

Chapter 3

Evasiveness of Graph Properties

In many real-world situations we are forced to draw conclusions based only on partial information. For example, when we buy a used car it is infeasible to check every single part of the car. Yet an experienced person is able to almost guarantee the reliability of a car after only a certain relatively small number of checks.

In this chapter we investigate graph properties and whether it is possible to decide whether a given graph has a certain property based only on partial information about the graph. The exposition is to some extent based on [Aig88], [Bol04], [Schy06], and [KSS84].

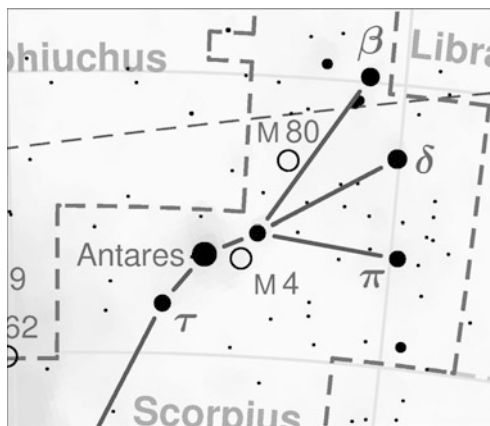


Fig. 3.1 A part of the Scorpius star constellation [Bro03]

3.1 Graph Properties and Their Complexity

In this chapter we consider graphs on a fixed set of n vertices, say $V = \{1, \dots, n\}$. A simple graph $G = (V, E)$ is then determined by its edge set $E \subseteq \binom{V}{2}$, which allows us to identify G with E .

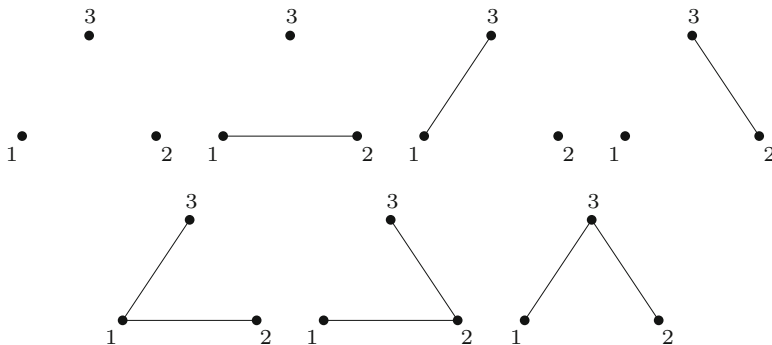


Fig. 3.2 The graphs on the vertex set $V = \{1, 2, 3\}$ with at most two edges

Graph Properties

We are interested in graph properties such as planarity, connectedness, and acyclicity. Graph properties are by definition required to be isomorphism invariant. In other words, if \mathcal{P} is a property of graphs on the vertex set V , then a graph $G = (V, E)$ has property \mathcal{P} if and only if any isomorphic copy $G' = (V, E')$ has property \mathcal{P} .

Since we consider graphs on a fixed vertex set V , each graph $G = (V, E)$ that we consider is determined by its edge set E . Hence, a property \mathcal{P} of graphs on the vertex set V can be identified with the family of edge sets of graphs satisfying the property.

Definition 3.1. Let V be a fixed set of $n \geq 1$ vertices. A *graph property* \mathcal{P} is a family of subsets of $\binom{V}{2}$ such that for any two isomorphic graphs $(V, E) \cong (V, E')$, either $E, E' \in \mathcal{P}$ or $E, E' \notin \mathcal{P}$.

As a first example, assume $n = 3$ and consider the property $\mathcal{P}_{3,2}$ of having at most two edges. Then

$$\mathcal{P}_{3,2} = \{\emptyset, \{12\}, \{13\}, \{23\}, \{12, 13\}, \{12, 23\}, \{13, 23\}\},$$

where we used the standard abbreviation uv for the edge $\{u, v\}$; cf. Fig. 3.2.

Hide and Seek

We consider a game for two players, let's call them Bob and Alice. They fix a vertex set V and a graph property \mathcal{P} of graphs with vertex set V . The idea of the game is roughly that Bob imagines a graph and Alice wants to find out whether Bob's graph has property \mathcal{P} .

From the viewpoint of Alice, Bob may have a fixed graph in mind. But Bob can change which graph he is imagining after each of Alice's questions, as long as it is consistent with the information he has already given.

A game takes place as follows. Alice asks questions of the type, “Is e an edge of the graph?” for potential edges $e \in \binom{V}{2}$, and Bob answers in each case with *yes* or *no*, thereby revealing information about the graph’s edges and nonedges. So in each stage of the game Alice has partial information about Bob’s graph: according to his answers, she knows about some edges that are in the graph and some that are not. Let’s call these sets of edges Y and N . She wants to decide as quickly as possible whether Bob’s graph has property \mathcal{P} . But what does that mean? Let’s call any graph $G = (V, E)$ on the vertex set V a *completion of the partial graph defined by (Y, N)* if $Y \subseteq E$ and $E \cap N = \emptyset$. So the graph that Bob has in mind is such a completion. Alice wants to decide as quickly as possible whether every such completion of the partial graph defined by (Y, N) has property \mathcal{P} or whether every completion of the partial graph does not have property \mathcal{P} . Bob, on the other hand, wants Alice to ask as many questions as possible.

For the graph property $\mathcal{P}_{3,2}$ given above, Alice might ask as follows: “Is 12 an edge of the graph?” If Bob’s answer is *no*, any completion of the graph has at most two edges, and Alice can answer, “The graph has property $\mathcal{P}_{3,2}$!” If the answer is *yes*, she must keep asking. Possibly, “Is 13 an edge of the graph?” If the answer is *no*, Alice is done; if it is *yes*, she indeed has to ask the third question, “Is 23 an edge of the graph?” We see that if Bob always answers the first two questions with *yes*, then Alice cannot do better than to ask all $\binom{3}{2} = 3$ potential questions.

As noted above, Bob does not necessarily have to have a fixed graph in mind. He may decide after each of Alice’s question which answer suits his goal best. But from Alice’s viewpoint, Bob may already have a certain fixed graph in mind. We can therefore also say that Alice wants to decide with certainty, and as quickly as possible, whether this *hypothetical graph* has property \mathcal{P} . At a particular stage of the game, this hypothetical graph may be just any completion of the partial graph that Alice has knowledge about so far.

Strategies

A *strategy ϕ of the seeker Alice* is an algorithm that, depending on Bob’s answers at each stage of the game, either assigns an edge that Alice uses for her next question or if possible gives one of the following answers: “The graph has property \mathcal{P} !” or “The graph does not have property \mathcal{P} !”

Alice’s strategy discussed in our previous example is shown schematically in Fig. 3.3. For obvious reasons, such an algorithm is called a *decision-tree algorithm*.

A *strategy ψ of the hider Bob* is given by a map that assigns to each triple (Y, N, e) one of the answers *yes* or *no*, where $Y, N \subseteq \binom{V}{2}$ are disjoint edge sets and $e \in \binom{V}{2} \setminus (Y \cup N)$ is an edge in the complement. The sets Y and N represent the sets of edges that Bob previously has answered with *yes*, respectively *no*, and e is the edge about which Alice is currently asking. The pairs (Y, N) are called the *stages of the game*, and their evolution completely describes the course of the game.

