{1}{|\mathrm{MS}(G^s)|} \sum_{w \in \mathrm{MS}(G^s)} \mathrm{rel}_w^s(a_2) \\
&= \frac{1}{|\mathrm{MS}(G^s)|} \left(\sum_{w \in M} \mathrm{rel}_w^s(a_2) + \sum_{w \in \mathrm{MS}(G^s) \setminus M} \mathrm{rel}_w^s(a_2) \right) \\
&\overset{(4.34)}{\leq} \frac{1}{|\mathrm{MS}(G^s)|} \left(\sum_{w \in M} \mathrm{rel}_w^s(a_2) + (|\mathrm{MS}(G^s)| - 4)\mathrm{rel}_v(a_2) \right) \\
&\overset{(4.33)}{<} \frac{1}{|\mathrm{MS}(G^s)|} \left(4 \cdot \mathrm{rel}_v(a_2) + (|\mathrm{MS}(G^s)| - 4)\mathrm{rel}_v(a_2) \right) \\
&= \mathrm{rel}_v(a_2) = \mathcal{C}(G, a_2).
\end{aligned}$$

Thus, the swap s is profitable, in contradiction to G being an SE.

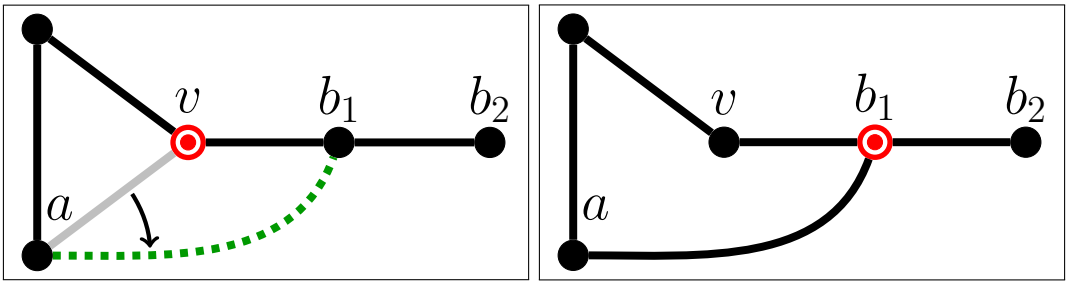

Figure 4.11: The graph G in Theorem 4.23 (ii) is no SE: The swap $t = (a, v, b_1)$ is profitable.

(ii). Due to (i) we know that $B+v$ is cycle-free. For $|B| \geq 3$ we can apply Lemma 4.26 and are done. So let $|B| \leq 2$ and assume that $|A| \leq |B| \leq 2$. Because $A + v$ contains a cycle, $|A| \geq 2$, so we get $|A| = |B| = 2$. Thus, the graph G is completely determined: $B + v$ is a path of the form (v, b_1, b_2) and $A + v$ is a triangle (see Figure 4.11). But then G is no SE because for $a \in A$ the swap $t = (a, v, b_1)$ is profitable, a contradiction. □

In the next theorem we will use Theorem 4.23 to show that an SE Graph G with exactly one max-sep vertex can't contain a cycle. For this we will need the following lemma.

Lemma 4.28. *Let $G = (V, E), v \in V$ and $A \in \mathcal{F}(v)$. If A doesn't contain any leaf of G, then $A + v$ contains a cycle C and $c_1, c_2 \in C$ with the following properties:*

(i) c_1 is a connecting vertex of C and v.

(ii) c_2 is a cycle neighbor of c_1 with $\mathrm{sep}(c_2) = 2(n-1)$.

Proof. We prove the claim via induction over A. For $|A| = 1$, $A = \{a\}$ for some leaf a, so there is nothing to show.

Now let $|A| > 1$ and suppose that A doesn't contain any leaf of G. Consequently, $A + v$ contains a cycle C'. Let c'_1 be a connecting vertex of C' and v and let c'_2 be a cycle neighbor of c'_1. If $\text{sep}(c'_2) = 2(n-1)$, we are done, so let $\text{sep}(c'_2) > 2(n-1)$. By Remark 4.7 it follows that $|\mathcal{F}(c'_2)| \geq 2$, so there exists a c'_2-flap B with $v \notin B$. Applying Lemma 4.13 (ii), we get $B \subset A$. Hence, $|B| < |A|$ and B doesn't contain a leaf of G. By applying the induction hypothesis to c'_2 and B we get that $B + c_2$ contains a cycle C and $c_1, c_2 \in C$ such that c_1 is connecting vertex of C and c'_2 with corresponding c_1-c'_2-path P_1 and c_2 is a cycle neighbor of c_1 with $\text{sep}(c_2) = 2(n-1)$.

