Der Abel-Preis:
Die Preisverleihung und eine Skizze einiger Aspekte des Werks der Preisträger von 2021

Martin Grötschel

Tag der Mathematik, FU Berlin
30.04.2022

- Institut für Mathematik, Technische Universität Berlin (TUB) (1991-2015, im Ruhestand)
- Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB) (1991-2015)
- DFG-Forschungszentrum "Mathematik für Schlüsseltechnologien" (MATHEON) (2002-2014)
- Berlin-Brandenburgische Akademie der Wissenschaften (2015-2020)

groetschel@bbaw.de
http://www.zib.de/groetschel

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Offizielle Ankündigung 2002

The Abel Prize – International Prize of Mathematics – Awarded yearly

The Abel Prize is named after Niels Henrik Abel, Norway's greatest mathematician throughout the times. Abel left lasting marks on the mathematical world. His mathematics have served as a base for a number of major technological breakthroughs, …. The Abel Prize was established by the Norwegian Parliament (The Storting) in 2002, on the occasion the 200-year anniversary of his birth.

- The Prize is 7,5 million Norwegian Kroner (heute: 775.000 Euro)
- The Prize is awarded by The Norwegian Academy of Science and Letters, on behalf of the Ministry of Education.
- The Abel Committee, consisting of five leading mathematicians from throughout the world, holds the task of appraising nominated candidates a worthy winner.

Ziel des Abel-Preises

Zitat aus den Statuten des Abel-Preises:

- The main objective of the Abel Prize is to recognize pioneering scientific achievements in mathematics.
- The Prize shall also help boost the status of the field of mathematics in society and stimulate children and youth to become interested in mathematics.

Aktivitäten für Schüler & Lehrer

Zitat:

"These…activities include…

- the Niels Henrik Abel competition for high school students
- the UngeAbel competition for class teams of elementary school pupils
- and the Bernt Michael Holmboe Memorial Prize, an annual prize awarded in connection with the Abel Prize ceremony, to a teacher or a group of teachers, who have done extraordinary efforts in mathematics teaching in Norway."

Berlin Special:

Der Hauptpreis des TdM ist traditionell der "Kleine Abelpreis": Das Siegerteam wohnt der Verleihung des Abelpreises am 24. Mai 2022 in Oslo bei.

Tragischer Aspekt (Abel: 5.8.1802-6.4.1829)

Abel und Berlin

Im Winter 1825-1826 war Abel in Berlin. Hier wurde August Leopold Crelle Abels enger Freund. Er unterstützte ihn in vielerlei Hinsicht. Im ersten Band des „Journals für die reine und angewandte Mathematik" –kurz „Crelles Journal"– erschienen allein sieben Artikel von Abel.

Abel beschäftigte sich u. a. mit Integralgleichungen (Abelsches Theorem), mit der Konvergenz von Reihen und Potenzreihen (Abelsches Kriterium, Abelscher Grenzwertsatz), mit Gruppentheorie (abelsche Gruppen) und bewies die Unlösbarkeit allgemeiner Polynomgleichungen fünften Grades.

Viele seiner Ergebnisse waren richtungsweisend für die Mathematik.

1829 sollte Niels Henrik Abel dank Crelles Einsatzes auf eine Professur für Mathematik in Berlin berufen werden. Crelle schrieb diese Nachricht am 8. April 1829 an Abel, zwei Tage nach Abels Tod, von dem er zu diesem Zeitpunkt noch nicht wusste.

Der kleine Abel-Preis

Abel und Berlin hatten eine besondere Beziehung. Ohne die Hilfe aus Berlin wäre Abels Genie vermutlich nicht erkannt worden.

Dies ist der Grund dafür, dass der norwegische Botschafter in jedem Jahr den „Kleinen Abel-Preis“ stiftet. Dieser Preis ist etwas Besonderes. Man kann ihn nicht kaufen, sondern wird zu einem ganz besonderen Event eingeladen. Die Berliner Mathematik ist dem norwegischen Botschafter für diese großzügige Geste sehr dankbar.

Berlin erinnert auch an Abel.
Wie das geschieht, erfahren Sie in ein paar Minuten.

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Wie kommt die IMU ins Spiel?

The Abel Committee

The Norwegian Academy of Science and Letters appoints the members of the Abel Committee, based on nominations from the International Mathematical Union and the European Mathematical Society.

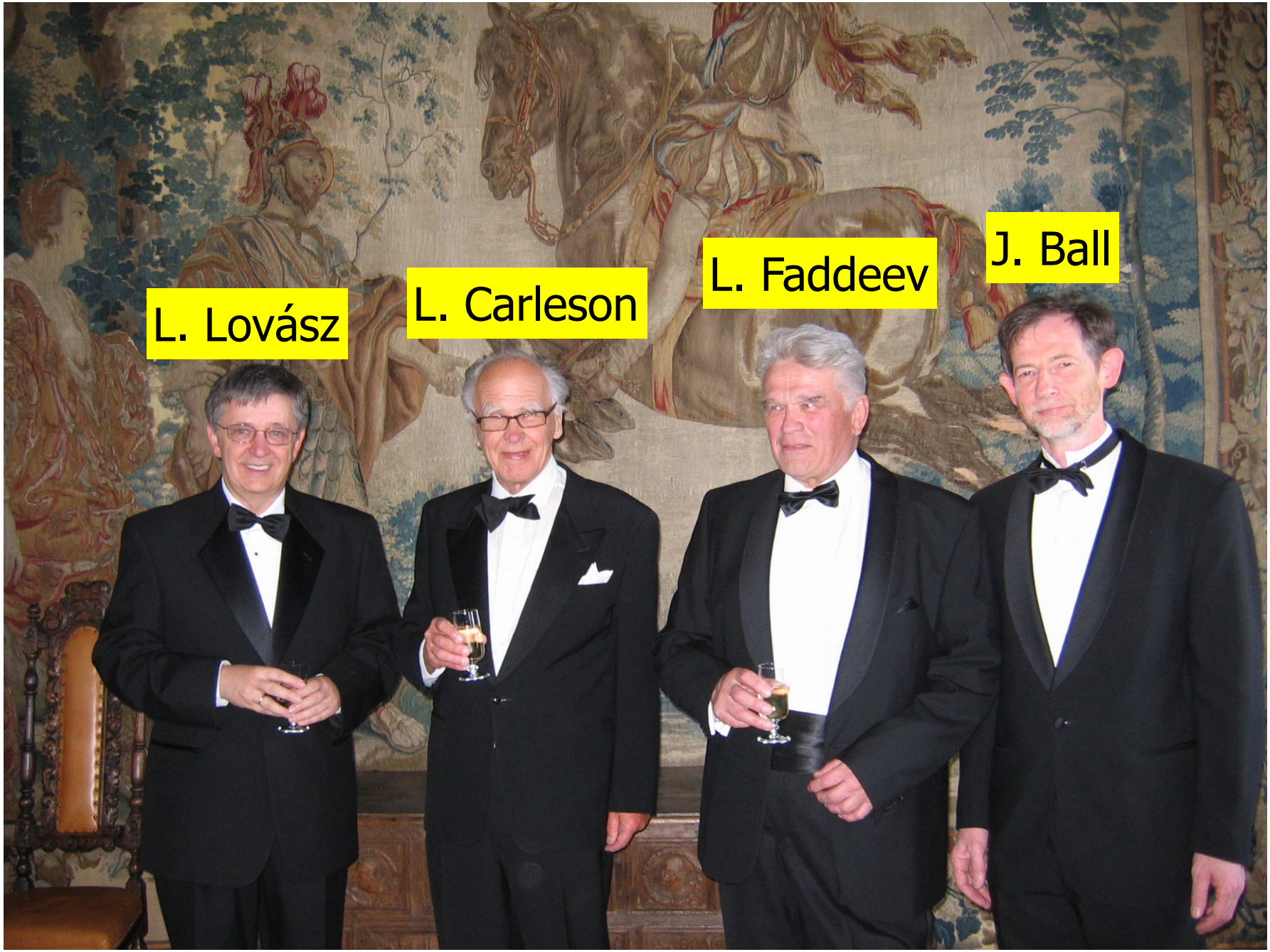
The Abel Committee consists of five outstanding research scientists in the field of mathematics appointed for a period of two years.

- Zwei der fünf Juroren werden von der IMU benannt.
- Das ist der Grund dafür, dass zu jeder Preisverleihung der IMU-Präsident und der IMU-Generalsekretär eingeladen werden.
- Gelegentlich nimmt das gesamte IMU Exekutivkomitee teil. So bekommt Günter Ziegler hoffentlich bald auch eine Einladung.

Vor dem „Dinner for Mathematicians“ 2007

Vor Schloss/Festung Akershus

Vier IMU-Präsidenten



Vor dem Bankett beim König im Rittersaal

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Die Preisverleihung und das Drumherum: Volles Programm

Monday:

11:00-12:00 The Holmboe Prize Ceremony (Oslo Cathedral School)

17:00-17:20 Wreath-Laying at the Abel Monument

18:00 Dinner for Mathematicians (Academy, by spec. invitation only)

Tuesday:

16:00 - 16:40 The Abel Prize Ceremony (University Aula)

19:00 The Norwegian Government's Abel Prize Banquet
(Akershus Castle, by special invitation only)

Wednesday

10:00 - 15:00 The Abel Lectures (Oslo University)

19:00 The Abel Party (Academy, by special invitation only)

Kranzniederlegung (am Montag)

Dinner for Mathematicians (Montagabend)

Einweihung der Abel-Gedenktafel am 6.4.2014

Am Kupfergraben 4, gegenüber dem Pergamon-Museum

Ergebnis des Treffens meiner Frau mit Arild Stubhaug beim Dinner for Mathematicians 2007 in der norwegischen Akademie.