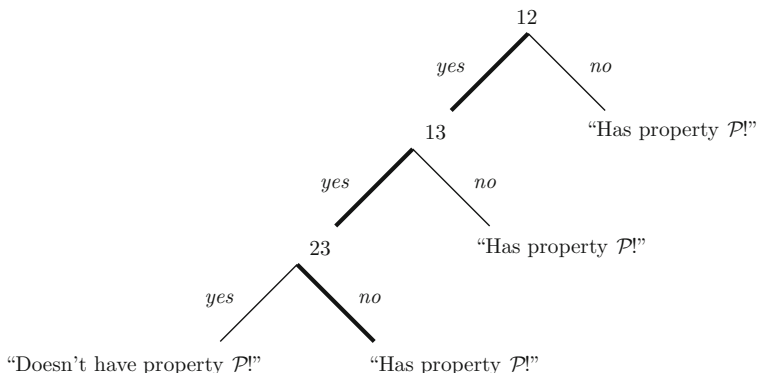


Fig. 3.3 The strategy of the seeker

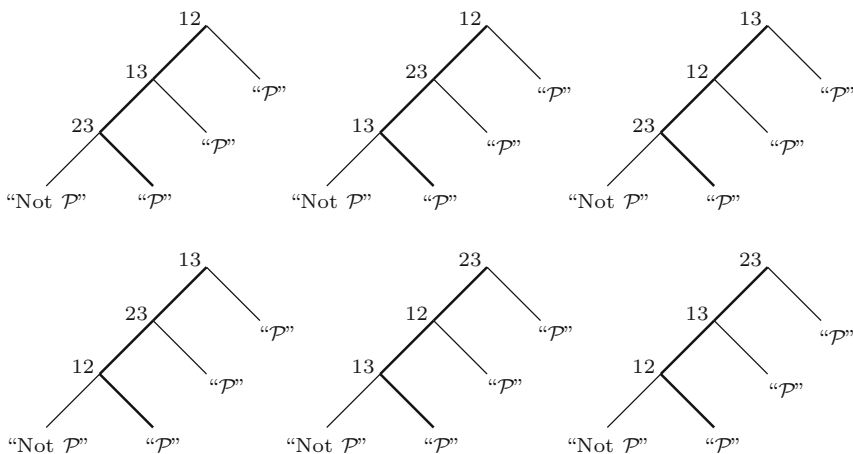


Fig. 3.4 All possible strategies of the seeker and one particular strategy of the hider

For the example $\mathcal{P}_{3,2}$, a strategy for Bob is given by the map

$$(Y, N, e) \mapsto \begin{cases} \text{yes,} & \text{if } |Y \cup \{e\}| = |Y| + 1 \leq 2, \\ \text{no,} & \text{otherwise.} \end{cases}$$

A strategy of Bob determines a path from the top of the tree to a leaf in each decision-tree corresponding to a strategy of Alice. Figure 3.4 shows all possible strategies of Alice and the paths determined—drawn in bold—by Bob's strategy that we just defined. We observe that with this particular strategy of Bob's, Alice is always forced to ask the maximal number $\binom{3}{2}$ of questions.

Complexity

Alice wants to play with a fixed strategy that is optimal for her, i.e., a strategy that minimizes the maximal length of a game with respect to all of Bob's strategies. The complexity of a graph property is a measure for precisely this length.

Definition 3.2. The *complexity* $c(\mathcal{P})$ of a graph property \mathcal{P} is the minimal number k for which there exists a seeker's strategy such that regardless of the hider's strategy, the seeker needs to ask at most k questions.

For our simple example above, the complexity is $c(\mathcal{P}) = \binom{3}{2} = 3$, as discussed. In order to phrase this definition in a formula, let $c(\mathcal{P}, \phi, \psi)$ be the number of questions that Alice has to ask when she is playing with strategy ϕ and Bob is playing with ψ . Then by definition,

$$c(\mathcal{P}) = \min_{\phi} \max_{\psi} c(\mathcal{P}, \phi, \psi),$$

where ϕ and ψ run through all possible strategies of the seeker and hider. Since a simple graph on n vertices has at most $\binom{n}{2}$ edges, we clearly have $c(\mathcal{P}) \leq \binom{n}{2}$. We call a strategy ϕ_0 for Alice *optimal* if it attains the minimum, i.e.,

$$c(\mathcal{P}) = \max_{\psi} c(\mathcal{P}, \phi_0, \psi).$$

With this new language in hand, we want to discuss the idea of a *hypothetical graph* in Bob's mind mentioned earlier. If $G = (V, E)$ is an arbitrary graph, then G defines a particular strategy ψ_G for Bob. Namely,

$$(Y, N, e) \mapsto \begin{cases} \text{yes,} & \text{if } e \in E, \\ \text{no,} & \text{if } e \notin E. \end{cases}$$

In other words, Bob has chosen the graph G and answers according to its edges and nonedges.

Lemma 3.3. For any graph property \mathcal{P} of graphs on the vertex set V ,

$$c(\mathcal{P}) = \min_{\phi} \max_{\psi} c(\mathcal{P}, \phi, \psi) = \min_{\phi} \max_G c(\mathcal{P}, \phi, \psi_G),$$

where the right-side maximum is taken over all possible graphs G with vertex set V .

Proof. Let ϕ and ψ be arbitrary strategies for Alice and Bob. It suffices to show that there exists a graph G such that $c(\mathcal{P}, \phi, \psi) = c(\mathcal{P}, \phi, \psi_G)$. But this is easy. If Alice and Bob play according to the strategies ϕ and ψ , and if Y is the set of edges that Bob has answered during the game with *yes*, then let G be the graph $G = (V, Y)$. \square

In other words, for Alice to choose an optimal strategy it does not matter whether Bob is playing with a fixed graph in mind or is constructing the graph during the game.

Evasiveness

Let's consider some extreme cases for the values of $c(\mathcal{P})$. If the graph property is empty, $\mathcal{P} = \emptyset$, in other words no graph has property \mathcal{P} , then the seeker Alice can answer right away: "The graph does not have property \mathcal{P} !" Similarly, if all graphs satisfy property \mathcal{P} , i.e., \mathcal{P} is the set of all subsets of $\binom{V}{2}$, Alice can answer immediately. We call these two properties the *trivial graph properties*, and in these cases the complexity is zero: the seeker Alice does not need to ask a single question. Note that there are no other cases of graph properties with complexity zero.

The other extreme is more interesting, namely the case in which the complexity is $\binom{n}{2}$, i.e., the maximal number. An easy class of examples with this complexity is given by a generalization of our introductory example. For fixed $n \geq 2$ and $0 \leq k < \binom{n}{2}$, let $V = \{1, \dots, n\}$ and consider the graph property

$$\mathcal{P}_{n,k} = \left\{ E \subset \binom{V}{2} : |E| \leq k \right\},$$

i.e., all graphs on the vertex set V with at most k edges. For this property a possible strategy for the hider Bob might be to answer the first k questions with *yes*, and all others with *no*. In other words, regardless of Alice's strategy, she knows already after the first k questions about the existence of k edges in the graph. But then she has to keep asking about all other edges to make sure that there are not more than k edges in the graph. Hence the complexity is $c(\mathcal{P}_{n,k}) = \binom{n}{2}$, the maximal possible number.

We call all properties \mathcal{P} with maximal complexity $c(\mathcal{P}) = \binom{n}{2}$ *evasive*, as they "tend to avoid self-revelation" [JA01].

Most nontrivial graph properties turn out to be evasive. We will see quite a few examples later in this chapter.

The Greedy Strategy

One particular strategy for the hider Bob suggests itself, the following *greedy strategy*. Bob answers *yes* whenever the graph constructed so far is contained in a graph with property \mathcal{P} , and *no* otherwise. More precisely, consider a particular step in the game when the seeker asks, "Is e an edge of the graph?" and by the previous answers knows the existence of a set Y of edges and a set N of nonedges

already. The greedy strategy yields the answer *yes* whenever there exists an edge set $E \in \mathcal{P}$ disjoint from N such that $Y \cup \{e\} \subseteq E$, and *no* otherwise.

In our previous example for the property *having at most k edges*, the strategy we described is the greedy strategy.

Lemma 3.4. *Assume that Bob is playing the greedy strategy and that the game is in stage (Y, N) , i.e., Alice has knowledge about the existence of a set Y of edges and a set N of nonedges. Then any F with $Y \subseteq F \in \mathcal{P}$ is disjoint from N .*

Proof. Assume that there exists an $F \in \mathcal{P}$ such that $F \cap N \neq \emptyset$. Let $e \in F \cap N$ be the edge that came first in the order of Alice's questions. Then clearly because of the existence of $F \in \mathcal{P}$, Bob would have had to answer *yes* to Alice's question, "Is e an edge of the graph?" A contradiction. \square

The following lemma tells us when the greedy strategy witnesses evasiveness of the graph property.

Lemma 3.5. *Let $\mathcal{P} \neq \emptyset$ be a graph property, ϕ any strategy for the seeker Alice, and ψ the greedy strategy for the hider Bob. Then*

$$c(\mathcal{P}, \phi, \psi) = \binom{n}{2}$$

if for each $E \in \mathcal{P}$ and $e \in E$ with $E \setminus \{e\} \in \mathcal{P}$, there exist an $f \in \binom{V}{2} \setminus E$ and $F \in \mathcal{P}$ such that $(E \setminus \{e\}) \cup \{f\} \subseteq F$.