It remains to show that c_1 is a connecting vertex of C and v, so we need to prove the existence of a c_1-v-path Q with $Q \cap C = \{c_1\}$. Because $C \setminus \{c_1\}$ and v lie in different c'_2-flaps, there exists a c_2-v-path P_2 with $P_2 \cap C \subseteq \{c_1\}$ and $P_2 \cap P_1 = \{c'_2\}$. Moreover, because P_1 is a connecting path of C and c'_2, $P \cap C = \{c_1\}$. Thus, the path (P_1, P_2) is a connecting path of C and v, and we are done. □

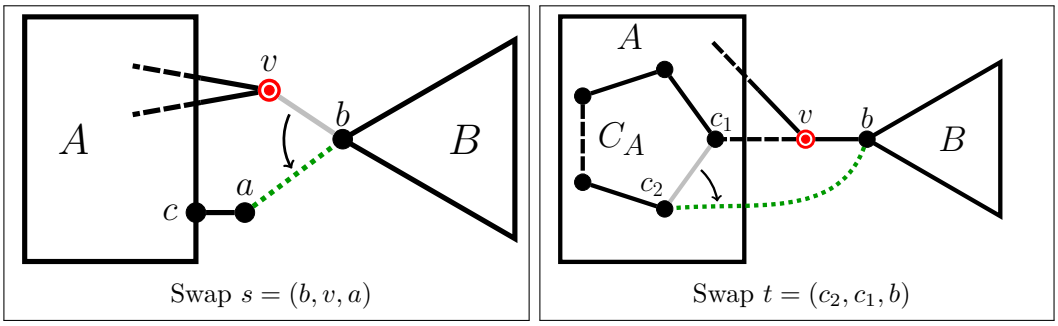

Figure 4.12: Swaps s and t in the proof of Theorem 4.29.

Theorem 4.29. *Every SE graph G with exactly one max-sep vertex is a tree.*

Proof. Assume that there exists an SE graph $G = (V, E)$ with exactly one max-sep vertex v and at least one cycle. Due to Theorem 4.27, $\mathcal{F}(v) = \{A, B\}$, where $A + v$ contains a cycle, $B + v$ is cycle-free and $|A| > |B|$. As $B + v$ is cycle-free, there exists a unique neighbor b of v in B. We prove the following auxiliary claim:

$$A \text{ doesn't contain any leaf of } G. \tag{4.35}$$

Assume that there exists $a \in A$ such that a is a leaf in G. We show that the swap $s = (b, v, a)$ is profitable (see Figure 4.12). Due to Lemma 4.10, $\text{sep}^s(b) = \text{sep}(b)$. Let c be the father of a in G. We have $\mathcal{F}^s(a) = \{(A \setminus \{a\}) \cup \{v\}, B\}$, so by Proposition 4.6 (ii),

$$\text{sep}^s(a) = n^2 - 1 - |A|^2 - |B|^2 = \text{sep}(v) > \text{sep}(b) = \text{sep}^s(b). \tag{4.36}$$

Note that $B \cup \{a\} \in \mathcal{F}^s(c)$. Denote all other c-flaps of G^s by $C_1, \dots, C_k$. Then, $\mathcal{F}^s(c) = \{B \cup \{a\}, C_1, \dots, C_k\}$ and $\sum_{i=1}^k |C_i| = n - |B| - 2 = |A| - 1$. By Proposition 4.6 (ii),

$$\begin{aligned}
\operatorname{sep}^s(c) &= n^2 - 1 - (|B|+1)^2 - \sum_{i=1}^k |C_i|^2 \\
&\geq n^2 - 1 - (|B|+1)^2 - \left(\sum_{i=1}^k |C_i|\right)^2 \\
&= n^2 - 1 - (|B|+1)^2 - (|A|-1)^2 \\
&= n^2 - 1 - |A|^2 - |B|^2 + 2(|A| - |B| - 1) \\
&= \operatorname{sep}^s(a) + 2(|A| - |B| - 1).
\end{aligned}$$

Since $|A| \geq |B| + 1$, this implies

$$\operatorname{sep}^s(c) \geq \operatorname{sep}^s(a) \overset{(4.36)}{>} \operatorname{sep}^s(b). \tag{4.37}$$