Geflaggte Karl Johans gate

Anmarsch einer Musikkapelle

Die Bühne der Universitätsaula vor der Verleihung

Abel Preiszeremonie in der Universitätsaula

Im Rittersaal vor dem Bankett (Dienstagabend)

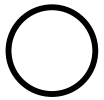
Eintreffen der Gäste im Bankettsaal

Srinivasan Varadan neben König Harald V.

Gliederung

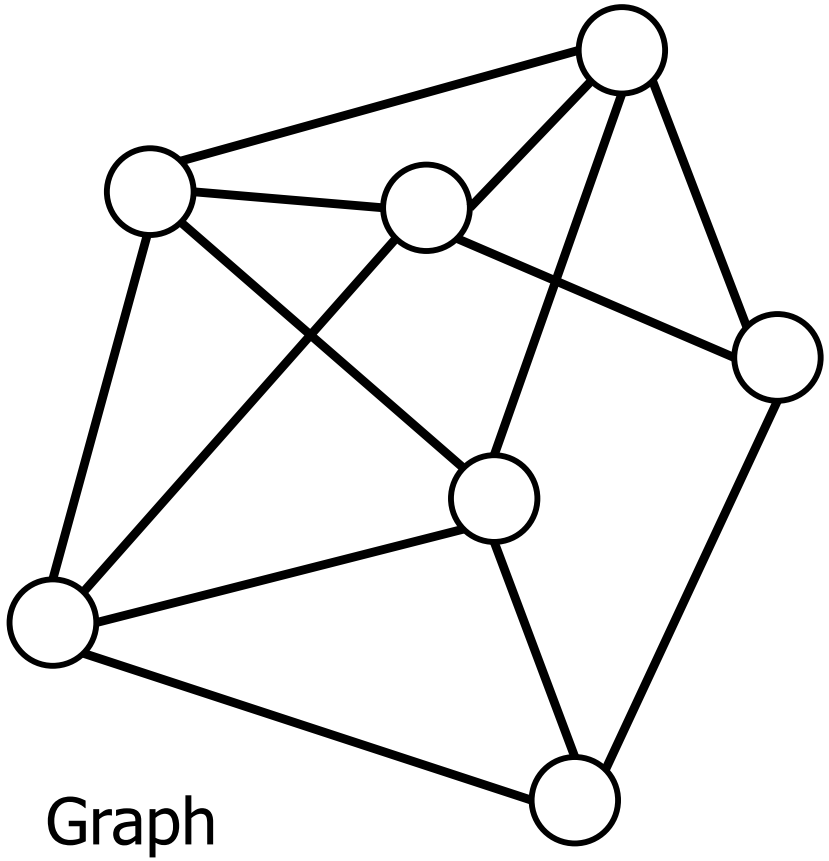
1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Graphen