Proof. Assume to the contrary that Alice has not yet asked $\binom{n}{2}$ questions and can already decide in stage (Y, N) , "The graph has property \mathcal{P} !" Then $Y \cup N \neq \binom{V}{2}$ and each E with $Y \subseteq E \subseteq \binom{V}{2} \setminus N$ satisfies $E \in \mathcal{P}$. Set $E = \binom{V}{2} \setminus N$ and choose an arbitrary

$$e \in E \setminus Y = \left(\left(\binom{V}{2} \setminus N \right) \setminus Y \right) = \binom{V}{2} \setminus (Y \cup N) \neq \emptyset.$$

Then $E \setminus \{e\} \in \mathcal{P}$, and by assumption there exist $f \in \binom{V}{2} \setminus E = N$ and an $F \in \mathcal{P}$ such that $(E \setminus \{e\}) \cup \{f\} \subseteq F$. In particular, $f \in F \cap N$, in contradiction to the previous lemma. \square

This simple criterion proves that quite a few graph properties are evasive.

Theorem 3.6. *Let $n \geq 3$ and $0 \leq k < \binom{n}{2}$. The following properties \mathcal{P} of graphs on n vertices are evasive:*

1. *The graph has at most k edges.*
2. *The graph has exactly k edges.*
3. *The graph is acyclic, i.e., it does not contain cycles.*
4. *The graph is a spanning tree.*
5. *The graph is connected.*

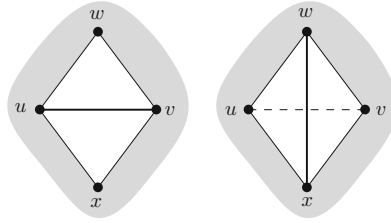


Fig. 3.5 The edge $e = uv$ and its neighboring triangles

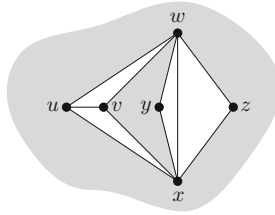


Fig. 3.6 The graph G when wx is present

Proof. In all of these cases, the condition of Lemma 3.5 is easily checked. \square

As an interesting application of Lemma 3.5, we show that planarity is an evasive property.

Theorem 3.7. *For $n \geq 5$, the property of being planar is evasive.*

Proof. Let E be the edge set of a planar graph and $e = uv \in E$. Since $E \setminus \{e\}$ is always a planar graph, we have to show that there is an edge $f \in \binom{V}{2} \setminus E$ such that $(E \setminus \{e\}) \cup \{f\}$ is planar. We may assume that E is the edge set of a maximal planar graph, since the statement is obvious otherwise. Consider a planar drawing of the graph $G = (V, E)$. All faces of this drawing are triangles, and the edge e is an edge of two neighboring triangular faces, say uvw and uvx . If $wx \notin E$, then $f = wx$ satisfies our needs, since after removal of e , we can draw the diagonal connecting w and x . Compare Fig. 3.5. The gray regions in the figure depict the unknown rest of the graph.

But if wx is an edge in G , then let wxy and wxz be the two triangles neighboring wx , as illustrated in Fig. 3.6.

There are two cases to consider. The first case is that the pair of vertices $\{u, v\}$ and $\{y, z\}$ are identical. Then the graph is the complete graph K_4 as shown in Fig. 3.7, which contradicts our assumption $n \geq 5$.

In the other case, the two pairs $\{u, v\}$ and $\{y, z\}$ are not identical. Let us assume that $u \notin \{y, z\}$, since the situation in which $v \notin \{y, z\}$ works analogously. Then yz cannot be an edge of G because in the drawing it would have to intersect one of the edges wx , uw , ux . This follows from the Jordan curve theorem, Theorem A.9. See Fig. 3.8.

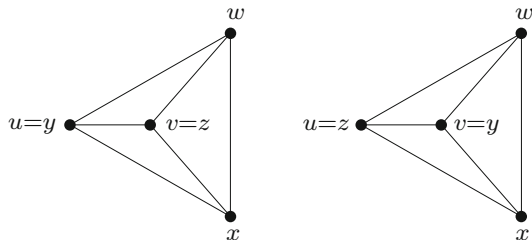


Fig. 3.7 The two cases in which $\{u, v\}$ and $\{y, z\}$ are identical

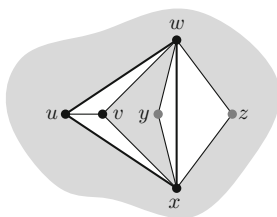


Fig. 3.8 The vertices y and z are separated by the circle $uwxu$

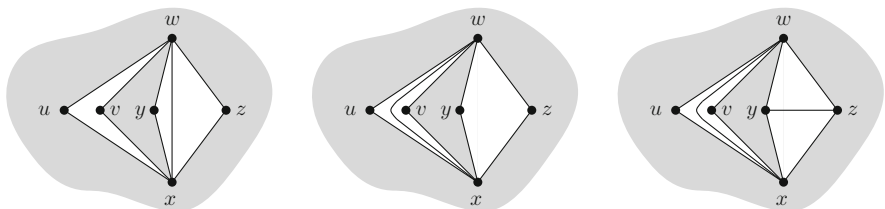


Fig. 3.9 Redrawing the edge wx and introducing yz in the drawing of $G \setminus \{uv\}$

Hence, in $G \setminus \{uv\}$ we may redraw the edge wx in the quadrilateral that appears after removal of uv , and draw the edge yz afterward. The whole procedure is shown in Fig. 3.9. In other words, $f = yz$ satisfies the required needs. \square

Nonevasive Graph Properties

There are only a few graph properties known to be not evasive. For an easy start, we will describe a nonevasive graph property of graphs on a set V of six vertices. Let \mathcal{B}_6 be the graph property given by all possible edge sets E of graphs $G = (V, E)$ that are isomorphic to one of the three graphs shown in Fig. 3.10. It is an easy exercise to see that property \mathcal{B}_6 is nonevasive.



Fig. 3.10 The three isomorphism classes of a nonevasive graph property

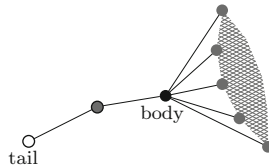


Fig. 3.11 A scorpion graph

We will now describe a whole family of nonevasive graph properties due to Best, van Emde Boas, and Lenstra [BEBL74]. Let $n \geq 5$ be fixed. A graph on n vertices is called a *scorpion graph* if it contains two nonadjacent vertices of degree 1 and degree $n - 2$, called *tail* and *body*, whose uniquely defined common neighbor (playing the role of Antares; cf. Fig. 3.1) has degree 2. There are no restrictions on the adjacencies among the remaining $n - 3$ vertices, see Fig. 3.11.

Note that the body is the unique vertex of degree $n - 2$, and hence body and tail are uniquely defined in any scorpion graph. Moreover, it is worth noting that there is a certain symmetry between body and tail: the body is adjacent to all but one vertex, while the tail is adjacent to exactly one vertex.

The remarkable fact about the property of being a scorpion graph is that it is recognizable in a linear number of steps with respect to the number of vertices. In particular, the property of being a scorpion graph is nonevasive for large enough n .

Theorem 3.8 (Best, van Emde Boas, and Lenstra [BEBL74]). *Let \mathcal{P} be the property of being a scorpion graph on $n \geq 5$ vertices. Then the complexity of \mathcal{P} is bounded by $c(\mathcal{P}) \leq 6n - 13$.*

Proof. We play the role of the seeker Alice and describe an algorithm that determines in the required number of steps whether the hypothetical graph of the hider Bob is a scorpion graph.

The idea is to determine a unique single candidate for a body or a tail vertex. During the course of the game the vertices will be categorized into body and tail candidates. We will refer to the edges to which Bob answers with *yes* as accepted edges and to the edges with answer *no* as rejected edges. Note that a body candidate is a vertex that has at most one rejected incident edge, and a tail candidate is a vertex with at most one accepted incident edge. The algorithm has three phases. The first phase serves to *partition* the vertex set into body and tail candidates. The second phase reduces at least one of these sets to at most one candidate. With a unique body or tail candidate the third, and final, phase decides whether the hypothetical graph is a scorpion graph. After the description of the three phases, we count the questions that are needed.

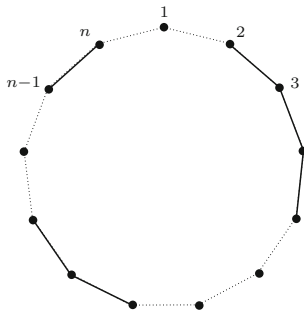


Fig. 3.12 The knowledge of the seeker after the first n questions

Phase I: Each vertex of $V = \{1, \dots, n\}$ can uniquely be classified

- As *body candidate* if it has at most one rejected and at least two accepted incident edges, and
- As *tail candidate* if it has at most one accepted and at least two rejected incident edges.