At this point, we don't know whether $a \in \mathrm{MS}(G^s)$, but we know that $b \notin \mathrm{MS}(G^s)$ and $\mathrm{MS}(G^s) \setminus \{a\} \neq \emptyset$, since c has at least the same separation in G^s as a. Note that with Proposition 4.6 (i),

$$\operatorname{rel}_a^s(b) = n - |B| = \operatorname{rel}_v(b). \tag{4.38}$$

Next we show that

$$\operatorname{rel}_w^s(b) < \operatorname{rel}_v(b) \quad \text{for all } w \in \mathrm{MS}(G^s) \setminus \{a\}. \tag{4.39}$$

So let $w \in \mathrm{MS}(G^s) \setminus \{a\}$. Then either $w \in (A \setminus \{a\}) \cup \{v\}$ or $w \in B$. Let $D \in \mathcal{F}(w)$ with $a \in D$.

If $w \in (A \setminus \{a\}) \cup \{v\}$, then $w \notin B$, so by Lemma 4.13 (ii), $B \subset D$ and with Proposition 4.6 (i) we get

$$\operatorname{rel}_w^s(b) = n - |D| < n - |B| = \operatorname{rel}_v(b).$$

On the other hand, if $w \in B$, then $w \notin (A \setminus \{a\}) \cup \{v\}$. By Lemma 4.13 (ii), $(A \setminus \{a\}) \cup \{v\} \subset D$, implying $|D| > |A| > |B|$. With Proposition 4.6 (i) we get

$$\operatorname{rel}_w^s(b) = n - |D| < n - |B| = \operatorname{rel}_v(b).$$

Finally, we show that the swap s is profitable and thereby complete the proof of (4.35).

The profit of s is

$$\begin{aligned}\mathcal{C}(G,b) - \mathcal{C}(G^s,b) &= \mathrm{rel}_v(b) - \frac{1}{|\mathrm{MS}(G^s)|}\sum_{w\in\mathrm{MS}(G^s)} \mathrm{rel}_w^s(b)\\ &= \frac{1}{|\mathrm{MS}(G^s)|}\left(\sum_{w\in\mathrm{MS}(G^s)} \mathrm{rel}_v(b) - \mathrm{rel}_w^s(b)\right)\\ &\overset{(4.38)}{=} \frac{1}{|\mathrm{MS}(G^s)|}\left(\sum_{w\in\mathrm{MS}(G^s)\setminus\{a\}} \mathrm{rel}_v(b) - \mathrm{rel}_w^s(b)\right)\\ &\overset{(4.39)}{>} 0.\end{aligned}$$

Having established (4.35), according to Lemma 4.28 there exists a cycle C_A in $A + v$ with connecting vertex c_1 to v and a cycle-neighbor c_2 of c_1 with $\mathrm{sep}(c_2) = 2(n-1)$.

Clearly, $\{c_2, b\} \notin E$, so we may consider the swap $t = (c_2, c_1, b)$ (see Figure 4.12). We aim to complete the proof of the theorem by showing that the swap t is profitable.

We start by showing that for every $w \in V \setminus \{c_2\}$ it holds

$$\mathrm{rel}_w^t(c_2) < \mathrm{rel}_v(c_2). \tag{4.40}$$

The proof of (4.40) works analogously to the proof of (4.24) in Theorem 4.27: We start by considering the case $w \in B$. Let $D \in \mathcal{F}^t(w)$ with $c_2 \in D$. Because $w \notin A \cup \{v\}$ and the swap t deletes a cycle edge from C_A, all vertices in $A \cup \{v\}$ are connected in $G^t - w$, hence $A \cup \{v\} \subseteq D$. This implies $|A| < |D|$. By Proposition 4.6 (i),

$$\mathrm{rel}_w^t(c_2) = n - |D| < n - |A| = \mathrm{rel}_v(c_2).$$

For the case $w = v$, note that $G^t - v$ is still connected, so

$$\mathrm{rel}_v^t(c_2) = n - |G^t - v| = 1 < n - |A| = \mathrm{rel}_v(c_2).$$

Finally, let $w \in A \setminus \{c_2\}$. Let $\mathcal{F}^t(w) = \{W_1, \ldots, W_j\}$ with $b \in W_1$. Obviously, also $v \in W_1$ and $c_2 \in W_1$. For every $2 \le i \le j$, by Lemma 4.13 (ii), as $v \notin W_i$ we have $W_i \subset A$. This implies $\bigcup_{i=2}^{j} W_i \subseteq A \setminus \{w\}$. Hence, $d := |A| - \sum_{i=2}^{j} |W_i| > 0$. Note that