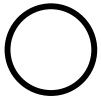
Knoten

Kante



Graph

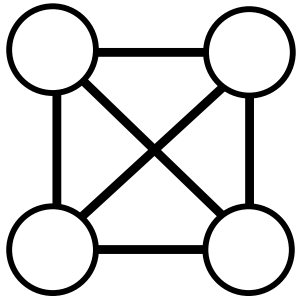
Graphen

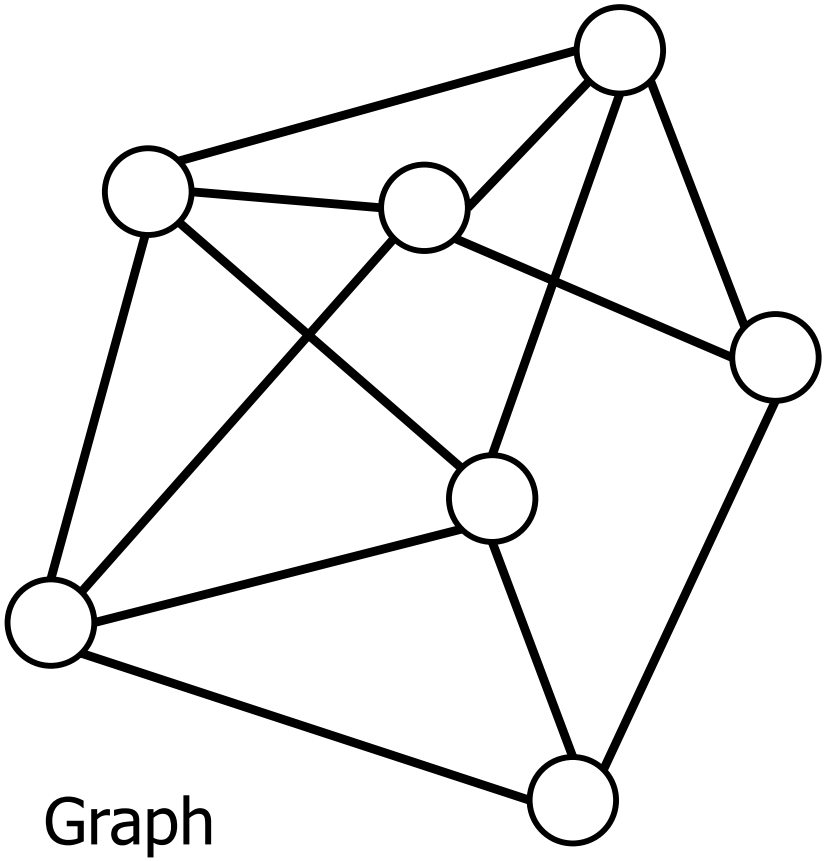


Knoten

Kante

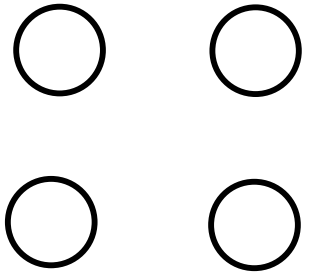
Clique

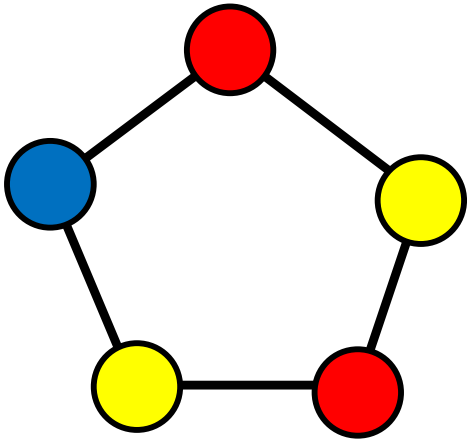




Graph

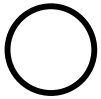
Stabile Menge





Knotenfärbung

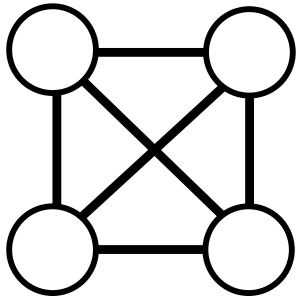
Graphen

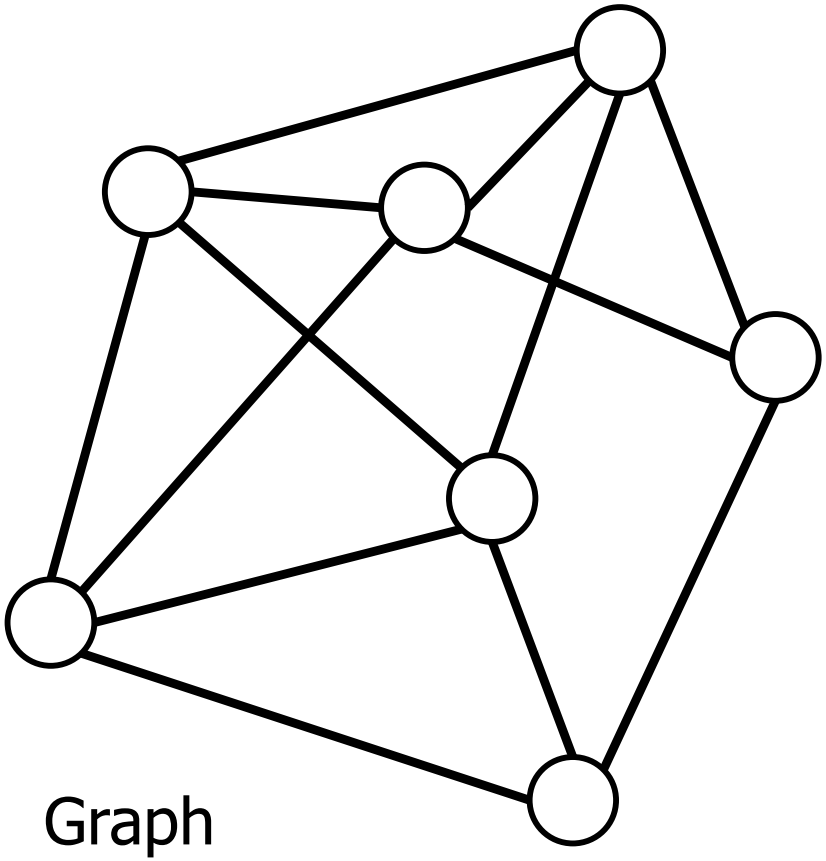


Knoten

Kante

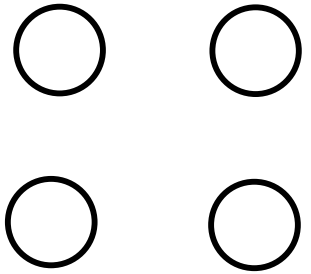
Clique

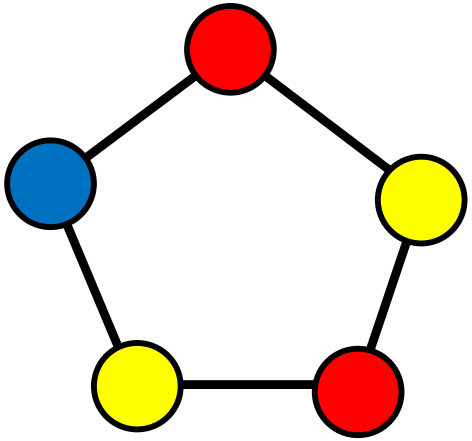




Graph

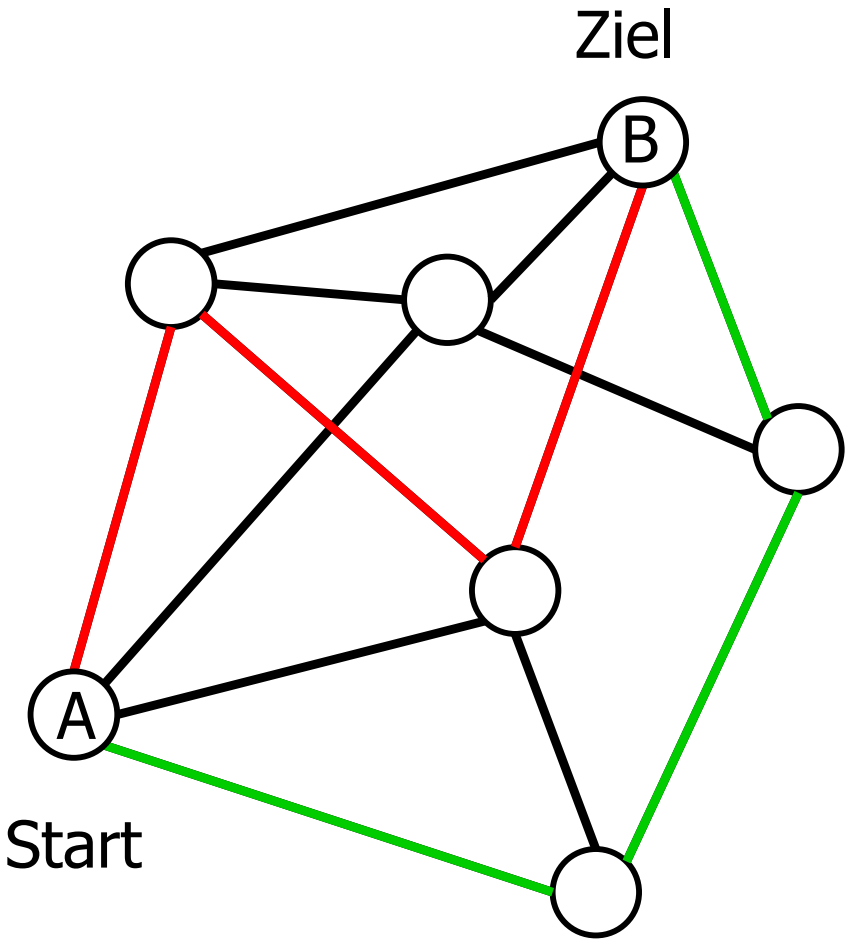
Stabile Menge

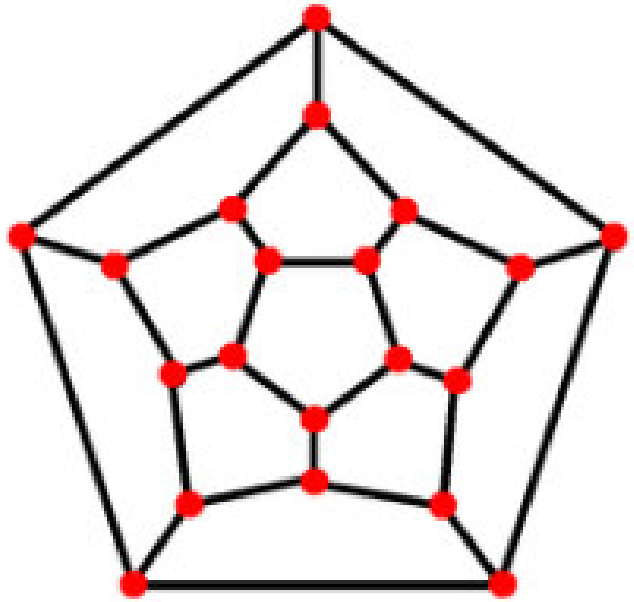


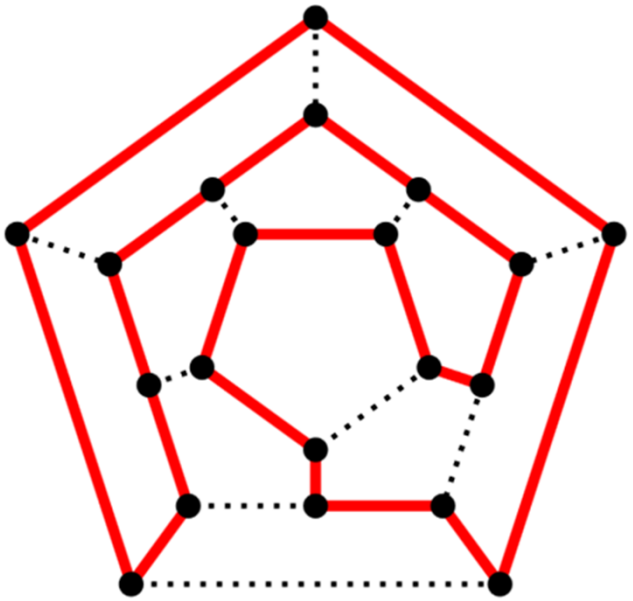


Knotenfärbung

Wege, Rundreisen







Komplexität in Informatik und Mathematik

- **Komplexität** bezeichnet in der Informatik die "Kompliziertheit" von mathematisch präzise definierten Problemen, Algorithmen oder Daten.
- Die **Komplexitätstheorie** befasst sich dabei mit dem Ressourcen-verbrauch von Algorithmen (z. B. Zeit- oder Speicheraufwand)

Für den heutigen Vortrag:

- Sei A ein Algorithmus, mit dem man ein Problem P lösen kann.
  - ➢ Beispiel: Algorithmus zur Berechnung eines kürzesten Weges in einem Fahrzeugnavigationssystem oder einer Rundreise in einem Graphen.
- Mit $\mathbf{l_A(n)}$ wird die **Laufzeit** bezeichnet, die der Algorithmus A zur Lösung eines Problems mit **Inputlänge n** benötigt.
- Ein Problem heißt **leicht**, wenn es einen Lösungsalgorithmus mit einer Laufzeit gibt, die durch ein Polynom p in n beschränkt ist ($\mathbf{l_A(n) \leq p(n)}$).
- Ein Problem heißt **schwer**, wenn …

Bezeichnungen

- $\mathcal{P}$ = Menge (Klasse) der leichten Probleme
- $\mathcal{NP}$ = Menge (Klasse) der schweren Probleme

Warnung!!!

Einem Problem sieht man nicht an, ob es einfach oder schwer ist.

Leicht:

- Berechnung eines kürzesten Weges
- Entscheidung, ob eine natürliche Zahl eine Primzahl ist

Schwer:

- Berechnung einer Rundreise
- Berechnung einer größten Clique
- Berechnung einer größten stabilen Menge
- Berechnung der Färbungszahl

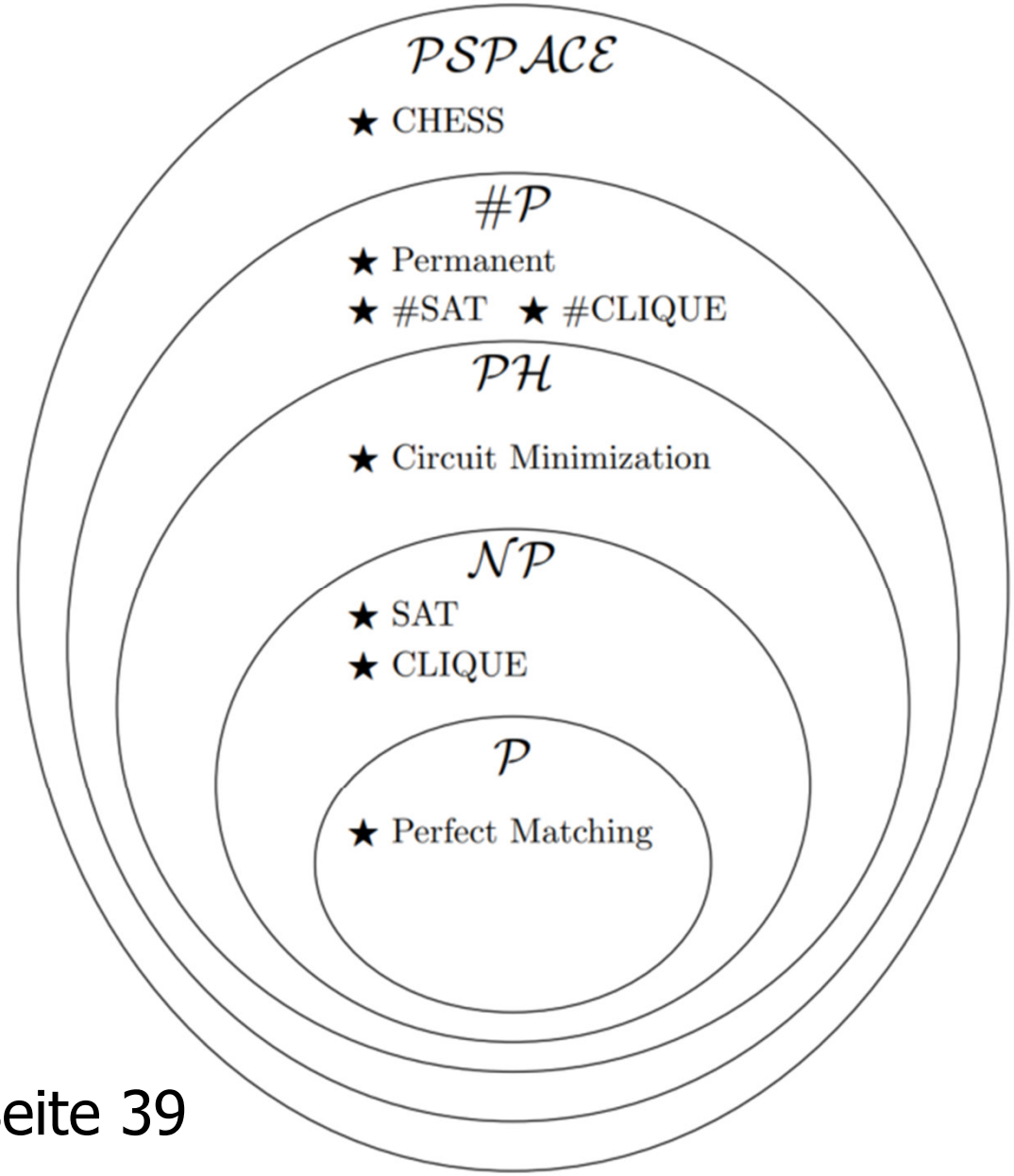
Unklar:

- Bestimmung der Primfaktoren einer zusammengesetzten Zahl
- Bestimmung des „kleinsten Chips" zur Berechnung einer Booleschen Funktion

Komplexitätstheorie

$\mathcal{P} = \mathcal{NP}$?