In order to classify the vertices, we have to check at most three incident edges per vertex. We start with the edge set of the cycle $1, 2, \dots, n, 1$, i.e., the edges $12, 23, 34, \dots, (n-1)n, n1$. After these n questions, we know about two incident edges of each vertex, and the result might look like Fig. 3.12. Accepted edges are shown in bold; rejected edges are dotted.

The vertices with two accepted incident edges (such as vertex 3 in the figure) already qualify as body candidates, while the vertices with two rejected incident edges (such as vertex 1 in the figure) qualify as tail candidates. The remaining vertices (e.g., vertex 2 in the figure) are still indifferent; they may qualify as body or tail vertices. We denote the set of indifferent vertices by I . If I is empty, then either all edges have been rejected, or all edges have been accepted. In the former case, none of the vertices can be a body, while the latter case implies that none of the vertices can be a tail. Either way, we can already answer, “The graph is not a scorpion graph!” Otherwise, this set I has even cardinality greater than or equal to 2. The case $|I| = 2$, i.e., I consists of two adjacent vertices only, is an easy exercise that we leave to the reader. In all other cases, $|I| \geq 4$, and we may divide I into pairs of vertices that are not adjacent on the cycle. We are now asking for exactly those edges that are given by these pairs. The result might look like Fig. 3.13. Now each vertex is either a body or a tail candidate, which we depict in the figure by a black, resp. white, bullet.

Phase II: We want to single out a unique candidate for either the body or the tail. In order to do so, we will start by assigning a weight of 1 or 2 to each vertex. We will then successively ask for edges and, after each step, adjust weights in such a way that exactly one weight reduces by one and all others remain fixed. If a vertex

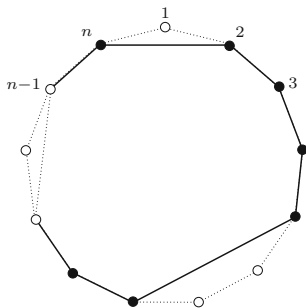


Fig. 3.13 The knowledge of the seeker after $n + \frac{|I|}{2}$ questions at the end of Phase I

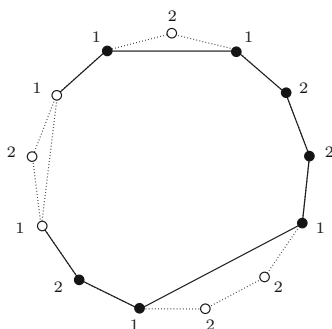


Fig. 3.14 The initial weights after Phase I

obtains weight 0 in this way, it is no longer considered a candidate, and we will no longer ask for edges incident to this vertex.

The weights are defined differently for body and tail candidates as follows:

- A body candidate obtains weight 2 minus the number of rejected incident edges, while
- a tail candidate obtains weight 2 minus the number of accepted incident edges.

Figure 3.14 shows the initial weights after Phase I.

Initially, the *total weight*, i.e., the sum of all weights, is obviously equal to $2n - |I|$. We now successively ask for edges with one vertex in the set of body candidates, and one vertex in the set of tail candidates. Say v is a body candidate and w is a tail candidate. We ask, “Is vw an edge of the graph?” If the answer is *yes*, then the number of accepted edges incident to w increases by 1, and hence the weight of w decreases by 1. Similarly, if the answer is *no*, the number of rejected edges incident to v increases, and hence the weight of v decreases by 1. If either of the two weights drops to zero, the vertex of weight zero is no longer considered a candidate, since it has at least two accepted and two rejected incident edges. A few iterations of this procedure are shown in Fig. 3.15.

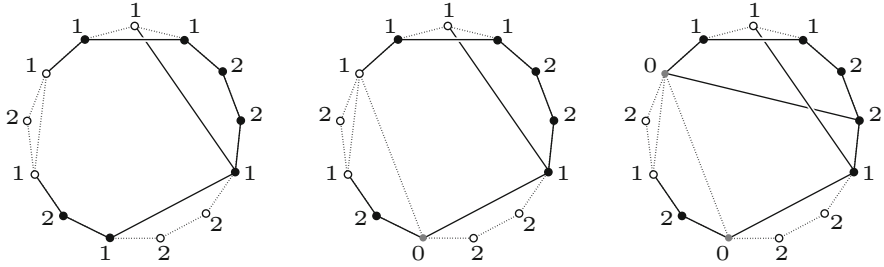


Fig. 3.15 A few iterations of Phase II

Since the total weight decreases by one in each iteration, after at most $2n - |I| - 2$ steps one of the three following situations occurs:

1. The set of body or tail candidates becomes empty.
2. The sets of body and tail candidates are both nonempty and one of them contains exactly one element.
3. There are sets of $b \geq 1$ body candidates and $t \geq 1$ tail candidates remaining, where $\min\{b, t\} \geq 2$, and all edges between these sets have already been asked for.

In situation (a), we can obviously answer, “The graph is not a scorpion graph!” In situation (b), we proceed to Phase III. Now assume we are in situation (c). First of all, note that the total weight is at least three. Therefore at most $2n - |I| - 3$ questions have been asked so far in Phase II. Now let e be the number of accepted edges between the body and tail candidates. Since each body candidate must be adjacent to all but at most one tail candidate, we have $b(t - 1) \leq e$. Similarly, since each tail candidate has at most one neighbor among the body candidates, we have $e \leq t$. Hence $(b - 1)(t - 1) \leq 1$, and since $\min\{b, t\} \geq 2$, we must have $b = t = 2$. Let’s say the body candidate vertices are $\{a, b\}$ and the tail candidate vertices are $\{c, d\}$. Then $2 = b(t - 1) \leq e \leq t = 2$, and hence there are exactly two edges between the body and tail candidates. Without loss of generality, the edges are ac and bd . Then there are only two possibilities for a scorpion graph: either a is the body and d the tail, or b is the body and c the tail. Compare Fig. 3.16. Let x be any vertex other than a, b, c , and d . Now we ask for the edge ax . If ax is an edge of the graph, then only a remains as body candidate. Conversely, if ax is not an edge, then only b remains as body candidate. We then proceed to Phase III.

Phase III: We are left with a unique body or tail candidate u . Assume u is a body candidate. We ask for the adjacency relations of u that are not yet known. There are at most $n - 3$ of them. In case the degree of u is $n - 2$, we now know the unique tail candidate. Checking its adjacency relations and the adjacency relations of the unique common neighbor requires at most another $n - 3 + n - 3$ questions. The case that u is a tail candidate is similar.

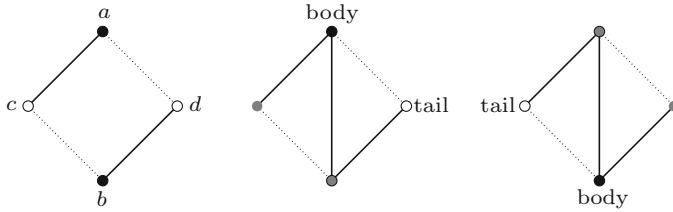


Fig. 3.16 The case $b = t = 2$

Step count: The three phases require at most $n + \frac{|I|}{2}$, $2n - |I| - 2$, and $3n - 9$ questions. Since $|I| \geq 4$, we obtain in total at most

$$n + \frac{|I|}{2} + 2n - |I| - 2 + 3n - 9 = 6n - \frac{|I|}{2} - 11 \leq 6n - 13. \quad \square$$

3.2 Evasiveness of Monotone Graph Properties

In the previous section we have seen quite a variety of evasive graph properties and a few nonevasive graph properties. A noticeable difference is that all nonevasive graph properties share one common feature: they are not monotone, i.e., they are not closed under removing (or alternatively adding) edges.

Monotone Graph Properties

Definition 3.9. A graph property \mathcal{P} is called *monotone* if it is closed under removing edges, i.e., whenever $E' \subseteq E \in \mathcal{P}$, then $E' \in \mathcal{P}$.

Obvious examples of monotone properties are the properties *having at most k edges*, *being planar*, *being acyclic*, etc.

Note that if a graph property \mathcal{P} is closed under adding edges, then the *complementary property*

$$\overline{\mathcal{P}} = \left\{ \binom{V}{2} \setminus E : E \in \mathcal{P} \right\}$$

is monotone. The fact that $c(\overline{\mathcal{P}}) = c(\mathcal{P})$, as shown in Exercise 7, now justifies that we concentrate only on properties closed under removing edges.