$$|W_1| = n - 1 - \sum_{i=2}^{j} |W_i| = |A| + |B| - \sum_{i=2}^{j} |W_i| = |B| + d, \tag{4.41}$$

so by Proposition 4.6 (ii) we have

$$\begin{aligned}\operatorname{sep}^t(w) &= n^2 - 1 - |W_1|^2 - \sum_{i=2}^{j} |W_i|^2 \\ &\geq n^2 - 1 - |W_1|^2 - \left(\sum_{i=2}^{j} |W_i|\right)^2 \\ &\overset{(4.41)}{=} n^2 - 1 - (|B| + d)^2 - (|A| - d)^2 \\ &= n^2 - 1 - |A|^2 - |B|^2 + 2d(|A| - |B| - d) \\ &= \operatorname{sep}(v) + 2d(|A| - |B| - d).\end{aligned}$$

Due to Lemma 4.25 (i) we have $\operatorname{sep}(w) \leq \operatorname{sep}^t(w)$, yielding

$$2d(|A| - |B| - d) \leq \operatorname{sep}^t(w) - \operatorname{sep}(v) \leq \operatorname{sep}(w) - \operatorname{sep}(v) < 0, \tag{4.42}$$

where the last inequality holds, because v is the only max-sep vertex in G. Because $d > 0$, (4.42) implies

$$|B| > |A| - d = \sum_{i=2}^{j} |W_i| = n - 1 - |W_1|. \tag{4.43}$$

Finally, because $c_2 \in W_1$, with Proposition 4.6 (i) we get

$$\operatorname{rel}_w^t(c_2) = n - |W_1| \overset{(4.43)}{<} |B| + 1 = n - |A| = \operatorname{rel}_v(c_2).$$

Thus, the proof of (4.40) is complete.

According to Lemma 4.10, $\operatorname{sep}^t(c_2) = \operatorname{sep}(c_2) = 2(n-1)$. We consider two possible cases.

Case 1: There exists $x \in V$ with $\operatorname{sep}^t(x) > 2(n-1)$. This implies $c_2 \notin \operatorname{MS}(G^t)$ and hence

$$\mathcal{C}(G^t, c_2) = \frac{1}{\operatorname{MS}(G^t)} \sum_{w \in \operatorname{MS}(G^t)} \operatorname{rel}_w^t(c_2) \overset{(4.40)}{<} \operatorname{rel}_v(c_2) = \mathcal{C}(G, c_2).$$

Case 2: $\operatorname{sep}^t(x) = 2(n-1)$ for all $x \in V$. In this case, $\operatorname{MS}(G^t) = V$. Due to Remark 4.7, for all $x \in V$ we have $|\mathcal{F}^t(x)| = 1$. Hence, for all $w \neq c_2$ it holds $\operatorname{rel}_w^t(c_2) = 1$ and we get

$$\mathcal{C}(G^t, c_2) = \frac{1}{n} \sum_{w \in V} \operatorname{rel}_w^t(c_2) = \frac{2(n-1)}{n} < 2.$$

But

$$\mathcal{C}(G, c_2) = \operatorname{rel}_v(c_2) = n - |A| = |V \setminus A| \geq |\{v, b\}| = 2,$$

so $\mathcal{C}(G^t, c_2) < \mathcal{C}(G, c_2)$, hence the swap t is profitable and the proof of the theorem is complete. □

Proof of Theorem 4.21. Let $G = (V, E)$ be an SE graph with exactly one max-sep vertex v. According to Theorem 4.29, G is a tree. By Theorem 4.23 we have $|\mathcal{F}(v)| = 2$, hence $\deg(v) = 2$. Let A and B be the v-flaps of G We show that $|A| \leq |B|$.