Ein Beispiel für eine Komplexitätsklassen-Hierarchie



Aus Wigderson, Seite 39

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Die Abel-Preisträger 2021

László Lovász

(Foto: Hungarian Academy of Sciences)

Avi Wigderson

(Foto: Andrea Kane/Institute for Advanced Study, Princeton, NJ, USA)

Würdigung beider Preisträger: Kurz-Statement

László Lovász (geb. 1948 in Budapest, Ungarn)

Alfréd Rényi Institute of Mathematics (ELKH, MTA Institute of Excellence) and Eötvös Loránd University, Hungary

Avi Wigderson (geb. 1956 in Haifa, Israel)

Institute for Advanced Study, Princeton, USA

"for their foundational contributions to theoretical computer science and discrete mathematics, and their leading role in shaping them into central fields of modern mathematics."

László Lovász (geb. 1948)

- 1964-1966: 3 Goldmedaillen bei der Internationalen Mathematik-Olympiade
- 1964: Gewinner einer Mathematik-Show im ungarischen Fernsehen
- 1967: Resultate über Homomorphismen von Strukturen
- 1970: Promotion (bereits 15 veröffentlichte Artikel)
- 1970: Das (f,g)-Faktor-Theorem der Matching-Theorie
- 1972: Das Perfekte-Graphen-Theorem (das werde ich erklären)
- 1975: Lovász-Local-Lemma über Zufallsgraphen
- 1978: Kneser-Vermutung in der Graphentheorie mit Methoden der algebraischen Topologie bewiesen
- 1979: Wichtiger Betrag zur Shannon-Kapazität in der Informationstheorie
- 1979-1987: Konsequenzen der Ellipsoid-Methode (semidefinite Optimierung, submodulare Funktionen,…) mit vielen praktischen Anwendungen
- 1982: LLL-Algorithmus mit Anwendungen in der Algebra, Zahlentheorie, Kryptographie (werde ich erwähnen)
- …
- 2012: Large Networks and Graph Limits (Graphons)
- …

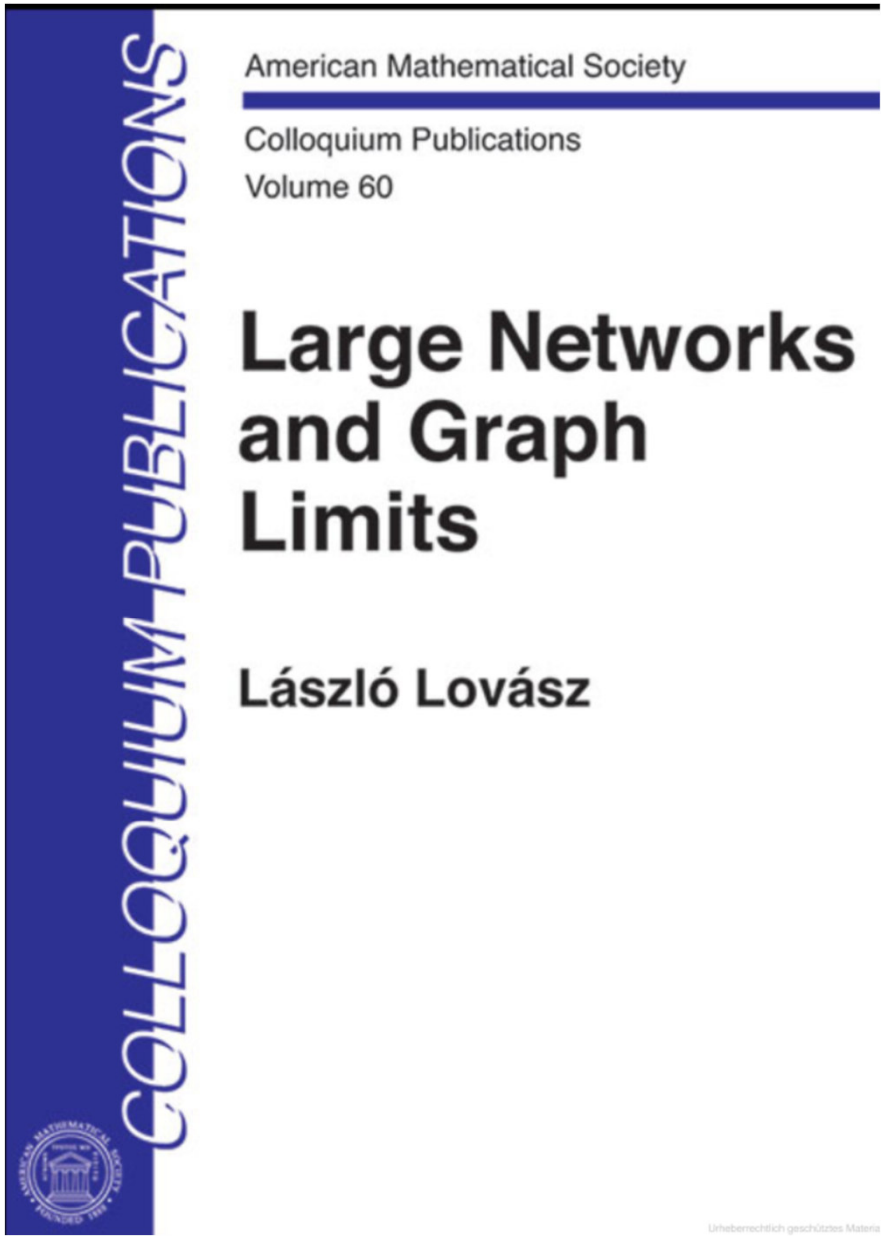
Riesige Graphen

Beispiele riesiger Netzwerken:

- Das Internet
- Soziale Netzwerke
- Ökologische & ökonomische Netzwerke
- Das Gehirn
- Chemische und biologische Cluster
- Computer Chip
- Das Universum

Viele Fragestellungen der „alten Graphen-theorie" sind bei riesigen Netzwerken sinnlos. Was sind die neuen Themen?

- Wie erhalte ich Information? Sampling!
- Globale und lokale Eigenschaften?
- Testen von Eigenschaften
- Konvergenz von Graphenfolgen
- Entwicklung wachsender Zufallsgraphen
- Regularitätseigenschaften
- Approximation solcher Graphen

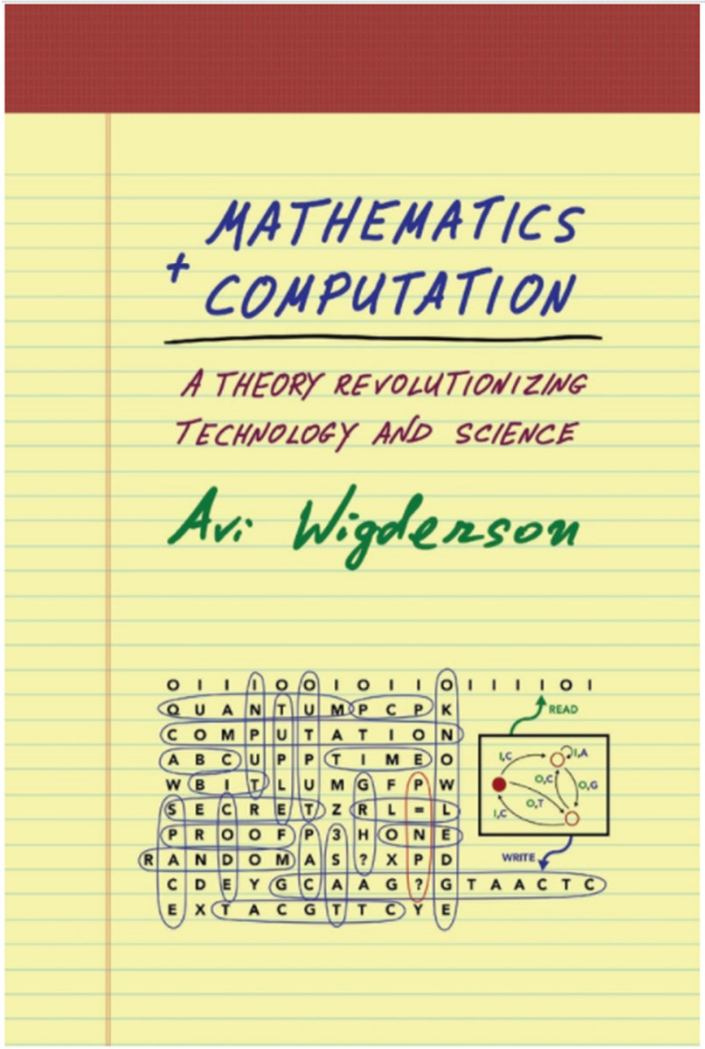


Avi Wigderson (geb. 1956)

- Komplexitätstheorie (speziell P = NP?)
- Komplexitätshierarchien (P=BPP Theorem werde ich andeuten)
- Rolle des Zufalls bei der Beschleunigung von Algorithmen
- Derandomisierung von Zufallsalgorithmen
- Zig-Zag Graph Product: Verbindung zwischen Graphen-, Gruppen- und Komplexitätstheorie
- Kryptographie / sichere Datenübertragung
- Zero-Knowledge-Proofs (das werde ich erklären) mit Anwendungen z. B. in der Block-Chain-Technologie
- …

Das derzeit umfassendste Buch zum Thema Komplexität in Mathematik und Informatik

book: math and computation



This is a final draft of a book that has been published by Princeton University Press.