All known monotone graph properties besides the trivial ones—as defined on page 74—are evasive. This led Richard Karp in the early 1970s to the following conjecture.

Conjecture 3.10 (R. Karp). Every nontrivial monotone graph property is evasive.

The main result of this section will show that the conjecture is true whenever \mathcal{P} is a monotone property of graphs on n vertices and n is a power of a prime number. This was shown by topological methods in a striking paper [KSS84] by Jeff Kahn, Michael Saks, and Dean Sturtevant in 1984. In the same publication, they also proved the conjecture in the case $n = 6$, the smallest non-prime-power case. All other cases are still open even though a great deal of research has been carried out since then.

The proof of the prime-power case involves several steps. The first important step will be to link the property of evasiveness to a topological property. Subsequently, we will apply a somewhat deeper topological result along with a little bit of algebra. The topological background will be explained in more detail in Appendix E.

Simplicial Complexes

The monotonicity condition yields a direct link to topology: every monotone graph property defines an (abstract) simplicial complex.

In fact, consider a graph property \mathcal{P} of graphs with vertex set V . Then \mathcal{P} is an abstract simplicial complex on the vertex set $X = \binom{V}{2}$, i.e., a simplicial complex on the edge set of the complete graph on V . Each $E \in \mathcal{P}$ constitutes a face $E \subseteq X$ of the simplicial complex.

As a first example, we return to the property *having at most two edges* for 3-vertex graphs

$$\mathcal{P} = \{\emptyset, \{12\}, \{13\}, \{23\}, \{12, 13\}, \{12, 23\}, \{13, 23\}\},$$

with our usual abbreviation uv for the edge $\{u, v\}$.

The graph property \mathcal{P} corresponds to the boundary of a 2-simplex with vertex set $X = \{12, 13, 23\}$ as shown in Fig. 3.17. The graph on V with no edges corresponds to the empty face, the graphs with precisely one edge correspond to the 0-dimensional faces of the complex, and the graphs with precisely two edges correspond to the 1-dimensional faces. Compare also Fig. 3.2 on page 70, where all graphs with property \mathcal{P} are shown.

In general, the property *having at most k edges* in an n -vertex graph corresponds to the $(k - 1)$ -skeleton of an $\left(\binom{n}{2} - 1\right)$ -simplex.

The topological spaces associated with these examples are not completely trivial: they have “holes.” It will turn out that any graph property is evasive as soon as the associated space is topologically nontrivial in a very strong sense. Before we make this precise by introducing the concept of *collapsibility*, we will first generalize our notion of evasiveness to general set systems and thereby to simplicial complexes.

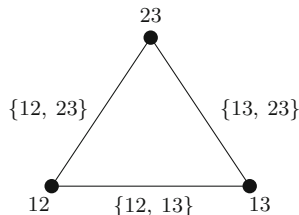


Fig. 3.17 The simplicial complex corresponding to the property *having at most two edges* in a 3-vertex graph

Evasiveness of Set Systems

We have seen that the graphs satisfying a given property correspond to the faces of the associated simplicial complex. We will now generalize the game between the hider and the seeker to arbitrary set systems.

The hider and seeker agree on a vertex set X and a set system $S \subseteq \mathcal{P}(X)$. Now the game is to decide whether a hypothetical subset $\sigma \subseteq X$ —unknown to the seeker Alice—of the vertex set is an element of the set system S .

Alice follows a decision-tree algorithm with questions of the type “Is $x \in \sigma$?” for vertices $x \in X$, and the hider Bob answers *yes* or *no*. Alice’s goal is to ask as few questions as possible, whereas the aim of Bob is to force Alice to ask as many questions as possible. The game is over as soon as Alice can decide whether $\sigma \in S$.

As before, the *complexity*, $c(S, X)$, is defined as the minimal number k such that there exists a strategy for Alice that allows her always to finish the game by asking at most k questions.

Definition 3.11. Let X be a set of m vertices and S a set system $S \subseteq \mathcal{P}(X)$. The pair (S, X) is called *evasive* if the complexity $c(S, X)$ is equal to m , i.e., for every strategy of the seeker Alice, there exists a subset $\sigma \subseteq X$ such that she needs to ask m questions in order to decide whether $\sigma \in S$.

We will be mostly interested in the case that the set system is a simplicial complex $K \subseteq \mathcal{P}(X)$.

There are two interesting observations to discuss. First of all, not all elements from X have to appear as vertices of K . This will be of some importance in the sequel.

Secondly, this type of game is more general than the game for graphs: the size of the vertex set of the simplicial complex can be arbitrary, while the number of edges of the complete graphs are always binomial coefficients. Moreover, a graph property is by definition invariant under graph isomorphism—which yields a certain symmetry of the associated simplicial complex that we will discuss later—whereas there is no such condition on the simplicial complexes we are now considering.

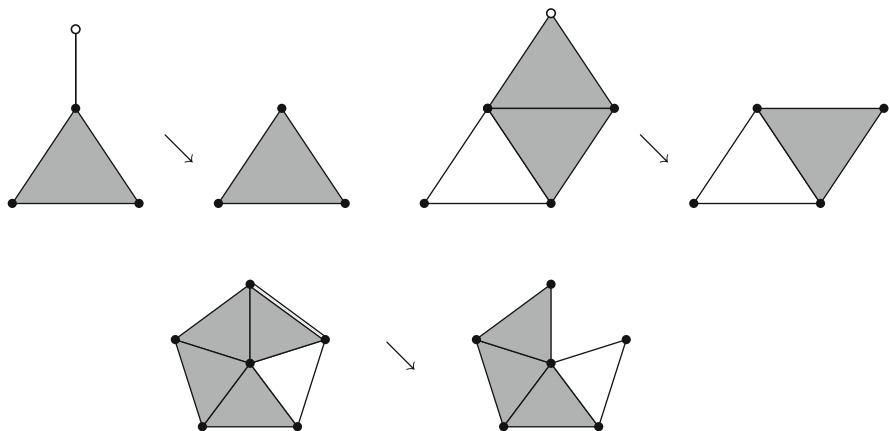


Fig. 3.18 Examples of elementary collapses

Furthermore, note that if \mathcal{P} is a monotone graph property of graphs on the vertex set V , and $X = \binom{V}{2}$, then \mathcal{P} is an evasive graph property if and only if (\mathcal{P}, X) is evasive.

Collapsibility

Collapsibility is a property of simplicial complexes. Loosely speaking, a simplicial complex is collapsible if it can be deformed to a single vertex by a sequence of “scrunching steps.” The scrunching steps are given by so-called elementary collapses. In order to define these, we first need to introduce the concept of a free face.

Definition 3.12. A nonempty face σ in a simplicial complex is a *free face* if

- It is not inclusion maximal in K , and
- It is contained in exactly one inclusion-maximal face of K .

An *elementary collapse* of K is a simplicial complex K' obtained from K by the removal of a free face $\sigma \in K$ along with all faces that contain σ , i.e., $K' = K \setminus \{\tau : \tau \in K, \sigma \subseteq \tau\}$. Whenever a complex K' is obtained from K by an elementary collapse, we denote this by $K \searrow K'$.

Figure 3.18 gives a few examples of elementary collapses. It is an easy exercise to show that an elementary collapse induces a homotopy equivalence of the polyhedra associated with K and K' . Similar to the concept of contractability, we introduce the concept of collapsibility.

Definition 3.13. A simplicial complex K is *collapsible* if there exists a sequence of elementary collapses $K = K_0 \searrow K_1 \searrow K_2 \searrow \cdots \searrow K_r = \{\emptyset, \{z\}\}$ onto a single vertex.