Assume for a moment that $|A| > |B|$. Let a be the neighbor of v in A and let $\mathcal{F}(a) = \{B \cup \{v\}, A_1, \ldots, A_k\}$. We have $\sum_{i=1}^{k} |A_i| = |A| - 1$, so by Proposition 4.6 (ii) we get

$$\begin{aligned}
\operatorname{sep}(a) &= n - 1 - (|B| + 1)^2 - \sum_{i=1}^{k} |A_i|^2 \\
&\geq n - 1 - (|B| + 1)^2 - \left(\sum_{i=1}^{k} |A_i| \right)^2 \\
&= n - 1 - (|B| + 1)^2 - (|A| - 1)^2 \\
&= n - 1 - |B|^2 - |A|^2 + 2(|A| - |B| - 1) \\
&\overset{|A|>|B|}{\geq} n - 1 - |B|^2 - |A|^2 = \operatorname{sep}(v).
\end{aligned}$$

This is a contradiction to $\mathrm{MS}(G) = \{v\}$, so $|A| \leq |B|$. For symmetry reasons, we also have $|B| \leq |A|$, thus $|A| = |B|$. Because G is a tree, $B + v$ is cycle-free, so Lemma 4.26 implies $|B| \leq 2$. There are only two possible cases left: If $|A| = |B| = 1$, then G is a path of length 2. If $|A| = |B| = 2$, because $\deg(v) = 2$, G is a path of length 4.

□

4.6 Open questions

We gave a characterization of SE graphs with one max-sep vertex and trees in the extreme vertex destruction model. An interesting open question is to find structural criteria for SE graphs in this model that hold for general graphs with multiple max-sep vertices.

Moreover, one could consider different destruction models, like the uniform destroyer and compare the structure of SE from different models.

Bibliography

[1] N. Alon, D. Demaine, M. T. Hajiaghayi, and T. Leighton. Basic Network Creation Games. *SIAM Journal on Discrete Mathematics*, pages 656–668, 2013. Conference version at SPAA 2010.

[2] N. Alon, E. Demaine, M. Hajiaghayi, and T. Leighton. Basic Network Creation Games. In *SPAA*, pages 106–113. ACM, 2010.

[3] C. Àlvarez and A. Messegué. Network Creation Games: Structure vs Anarchy, 2017. https://arxiv.org/abs/1706.09132.

[4] R. C. Baker, G. Harman, and J. Pintz. The Difference between Consecutive Primes ii. *London Math. Soc*, pages 83–532, 2001.

[5] József Balogh and Wojciech Samotij. On the Chvátal-Erdős Triangle Game. *Electr. J. Comb.*, 18(1), 2011.

[6] József Beck. Van der Waerden and Ramsey Type Games. *Combinatorica*, 1(2):103–116, Jun 1981.

[7] József Beck. Remarks on Positional Games. I. *Acta Math. Acad. Sci. Hungar.*, 40:65–71, 1982.

[8] József Beck. Random Graphs and Positional Games on the Complete Graph. In Michal Karo'nski and Andrzej Ruciński, editors, *Random Graphs '83*, volume 118 of *North-Holland Mathematics Studies*, pages 7 – 13. North-Holland, 1985.

[9] Małgorzata Bednarska and Tomasz Łuczak. Biased Positional Games for Which Random Strategies are Nearly Optimal. *Combinatorica*, 20(4):477–488, 2000.

[10] C. E. Bonferroni. Teoria Statistica delle Classi e Calcolo delle Probabilità. *Pubblicazioni del R Istituto Superiore di Scienze Economiche e Commerciali di Firenze*, 8:3–62, 1936.

[11] A. Chauhan, P. Lenzner, A.Melnichenko, and M. Münn. On Selfish Creation of Robust Networks. In *Proceedings of the 9th Annual ACM-SIAM Symposium on Algorithmic Game Theory, Liverpool, UK, September 2016 (SAGT 2016)*, Lecture Notes in Computer Science, 2016.

[12] V. Chvátal and P. Erdős. Biased Positional Games. *Annals of Discrete Math.*, 2:221–228, 1978.

[13] Benjamin Doerr, Reto Spöhel, Henning Thomas, and Carola Winzen. Playing Mastermind with Many Colors. *CoRR*, abs/1207.0773, 2012.

[14] M. El Ouali, C. Glazik, V. Sauerland, and A. Srivastav. On the Query Complexity of Black-Peg AB-Mastermind. *Games*, 9(1):2, 2018.

[15] A. Fabrikant, A. Luthra, E. Maneva, C. Papadimitriou, and S. Shenker. On a Network Creation Game. In *PODC*, pages 347–351. ACM, 2003.

[16] C. Glazik, G. Jäger, J. Schiemann, and A. Srivastav. Bounds for Static Black-Peg AB Mastermind. In *Proceedings of 11th Annual International Conference on Combinatorial Optimization and Applications (COCOA 2017)*, 2017.