Feel free to download if you will use it for your personal research and education needs.

Comments are welcome!

Mathematics and Computation (version 8/6/2019)

The publisher's cover page of the book, with description and reviews is here.

Previous Versions:

Draft from 3/25/2019 is available **here**
Draft from 3/27/2018 is available **here**

https://www.math.ias.edu/avi/book
Das Buch ist kostenlos online verfügbar.

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

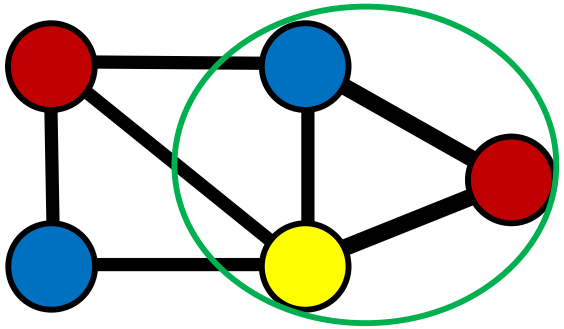
Perfekte Graphen

Die **Cliquenzahl** ist die Anzahl der Knoten einer größten Clique.

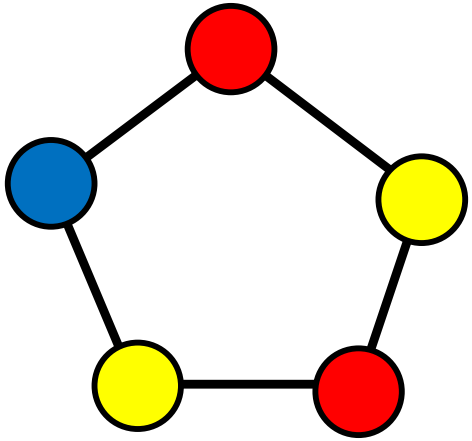
Die **Färbungszahl** ist die kleinste Anzahl von Farben, mit denen die Knoten so gefärbt werden können, dass je zwei benachbarte Knoten verschiedene Farben besitzen.

Beobachtung: Die Färbungszahl ist nie kleiner als die Cliquenzahl, da alle Knoten einer Clique verschiedene Farben haben müssen.

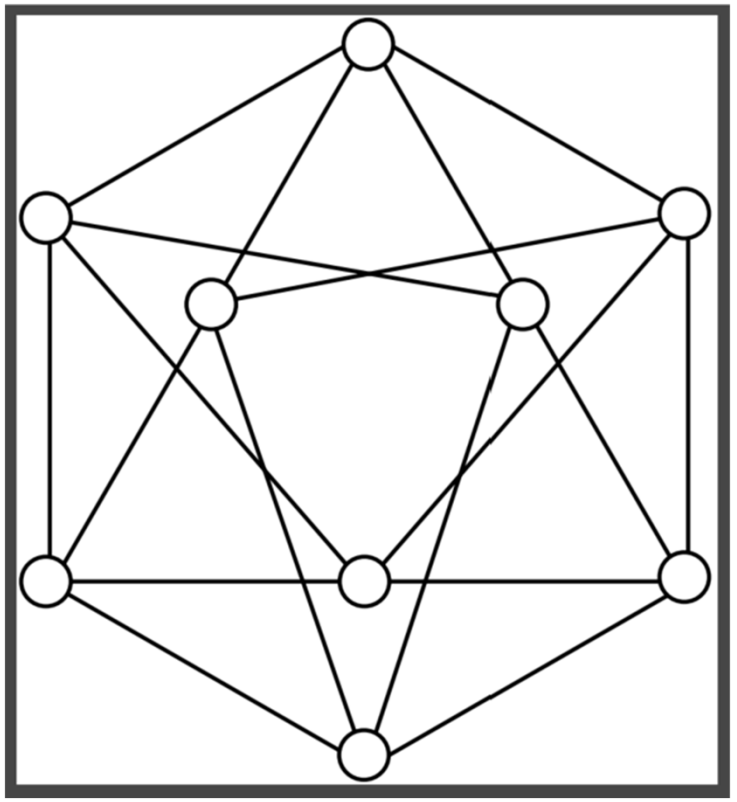
Definition: Ein Graph G=(V,E) heißt **perfekt**, wenn für G und jeden Teilgraphen von G, der durch Löschen von Knoten und die mit diesen Knoten verbundenen Kanten entsteht, die Färbungszahl und die Cliquenzahl übereinstimmen.



Perfekte und imperfekte Graphen



Der kleinste imperfekte Graph mit der Eigenschaft, dass jedes Entfernen oder Hinzufügen einer Kante einen perfekten Graphen ergibt.



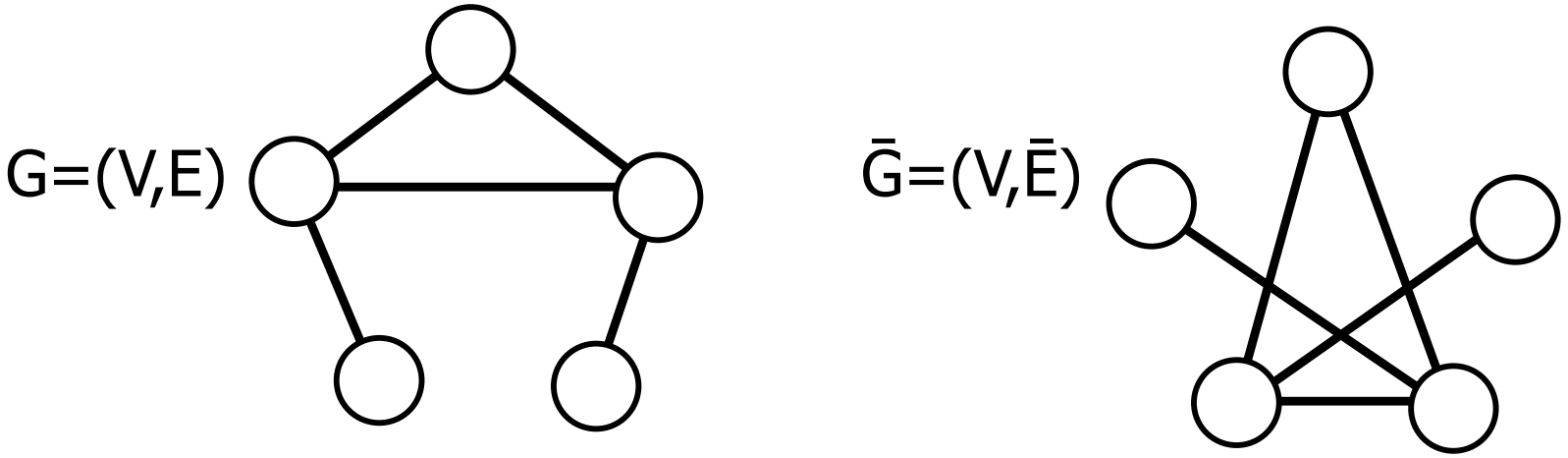
Der kleinste perfekte Graph mit der Eigenschaft, dass jedes Entfernen oder Hinzufügen einer Kante einen imperfekten Graphen ergibt.

Eine Liste perfekter Graphen (Wikipedia)

- Bipartite graphs, which are graphs that can be colored with two colors, including forests (graphs without cycles).
- Line graphs of bipartite graphs (see Kőnig's theorem). Rook's graphs (line graphs of complete bipartite graphs) are a special case.
- Chordal graphs, the graphs in which every cycle of four or more vertices has a *chord*, an edge between two vertices that are not consecutive in the cycle. These include
  - forests, *k*-trees (maximal graphs with a given treewidth),
  - split graphs (graphs that can be partitioned into a clique and an independent set),
  - block graphs (graphs in which every biconnected component is a clique),
  - Ptolemaic graphs (graphs whose distances obey Ptolemy's inequality),
  - interval graphs (graphs in which each vertex represents an interval of a line and each edge represents a nonempty intersection between two intervals),
  - trivially perfect graphs (interval graphs for nested intervals), threshold graphs (graphs in which two vertices are adjacent when their total weight exceeds a numerical threshold),
  - windmill graphs (formed by joining equal cliques at a common vertex),
  - and strongly chordal graphs (chordal graphs in which every even cycle of length six or more has an odd chord).
- Comparability graphs formed from partially ordered sets by connecting pairs of elements by an edge whenever they are related in the partial order. These include:
  - bipartite graphs, complements of interval graphs, trivially perfect graphs, threshold graphs, windmill graphs,
  - permutation graphs (graphs in which the edges represent pairs of elements that are reversed by a permutation),
  - and cographs (graphs formed by recursive operations of disjoint union and complementation).
- Perfectly orderable graphs, which are graphs that can be ordered in such a way that a greedy coloring algorithm is optimal on every induced subgraph. These include the bipartite graphs, the chordal graphs, the comparability graphs,
  - distance-hereditary graphs (in which shortest path distances in connected induced subgraphs equal those in the whole graph),
  - and wheel graphs with an odd number of vertices.
- Trapezoid graphs, which are intersection graphs of trapezoids whose parallel pairs of edges lie on two parallel lines. These include the interval graphs, trivially perfect graphs, threshold graphs, windmill graphs, and permutation graphs; their complements are a subset of the comparability graphs.