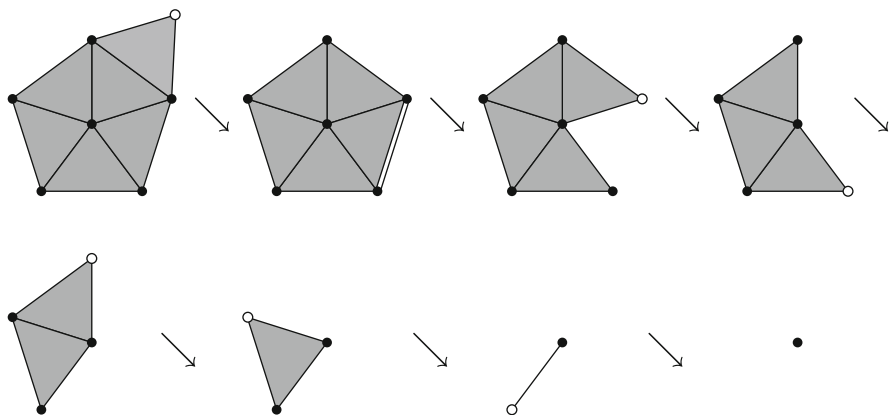


Fig. 3.19 A collapsible simplicial complex

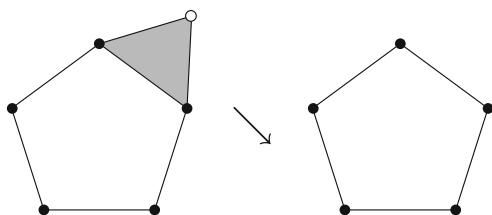


Fig. 3.20 A noncollapsible simplicial complex

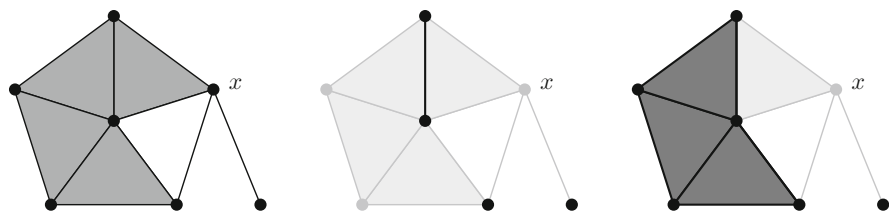


Fig. 3.21 A complex and the link and deletion of the vertex x

Figure 3.19 shows a collapsible simplicial complex along with the sequence of elementary collapses, while Fig. 3.20 illustrates a simplicial complex that is not collapsible: it allows one elementary collapse, but afterward does not possess any more free faces.

Since elementary collapses induce homotopy equivalences, any collapsible complex is also contractible. (For simplicity, we will call a simplicial complex contractible if its polyhedron is contractible.) But note that the concepts of contractibility and collapsibility are not identical. There exist contractible complexes that are not collapsible. A prominent example for such a complex is the dunce hat [Zee63] and Bing's house with two rooms [Bin64].

Link, Deletion, and Collapsibility

In order to show the main result of this section—as stated in the section title—we need the concept of two particular complexes that occur in our setting. Let $K \subseteq \mathcal{P}(X)$ be a simplicial complex and $x \in X$. The simplicial complexes *link* and *deletion* of x are defined to be

$$\text{lk}(x, K, X) = \{\sigma \subseteq X \setminus \{x\} : \sigma \cup \{x\} \in K\},$$

$$\text{del}(x, K, X) = \{\sigma \subseteq X \setminus \{x\} : \sigma \in K\}.$$

If no confusion about K and X can occur, we will abbreviate the two complexes by $\text{lk}(x)$ and $\text{del}(x)$. Note that if $x \in X \setminus \text{vert}(K)$, then $\text{lk}(x) = \emptyset$ and $\text{del}(x) = K$. Also note that if x is an isolated vertex of K , i.e., when $\{x\}$ is a maximal face of K , then $\text{lk}(x) = \{\emptyset\}$. A more illuminating example, where $x \in \text{vert}(K)$, is given in Fig. 3.21.

Lemma 3.14. *Let $K \subseteq \mathcal{P}(X)$ be a simplicial complex and $x \in X$. If $\text{lk}(x)$ and $\text{del}(x)$ are collapsible, then so is K .*

Proof. Note that the collapsibility of $\text{lk}(x)$ implies in particular that $\text{lk}(x)$ is nonempty and hence $x \in \text{vert}(K)$. It clearly suffices to show that K can be collapsed down to $\text{del}(x)$. Since this is fairly straightforward, the reader is encouraged to provide the details accompanying the *picture proof* [Pól56] as shown in Figs. 3.22–3.24. \square

Nonevasive Complexes Are Collapsible

The following theorem establishes the essential link between evasiveness and topology.

Theorem 3.15. *Let $X \neq \emptyset$ and $K \subseteq \mathcal{P}(X)$ be a nonempty simplicial complex. If (K, X) is nonevasive, then K is collapsible.*

Proof. First of all, note that $K \neq \{\emptyset\}$, since $(\{\emptyset\}, X)$ is easily seen to be evasive for $X \neq \emptyset$. And hence K has at least one vertex. We now proceed by induction on $n = |X|$. The case $n = 1$ is clear. For the induction step $n \geq 2$ consider the decision-tree of an algorithm that proves nonevasiveness of (K, X) and assume “ $x \in \sigma$?” is the first question according to the algorithm.

Denote by ϕ_L , respectively ϕ_R , the strategies belonging to the left branch L succeeding the *yes* answer to the first question, respectively the right branch R succeeding the *no* answer, as shown in Fig. 3.25.

Consider $\text{lk}(x) = \text{lk}(x, K, X)$ and $\text{del}(x) = \text{del}(x, K, X)$. We claim that $(\text{lk}(x), X \setminus \{x\})$ and $(\text{del}(x), X \setminus \{x\})$ are nonevasive. In order to see this, observe that for any subset $\tau \subseteq X \setminus \{x\}$, we have $\tau \in \text{lk}(x)$ if and only if $\tau \cup \{x\} \in K$, and

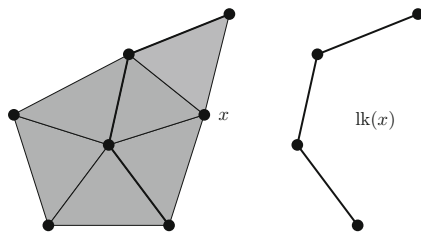


Fig. 3.22 The complex K , a vertex x , and $\text{lk}(x)$

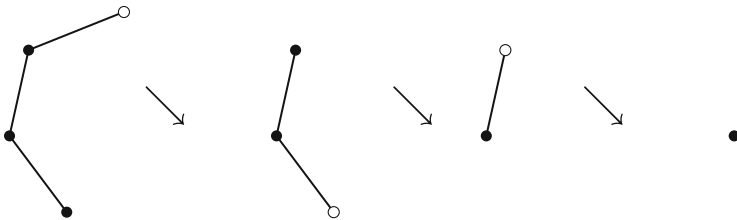


Fig. 3.23 The collapsing sequence of $\text{lk}(x)$

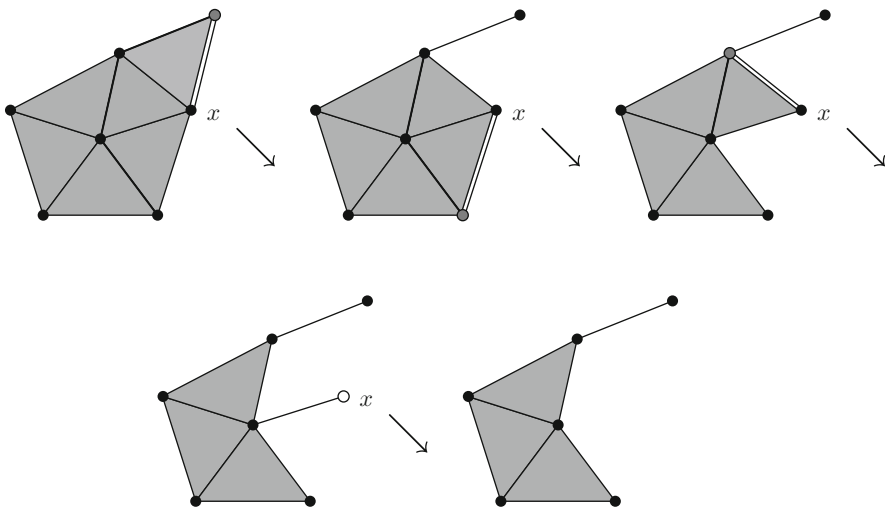


Fig. 3.24 Collapsing K onto $\text{del}(X)$

$\tau \in \text{del}(x)$ if and only if $\tau \in K$. Hence ϕ_L is a strategy proving nonevasiveness of $(\text{lk}(x), X \setminus \{x\})$, and ϕ_R is a strategy proving nonevasiveness of $(\text{del}(x), X \setminus \{x\})$.

We want to apply the induction hypothesis. We have to be a little careful about the possibility that $\text{lk}(x)$ or $\text{del}(x)$ may be empty.