[17] C. Glazik, L. Kliemann, J. Schiemann, and A. Srivastav. On Swap Equilibrium Graphs in the Extreme Vertex Destruction Model, 2018. previously unpublished.

[18] C. Glazik and A. Srivastav. A new Bound for the Maker-Breaker Triangle Game, 2018. https://arxiv.org/abs/1812.01382.

[19] D. Hefetz, M. Krivelevich, M. Stojacović, and T. Szabó. *Positional Games*. 2014.

[20] M.O. Jackson and A. Wolinsky. A Strategic Model of Social and Economic Networks. *Journal of Economic Theory*, 71(1):44–74, 1996.

[21] Gerold Jäger and Marcin Peczarski. The Number of Pessimistic Guesses in Generalized Mastermind. *Inf. Process. Lett.*, 109(12):635–641, 2009.

[22] B. Kawald and P. Lenzner. On Dynamics in Selfish Network Creation. In *Proceedings of the 25th ACM Symposium on Parallel Algorithms and Architectures, Montreal, Canada, July 2013 (SPAA 2013)*, 2013.

[23] L. Kliemann, E. Sheykhdarabadi, and A. Srivastav. Swap Equilibria under Link and Vertex Destruction. *Games*, 8(1):14, 2017.

[24] Lasse Kliemann. Brief Announcement: The Price of Anarchy for Distributed Network Formation in an Adversary Model. In Andréa W. Richa and Rachid Guerraoui, editors, *Proceedings of the 29th Annual ACM Symposium on Principles of Distributed Computing, PODC 2010, Zurich, Switzerland, July 25-28, 2010*, pages 229–230. ACM, 2010.

[25] Lasse Kliemann. The Price of Anarchy for Network Formation in an Adversary Model. *Games*, 2(3):302–332, 2011.

[26] Lasse Kliemann. Price of Anarchy in the Link Destruction (Adversary) Model. In Marco E. Lübbecke, Arie Koster, Peter Letmathe, Reinhard Madlener, Britta Peis,

and Grit Walther, editors, *Operations Research Proceedings 2014, Selected Papers of the Annual International Conference of the German Operations Research Society (GOR), RWTH Aachen University, Germany, September 2-5, 2014*, pages 285–291. Springer, 2014.

[27] Lasse Kliemann. The Price of Anarchy in Bilateral Network Formation in an Adversary Model. *Algorithmica*, 77(3):921–941, 2017.

[28] D. Knuth. The Computer as Master Mind. *Journal of Recreational Mathematics*, 9(1), 1976.

[29] K. Koyama and T. Lai. An Optimal Mastermind Strategy. *Journal of Recreational Mathematics*, 25:251–256, 1993.

[30] Michael Krivelevich. Positional Games. *Proceedings of the International Congress of Mathematicians(ICM 2014)*, 4:355 – 379, 2014.

[31] C. Kusch, J. Ru'e, C. Spiegel, and T. Szab'o. Random Strategies are Nearly Optimal for Generalized van der Waerden Games. *Electronic Notes in Discrete Mathematics*, 61:789 – 795, 2017. The European Conference on Combinatorics, Graph Theory and Applications (EUROCOMB'17).

[32] J. Riordan. *Introduction to Combinatorial Analysis*. Dover Books on Mathematics, Dover Publications, 2002.

[33] A. Schrijver. *Combinatorial Optimization: Polyhedra and Efficiency, v. 1.* Algorithms and Combinatorics, Springer, 2003.

[34] Jeff Stuckman and Guo-Qiang Zhang. Mastermind is NP-Complete. *CoRR*, abs/cs/0512049, 2005.

Erklärung

Hiermit erkläre ich,

- dass die Abhandlung - abgesehen von der Beratung durch den Betreuer - nach Inhalt und Form die eigene Arbeit ist,
- dass die Arbeit weder ganz noch zum Teil schon einer anderen Stelle im Rahmen eines Prüfungsverfahrens vorgelegen hat, veröffentlicht worden ist oder zur Veröffentlichung eingereicht wurde,
- dass die Arbeit unter Einhaltung der Regeln guter wissenschaftlicher Praxis der Deutschen Forschungsgemeinschaft entstanden ist,
- dass mir kein akademischer Grad entzogen wurde.

Christian Glazik
Kiel, 2019