Perfekte Graphen und Komplementbildung

Im Komplementgraphen $\bar{G}=(V,\bar{E})$ eines Graphen $G=(V,E)$ sind zwei Knoten genau dann mit einer Kanten verbunden, wenn sie in G nicht durch eine Kante verbunden sind.



Das **Perfekte-Graphen-Theorem** von Lovász:

> Ein Graph $G=(V,E)$ ist genau dann perfekt,
> wenn sein Komplement $\bar{G}=(V,\bar{E})$ perfekt ist.

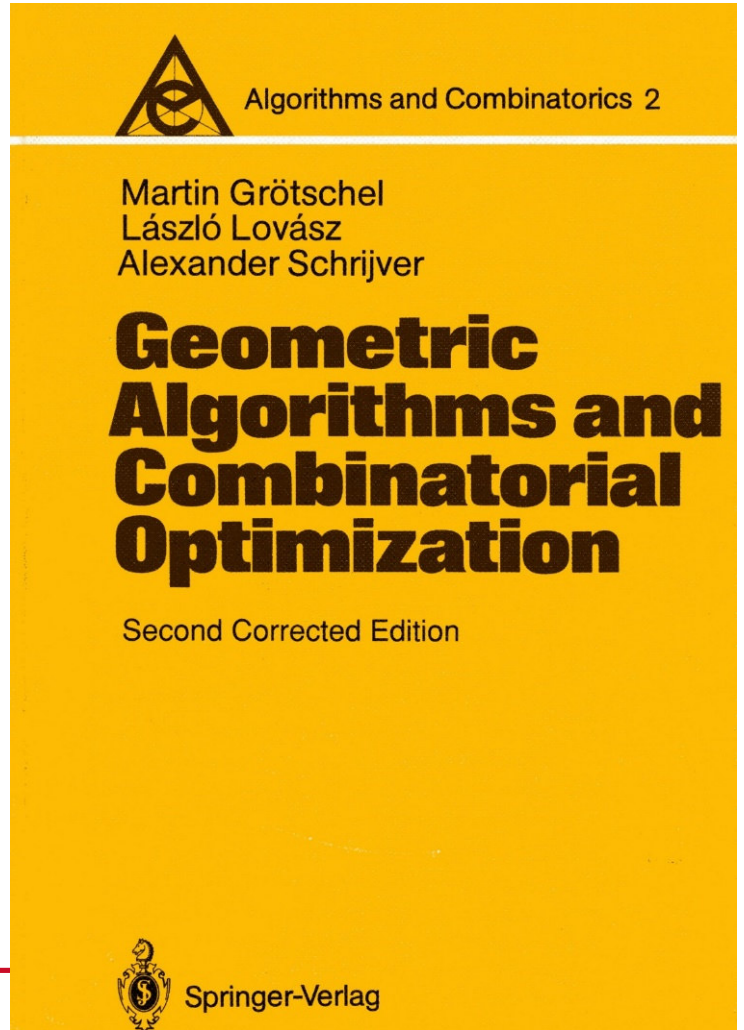
Schnelle Algorithmen für perfekte Graphen?

In perfekten Graphen hängen die algorithmisch schwierigen Probleme „Berechnung einer größten Clique oder stabilen Menge, der Färbungszahl oder Cliqenüberdeckungszahl“ eng zusammen.

Kann es sein, dass diese grundsätzlich schwierigen Probleme für perfekte Graphen leicht sind?

In der Tat, der Nachweis gelang durch Untersuchung des Stabile Mengen-Problems, eine verblüffende Idee von Lovász und die Verallgemeinerung der Ellipsoidmethode.

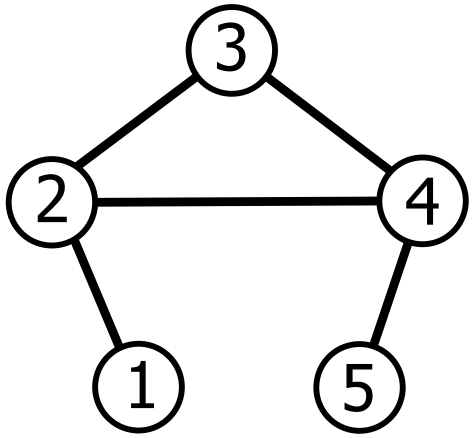
Eine ausführliche Darstellung findet sich in dem Buch rechts.



Skizze der Idee

1. Wir verwandeln jede stabile Knotenmenge eines Graphen G=(V,E) in einen Vektor im Vektorraum $\mathbb{R}^V$.

Von stabilen Mengen zu Vektoren
von der Graphentheorie zur Geometrie



Stabile Mengen: leere Menge, {1},{2},{3},{4},{5},
{1,3},{1,4},{2,5},{3,5},{1,3,5}

Überführung dieser in 0/1-Vektoren
(Inzidenzvektoren) im 5-dimensionalen Raum

leere Menge, {1},{2},{3},{4},{5},{1,3}, {1,4},{2,5},{3,5},{1,3,5}

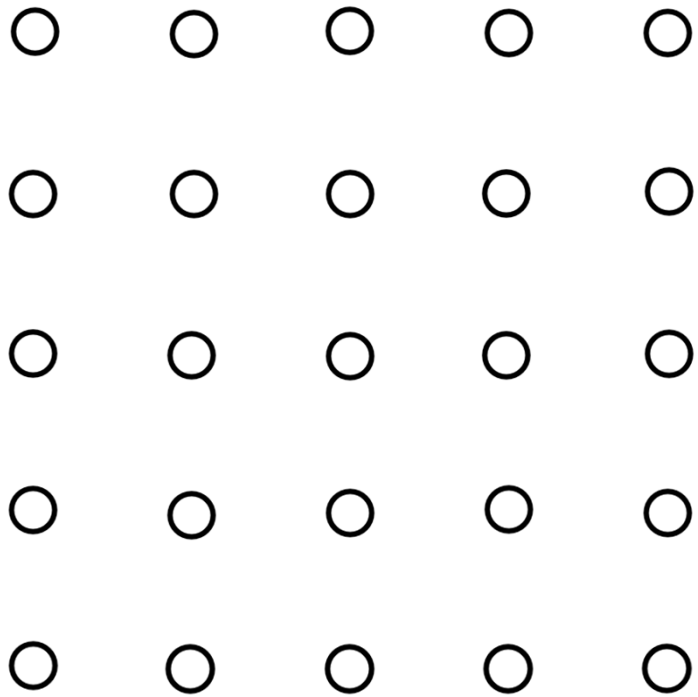
Kno-ten											
1	0	1	0	0	0	0	1	1	0	0	1
2	0	0	1	0	0	0	0	0	1	0	0
3	0	0	0	1	0	0	1	0	0	1	1
4	0	0	0	0	1	0	0	1	0	0	0
5	0	0	0	0	0	1	0	0	1	1	1

Skizze der Idee

1. Wir verwandeln jede stabile Knotenmenge eines Graphen G=(V,E) in ihren Inzidenzvektor im Vektorraum $\mathbb{R}^V$.
2. Wir bezeichnen die konvexe Hülle dieser Vektoren als STAB(G). STAB(G) ist ein Polyeder.
3. Wir untersuchen die LP-Relaxierung QSTAB(G) von STAB(G). QSTAB(G) ist ebenfalls ein Polyeder.

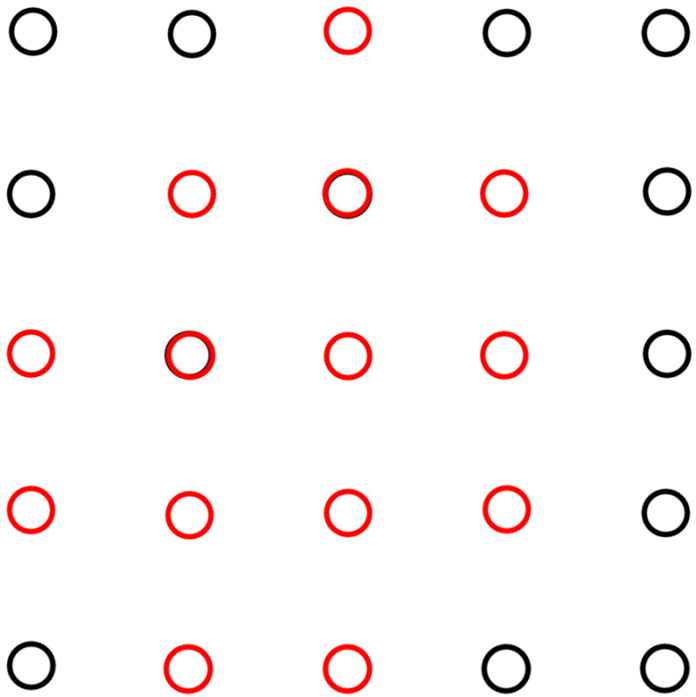
Die Konvexifizierung des Stabile-Mengen-Problems

Wir stellen uns vor, dass dies Punkte
in einem hochdimensionalen Raum sind.