If $\text{lk}(x) = \emptyset$, then clearly $K = \text{del}(x)$, which is nonempty by assumption. Since $(\text{del}(x), X \setminus \{x\})$ is nonevasive, we obtain by the induction hypothesis that K is collapsible. If $\text{del}(x) = \emptyset$, then by the fact that K has at least one vertex, we must

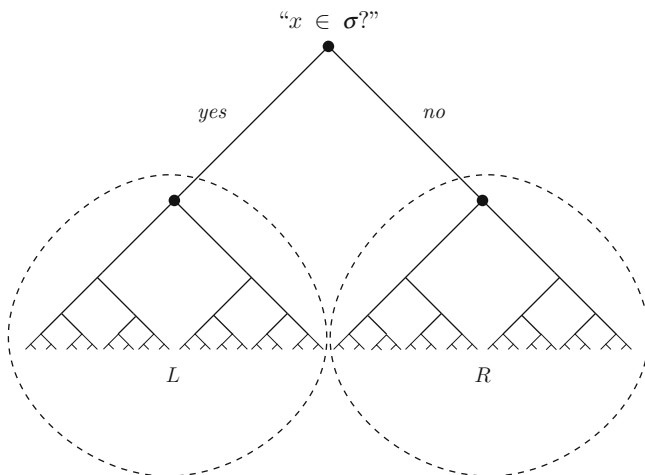


Fig. 3.25 The two branches L and R succeeding the first question of the seeker

have $K = \{\emptyset, \{x\}\}$, which is collapsible by definition. If neither $\text{lk}(x)$ nor $\text{del}(x)$ is empty, then by the induction hypothesis, both complexes are collapsible, and we are done by an application of Lemma 3.14. \square

3.3 Karp's Conjecture in the Prime-Power Case

In this section we will finally prove Karp's conjecture, Conjecture 3.10, in the prime-power case, i.e., we are going to prove that every nontrivial monotone property of graphs with a prime-power number of vertices is evasive.

We give a brief outline of the proof that also serves as a guide through the section. Let \mathcal{P} be a property of graphs on the vertex set V and let $|V|$ be a prime-power. Consider the simplicial complex $K \subseteq \mathcal{P}(X)$ associated with \mathcal{P} , where $X = \binom{V}{2}$. We will prove the contrapositive of Karp's conjecture: If $K \neq \emptyset$ and \mathcal{P} is not evasive, then $K = \mathcal{P}(X)$, i.e., \mathcal{P} must be the trivial property containing all graphs. Thinking of K as a simplicial complex, $K = \mathcal{P}(X)$ means that it is the complex given by the simplex X and all its faces.

The nonevasiveness of K yields, by Theorem 3.15, that K is collapsible. Now the symmetry of K inherited by the fact that \mathcal{P} is invariant under graph isomorphisms comes into play. We will consider a symmetry subgroup that acts *transitively* on the vertices of K , i.e., for each pair of vertices of K there is a symmetry interchanging the two vertices.

In the subsequent step, we will employ a strong topological result that states that a contractible simplicial complex with a symmetry group satisfying some group-theoretic condition must contain a simplex that remains fixed under the whole symmetry group. In turn, the transitivity of the group action implies the desired equality $K = \mathcal{P}(X)$.

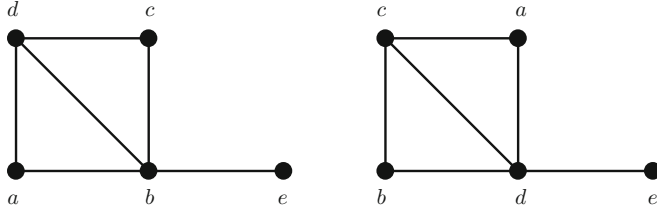


Fig. 3.26 The graphs $G = (V, E)$ and $(V, \pi \cdot E)$

Group Actions on Graph Properties

Let \mathcal{P} be a property of graphs on the vertex set V , i.e., $\mathcal{P} \subseteq \mathcal{P}(X)$, where $X = \binom{V}{2}$ is the set of all edges.

The symmetric group, $\text{Sym}(V)$, acts on the set V via $\pi \cdot u = \pi(u)$, and this action induces an action on the set X of edges via $\pi \cdot uv = \pi(u)\pi(v)$.

Moreover, if $E \subseteq X$ is the edge set of a graph, then $\pi \cdot E$ is defined to be the set of edges

$$\pi \cdot E = \{\pi \cdot uv : uv \in E\} \subseteq X$$

defining a new graph $(V, \pi \cdot E)$. Hence we have an induced action of $\text{Sym}(V)$ on the set of graphs on the vertex set V . Figure 3.26 shows an example of a graph $G = (V, E)$ on the vertex set $V = \{a, b, c, d, e\}$ and its image $(V, \pi \cdot E)$ under the induced action of the element

$$\pi = \begin{pmatrix} a & b & c & d & e \\ b & d & a & c & e \end{pmatrix} \in \text{Sym}(V).$$

The invariance of \mathcal{P} under graph isomorphism translates into the condition that for any $\pi \in \text{Sym}(V)$,

$$E \in \mathcal{P} \text{ if and only if } \pi \cdot E \in \mathcal{P}.$$

In other words, any graph property is invariant under the action of the group $\text{Sym}(V)$.

It is easy to see that this group action is *transitive* on the set X , i.e., if $uv, xy \in \binom{V}{2} = X$ is an arbitrary pair of edges, then there exists a $\pi \in \text{Sym}(V)$ such that $\pi \cdot uv = xy$.

Lemma 3.16. *Let $K \subseteq \mathcal{P}(X)$ be a simplicial complex. Assume that the group G acts transitively on X such that K is invariant under the induced action. If the set of fixed points $|K|^G$ of the induced action on the polyhedron $|K|$ is nonempty, then $K = \mathcal{P}(X)$.*

Proof. Let $x \in |K|^G$ be a fixed point and $\sigma \in K$ the simplex that is minimal under inclusion with the property that $x \in |\sigma|$. We claim that $\sigma = X$, which proves the lemma. Since σ cannot be a vertex by the transitivity of the group action, x is, in fact, contained in the interior of $|\sigma|$. If $\sigma \neq X$, then choose elements $a \in \sigma$ and $b \in X \setminus \sigma$, and let $g \in G$ be such that $g \cdot a = b$. Then clearly $g \cdot \sigma \neq \sigma$, and hence in particular, $\text{int}(g \cdot |\sigma|) \cap \text{int}(|\sigma|) = \text{int}(|g \cdot \sigma|) \cap \text{int}(|\sigma|) = \emptyset$. This contradicts the fact that $|\sigma|$ contains the fixed point x . \square

The following theorem from Smith theory—the homological theory of orbits and fixed points of group actions on simplicial complexes—is an immediate corollary of Theorem E.16 on page 228.

Theorem 3.17. *Let $K \subseteq \mathcal{P}(X)$ be a simplicial complex. Assume that the finite group G acts on X such that K is invariant under the induced action. Furthermore, assume that*

- $|K|$ is contractible,
- There exists a normal subgroup $H \trianglelefteq G$, such that H is a p -group, i.e., the order of H is a power of a prime p , and
- The quotient G/H is cyclic.

Then the set of fixed points $|K|^G$ is nonempty. \square

A Group Action in the Prime-Power Case

Assume now that the number of elements of the vertex set V is a prime-power. Let's say $|V| = p^r$ for some prime p . Without loss of generality, we may assume that $V = F$ is the ground set of the finite Galois field F with p^r elements [Hun74]. Consider the following subgroup G of $\text{Sym}(V)$:

$$G = \{f_{a,b} : a, b \in F, a \neq 0\},$$

where $f_{a,b} : V \rightarrow V$ is the affine linear function defined by $f_{a,b}(x) = ax + b$. Then G acts transitively on $\binom{V}{2}$ due to the fact that $\det \begin{pmatrix} u & 1 \\ v & 1 \end{pmatrix} = u - v$ is nonzero for $u \neq v$. Now consider the subgroup

$$H = \{f_{0,b} : b \in F\}$$

of G . Clearly H is a p -group, since its cardinality $|H| = |F| = p^r$ is a power of a prime. Moreover, the quotient G/H is isomorphic to the multiplicative group $(F \setminus \{0\}, \cdot)$ of the field F . It is a basic exercise in algebra to see that this group is always cyclic for finite fields F .

A Proof of Karp's Conjecture in the Prime-Power Case

Now we have only to put the pieces together in order to obtain a proof of Karp's conjecture in the prime-power case.

Theorem 3.18 (Khan, Saks, Sturtevant [KSS84]). *Assume that \mathcal{P} is a nontrivial monotone graph property of graphs on the vertex set V and that $|V| = p^r$ is a power of a prime. Then \mathcal{P} is evasive.*

Proof. Assume that $\mathcal{P} \neq \emptyset$ is a monotone nonevasive property of graphs on the vertex set V . We have to show that $\mathcal{P} = \mathcal{P}(X)$ is the remaining trivial property. Let $X = \binom{V}{2}$ and let G be defined as above, acting transitively on X . By Theorem 3.15, \mathcal{P} is collapsible. Since collapsible complexes are contractible, the desired result follows from Theorem 3.17 and Lemma 3.16. \square

3.4 The Rivest–Vuillemin Theorem on Set Systems

We end this chapter with a theorem by Rivest and Vuillemin [RV76] that is very similar to Theorem 3.18 and proves evasiveness for general set systems on a ground set of prime-power cardinality with a transitive group action. In contrast to Theorem 3.18, it has an elementary proof based purely on a counting argument.

Let X be a set and $S \subseteq \mathcal{P}(X)$ a family of subsets. The starting point is a very interesting observation, the proof of which we leave as an exercise.

Lemma 3.19. *If the number of sets in S of even cardinality is different from the number of sets of odd cardinality, then (S, X) is evasive.* \square

Now assume that a group $G \leq \text{Sym}(X)$ acts transitively on X and leaves S invariant, i.e., $\pi \cdot S = \{\pi(\sigma) : \sigma \in S\} = S$ for every $\pi \in G$. Let $\sigma \in S$ be an element of S and $G \cdot \sigma = \{\sigma_1, \dots, \sigma_k\} \subseteq S$ the orbit of σ . For $x \in X$, let $h(x)$ be defined to be the number of sets in the orbit that contain x , i.e.,

$$h(x) = |\{i \in [k] : x \in \sigma_i\}|.$$

By the transitivity of the group action, we easily see that $h(x)$ is independent of the choice of $x \in X$. So let us denote this number simply by h . Then, by double counting, we obtain the identity $k|\sigma| = h|X|$.

Theorem 3.20. *Let X be a set of prime-power cardinality p^r and $S \subseteq \mathcal{P}(X)$ a family of subsets such that $\emptyset \in S$ and $X \notin S$. If, moreover, there exists a transitive group action on X leaving S invariant, then (S, X) is evasive.*

Proof. Let $\sigma \in S$, $\sigma \neq \emptyset$, and let $G \cdot \sigma = \{\sigma_1, \dots, \sigma_k\} \subseteq S$ be the corresponding orbit. Then, by the preceding considerations, $k|\sigma| = hp^r$. Since $|\sigma| < p^r$, we conclude that p divides the size k of the orbit. Hence p divides the size of each

orbit in S except the size of the orbit $\{\emptyset\}$. Since S is partitioned by the orbits, the number of sets in S of even cardinality turns out to be different from the number of sets of odd cardinality. \square

Note that this beautiful theorem has no effect on Karp's conjecture since the number of edges of a complete graph K_n is a prime-power only in the case $n = 3$.

Exercises

1. Let (a_{ij}) be a matrix with real entries. Show that

$$\max_i \min_j a_{ij} \leq \min_j \max_i a_{ij}$$

with equality if and only if there exist i_0 and j_0 such that the entry $a_{i_0 j_0}$ is minimal in row i_0 and maximal in column j_0 .

2. Give an example of a graph property \mathcal{P} satisfying

$$\min_{\phi} \max_G c(\mathcal{P}, \phi, \psi_G) \neq \max_G \min_{\phi} c(\mathcal{P}, \phi, \psi_G).$$

3. Let $I = [0, 1]$ be the unit interval. Prove or disprove: if $f : I \times I \rightarrow \mathbb{R}$ is a continuous map, then

$$\max_{x \in I} \min_{y \in I} f(x, y) = \min_{y \in I} \max_{x \in I} f(x, y).$$

4. Prove the converse of Lemma 3.5. More precisely, show that if ψ is the greedy strategy for the hider and if

$$\min_{\phi} c(\mathcal{P}, \phi, \psi) = \binom{n}{2},$$

then for each $E \in \mathcal{P}$ and $e \in E$ with $E \setminus \{e\} \in \mathcal{P}$, there exist an $f \in \binom{V}{2} \setminus E$ and $F \in \mathcal{P}$ such that $(E \setminus \{e\}) \cup \{f\} \subseteq F$.

5. Give a proof of Theorem 3.6 on page 75.
6. Provide the missing details for the case $|I| = 2$ in Phase I of the algorithm in the proof of Theorem 3.8, thereby completing the proof.
7. Prove that $c(\mathcal{P}) = c(\overline{\mathcal{P}})$ for any graph property \mathcal{P} , where $\overline{\mathcal{P}}$ is as defined on page 82.
8. Show that the graph property \mathcal{B}_6 defined on page 77 is not evasive.
9. Property \mathcal{B}_6 can easily be generalized to a property of graphs on a fixed number $n \geq 6$ of vertices. Let \mathcal{B}_n be the property given by all graphs on n vertices isomorphic to any of the three shown in Fig. 3.27. Compared to Fig. 3.10, the center edge has been replaced by a path of length $n - 5$. Show that the graph property \mathcal{B}_n is not evasive.

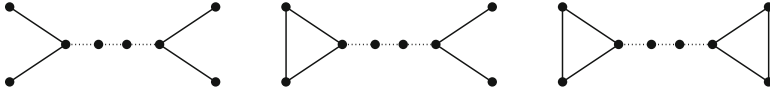


Fig. 3.27 The three isomorphism types of graphs in \mathcal{B}_n

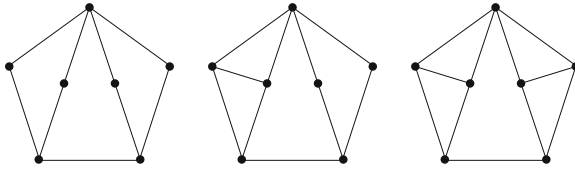


Fig. 3.28 Graphs describing a nonevasive graph property

10. Let \mathcal{P} be the graph property given by all possible graphs that are isomorphic to one of the three graphs shown in Fig. 3.28. Show that \mathcal{P} does not satisfy the condition of Lemma 3.5.
11. Show that the graph property \mathcal{P} defined in the previous exercise is not evasive [MW76].
12. Show that if K' is obtained from K by an elementary collapse, i.e., $K \searrow K'$, then the polyhedron $|K'|$ is a strong deformation retract of $|K|$. In particular, the polyhedra $|K|$ and $|K'|$ are homotopy equivalent.
13. Provide the details of the proof of Lemma 3.14 on page 87.
14. Show that the group $G = \{f_{a,b} : a, b \in F, a \neq 0\} \leq \text{Sym}(F)$ as defined on page 91 acts transitively on $\binom{F}{2}$ for any finite field F .
15. Let G be defined as in the previous exercise and $H = \{f_{0,b} : b \in F\} \leq G$. Show that the quotient G/H is isomorphic to the multiplicative group $(F \setminus \{0\}, \cdot)$.
16. Let (G, \cdot, e) be a finite multiplicative group and m the largest order among its elements. Show that $g^m = e$ for any $g \in G$.
17. Let F be a finite field. Use the previous exercise to show that the multiplicative group $(F \setminus \{0\}, \cdot)$ is cyclic. Hint: Consider the polynomial $x^m - 1 \in F[x]$.
18. This exercise is concerned with a result by Kahn, Saks, and Sturtevant [KSS84] showing asymptotic quadratic complexity for nontrivial monotone graph properties. Let

$$c(n) = \min\{c(\mathcal{P}) : \mathcal{P} \text{ monotone, nontrivial property of } n\text{-vertex graphs}\}.$$

Prove that $c(n) \geq \frac{n^2}{4} - \varphi(n)$, where $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ is a function with $\lim_{n \rightarrow \infty} \frac{\varphi(n)}{n^2} = 0$.

Besides Theorem 3.18, you may use the following results.

- (a) A lemma by Kleitman and Kwiatkowski [KK80] stating that

$$c(n) \geq \min\{c(n-1), q(n-q)\},$$

where q is the prime-power nearest to $\frac{n}{2}$.

- (b) A result from number theory that states that there is a function $\psi : \mathbb{N} \rightarrow \mathbb{N}$ with $\lim_{n \rightarrow \infty} \frac{\psi(n)}{n} = 0$ and the property that for each n there exists a prime number between $n - \psi(n)$ and $n + \psi(n)$.
19. Provide a proof of Lemma 3.19 on page 92.
20. Show that $h(x)$, as defined on page 92, is independent of the choice of $x \in X$.