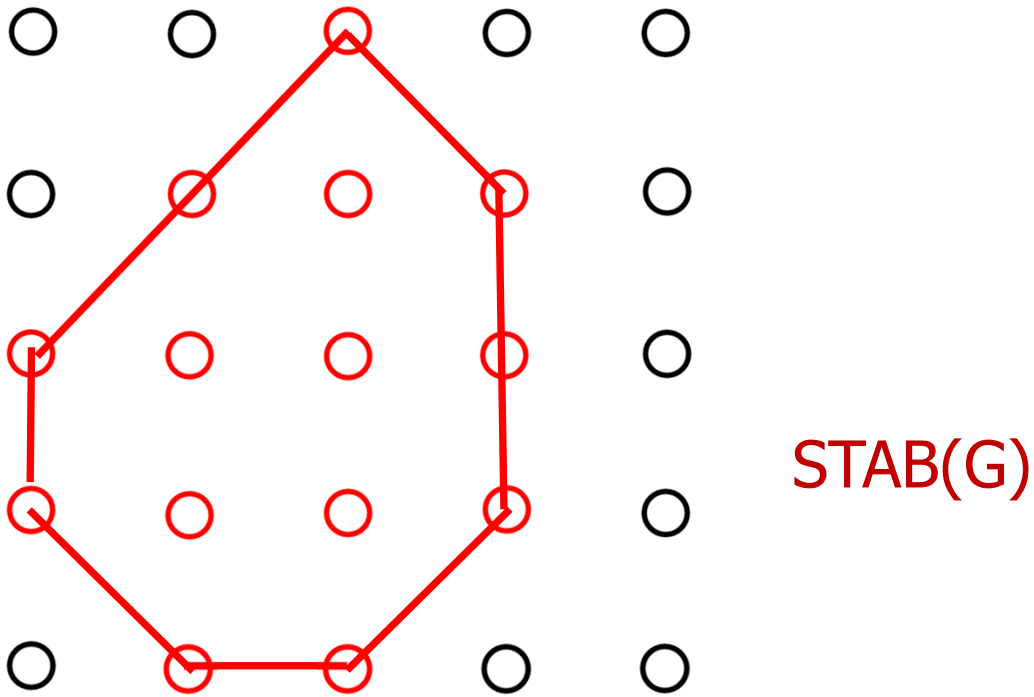
Die Konvexifizierung des Stabile-Mengen-Problems

Uns interessieren die roten Punkte. Diese symbolisieren die Inzidenzvektoren der stabilen Mengen.



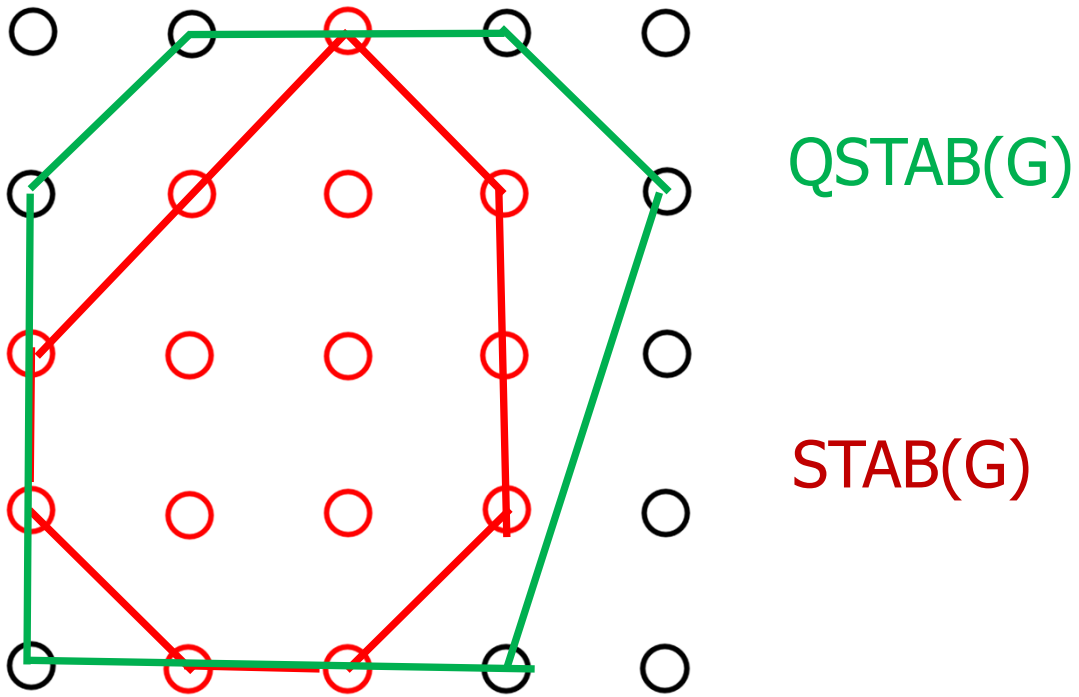
Die Konvexifizierung des Stabile-Mengen-Problems

Wir berechnen die Konvexkombination STAB(G) der roten Punkte.
Dies geht theoretisch. In der Praxis können wir das nicht.



Die Konvexifizierung des Stabile-Mengen-Problems

Wir erfinden Ungleichungen, deren Durchschnitt QSTAB(G)
die Konvexkombination STAB(G) der roten Punkte enthält
Das schafft man auch in der Praxis.



Skizze der Idee

1. Wir verwandeln jede stabile Knotenmenge eines Graphen G=(V,E) in ihren Inzidenzvektor im Vektorraum $\mathbb{R}^V$.
2. Wir bezeichnen die konvexe Hülle dieser Vektoren als STAB(G).
3. Wir untersuchen die LP-Relaxierung QSTAB(G) von STAB(G).
4. Wir müssen leider feststellen, dass für allgemeine Graphen die Lösung von Optimierungsproblemen über STAB(G) und QSTAB(G) schwer ist. Was nun?

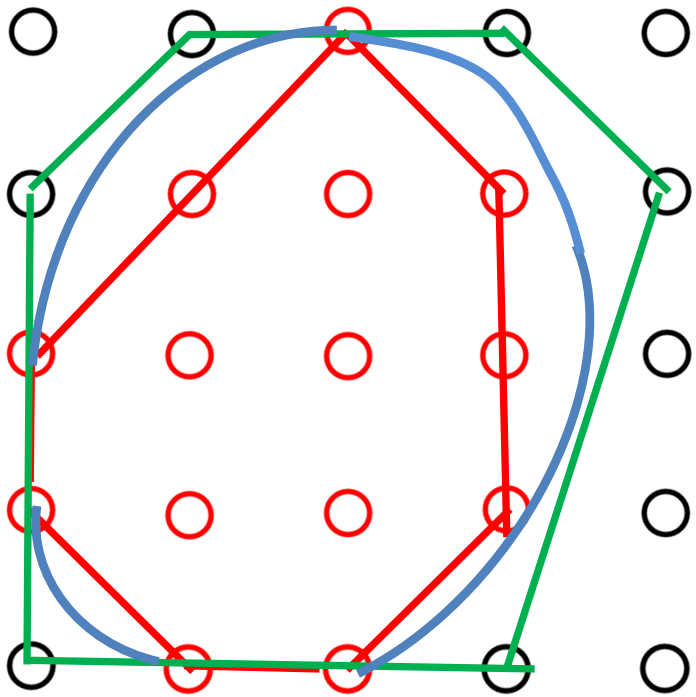
Skizze der Idee

1. Wir verwandeln jede stabile Knotenmenge eines Graphen G=(V,E) in ihren Inzidenzvektor im Vektorraum $\mathbb{R}^V$.
2. Wir bezeichnen die konvexe Hülle dieser Vektoren als STAB(G).
3. Wir untersuchen die LP-Relaxierung QSTAB(G) von STAB(G).
4. Wir müssen leider feststellen, dass für allgemeine Graphen die Lösung von Optimierungsproblemen über STAB(G) und QSTAB(G) schwer ist. Was nun?

5. Lovász hat in der Informationstheorie zur Charakterisierung der Shannon-Kapazität die theta-Funktion eingeführt und wichtige Sachverhalte bewiesen.
   Diese Funktion kann benutzt werden, um für jeden Graphen G eine neue konvexe Menge, genannt TH(G), zu definieren, welche die folgende Eigenschaft hat:
   $STAB(G) \subset TH(G) \subset QSTAB(G)$

Die Konvexifizierung des Stabile-Mengen-Problems

Die von der blauen Linie umrandete Menge deutet die von Lovász eingeführte konvexe Menge TH(G) an.



$$\mathrm{TH}(G) = \{\, x \in \mathbb{R}^V_+ \mid x^T y \le \vartheta(G,y) \ \textit{for all}\ y \in \mathbb{R}^V_+ \,\}$$

Verblüffende Ergebnisse

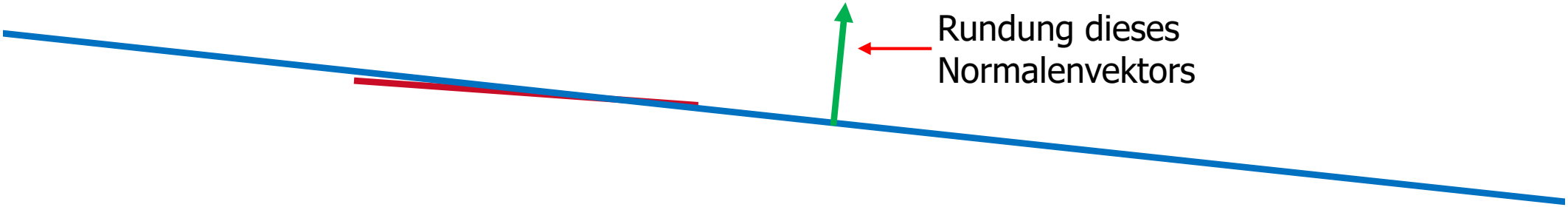
Theorem: Obwohl zur Beschreibung von TH(G) durch lineare Ungleichungen beweisbar unendlich viele Ungleichungen erforderlich sind, kann man über TH(G) in polynomialer Zeit optimieren.

Theorem: Ein Graph ist genau dann perfekt, wenn gilt: STAB(G)=TH(G)=QSTAB(G).

Folgerung: Die Berechnung der Färbungszahl, Cliquenzahl und Stabile-Mengen-Zahl ist für perfekte Graphen leicht.

Eine „Trivialität“ mit weitreichenden Konsequenzen

Bei unserer Beschäftigung mit der Verallgemeinerung der Ellipsoidmethode war es notwendig, Hyperebenen zu finden, die eine durch ein Orakel gegebene konvexe Menge enthalten.



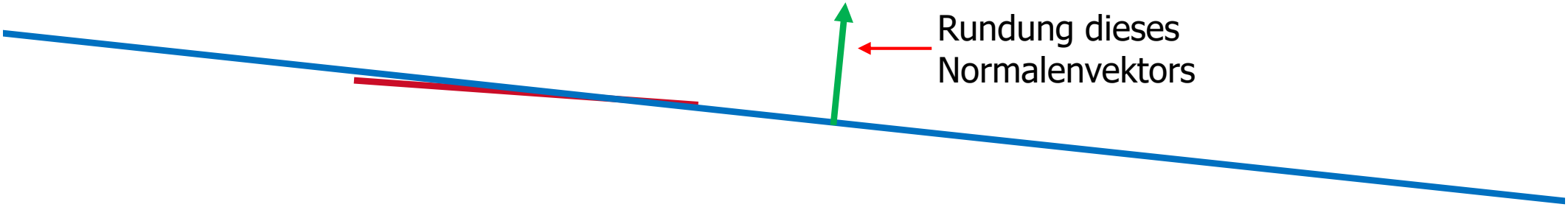
Lovász, Schrijver und ich konnten das Problem auf ein mehrdimensionales „simultanes Rundungsproblem“ reduzieren (technisch heißt das simultane diophantische Approximation).

Uns gelang es bei unserem Treffen im September 1981 nicht, einen schnellen Algorithmus dafür zu erfinden.

Drei Monate später bekam ich den folgenden Brief:

Eine „Trivialität“ mit weitreichenden Konsequenzen

Bei unserer Beschäftigung mit der Verallgemeinerung der Ellipsoidmethode war es notwendig, Hyperebenen zu finden, die eine durch ein Orakel gegebene konvexe Menge enthalten.

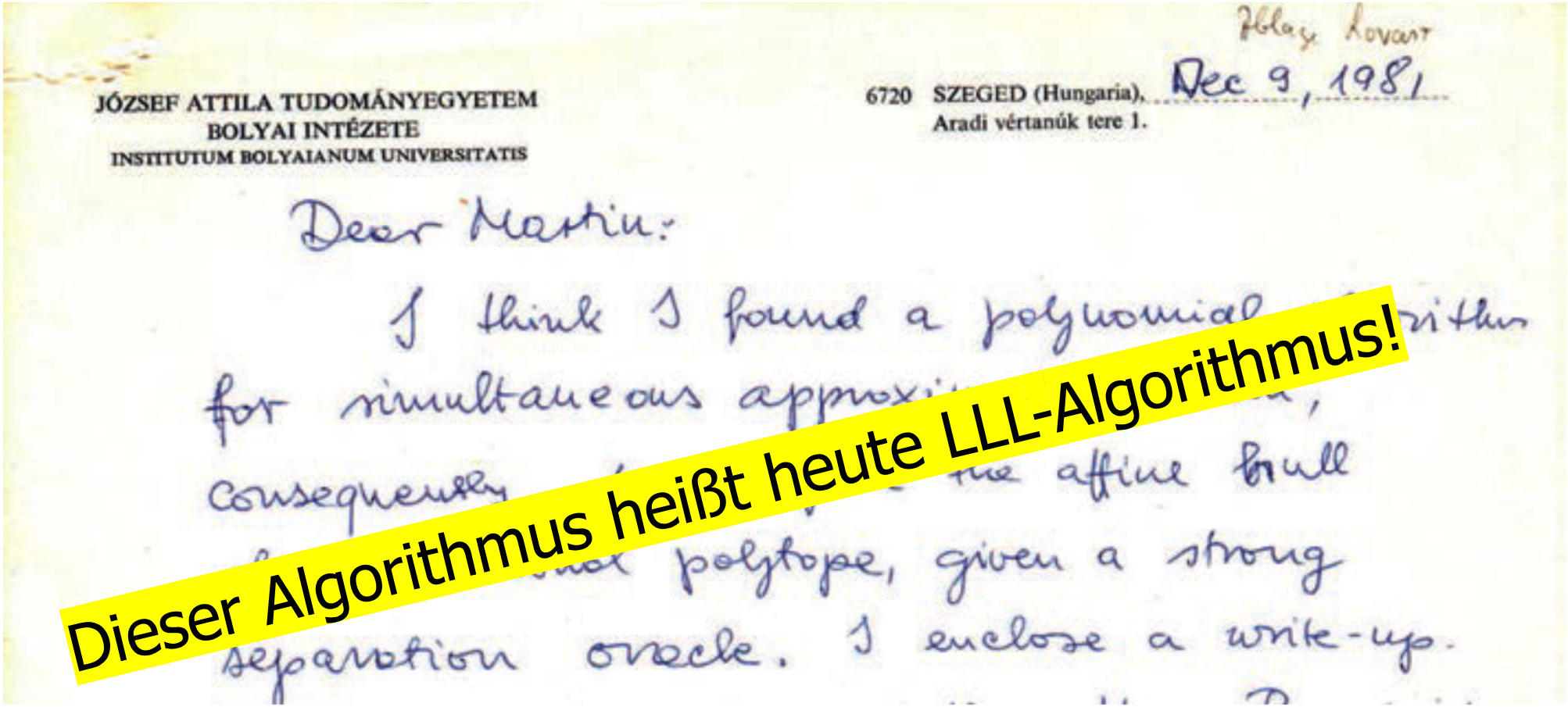


Lovász, Schrijver und ich konnten das Problem auf ein mehrdimensionales „simultanes Rundungsproblem“ reduzieren (technisch heißt das simultane diophantische Approximation).

Uns gelang es bei unserem Treffen im September 1981 nicht, einen schnellen Algorithmus dafür zu erfinden.

Drei Monate später bekam ich den folgenden Brief:

Brief von L. Lovász am 9.12.1981



Laszlo Lovasz

JÓZSEF ATTILA TUDOMÁNYEGYETEM
BOLYAI INTÉZETE
INSTITUTUM BOLYAIANUM UNIVERSITATIS

6720 SZEGED (Hungaria), Dec 9, 1981
Aradi vértanúk tere 1.

Dear Martin:

I think I found a polynomial ...rithm
for simultaneous approxi...,
consequently ... the affine hull
... polytope, given a strong
separation oracle. I enclose a write-up.

Dieser Algorithmus heißt heute LLL-Algorithmus!

Methode: Berechnung einer reduzierten Gitterbasis (Verwendung von Algebra, und Zahlentheorie).

Damit konnte die gewünschte Rundung berechnet werden, was zu einem polynomialen Algorithmus zur Bestimmung der affinen Hülle eines Polyeders geführt hat.

Bedeutende Anwendungen des LLL-Algorithmus

A. K. Lenstra, H. W. Lenstra, Jr., L. Lovász: *Factoring polynomials with rational coefficients*. In: Mathematische Annalen. Band 261, Nr. 4, 1982, S. 515–534, doi:10.1007/BF01457454
Zitat: In this paper we present a polynomial-time algorithm to solve the following problem: given a non-zero polynomial f ε Q(X) in one variable with rational coefficients, find the decomposition of f into irreducible factors in Q(X).

Beispiel: $6x^3+23x^2-6x-8= (3x-2)(2x+1)(x+4)$

Hunderte von anderen Anwendungen in Algebra, Zahlentheorie, Informatik,...:

- A. M. Odlyzko, H. J. J. te Riele: *Disproof of the Mertens conjecture*
- William R. Unger: *Computing the character table of a finite group*
- D. Simon: *Selected applications of LLL in number theory*
- Oded Regev: *Lattices in Computer Science: LLL Algorithm*
- C.P. Schnorr: *Gitter und Kryptographie*

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Beweise

Leider werden in Schulen heutzutage Beweise nicht mehr gelehrt, obwohl sie das Herz der Mathematik sind.

Als Aufwärmübung führe ich einen berühmten Beweis vor.

Primzahlen sind natürliche Zahlen >1, die nur durch 1 und sich selbst teilbar sind.

Theorem: Es gibt unendlich viele Primzahlen.

Beweis: Die Griechen wussten schon: Jede natürlich Zahl n ist als Produkt von Primzahlen eindeutig darstellbar, d.h. $n=p_1 \bullet p_2 \bullet \ldots \bullet p_k$.

- Angenommen, es gibt nur endlich viele Primzahlen $p_1,p_2,\ldots,p_r$.
- Definiere ihr Produkt: $z=p_1 \bullet p_2 \bullet \ldots \bullet p_r$.
- Offensichtlich: Keine Zahl >1 teilt gleichzeitig eine Zahl x und x+1.
- Folglich teilt keine der Primzahlen $p_1,p_2,\ldots,p_r$ die Zahl z+1.
- Daraus schließen wir, dass z+1 eine Primzahl sein muss. Und somit ist die Annahme falsch, dass es nur endlich viele Primzahlen gibt.

Kryptographie

- Die Entscheidung, ob eine natürliche Zahl eine Primzahl ist oder nicht, ist leicht.
- Wenn eine natürliche Zahl z keine Primzahl ist, so ist derzeit unbekannt, ob man die Primfaktorzerlegung von z in polynomialer Zeit berechnen kann.
- In der Praxis ist die Aufgabe schwer!

- Auf dieser Erfahrungstatsache, die theoretisch nicht bewiesen ist, basieren heute fast alle in der Praxis verwendeten Kryptosysteme.
- Primzahlen spielen also eine große Rolle in Sicherheitsfragen.

Zero-Knowledge-Proofs (Null-Wissen-Beweis, kenntnisfreier Beweis)

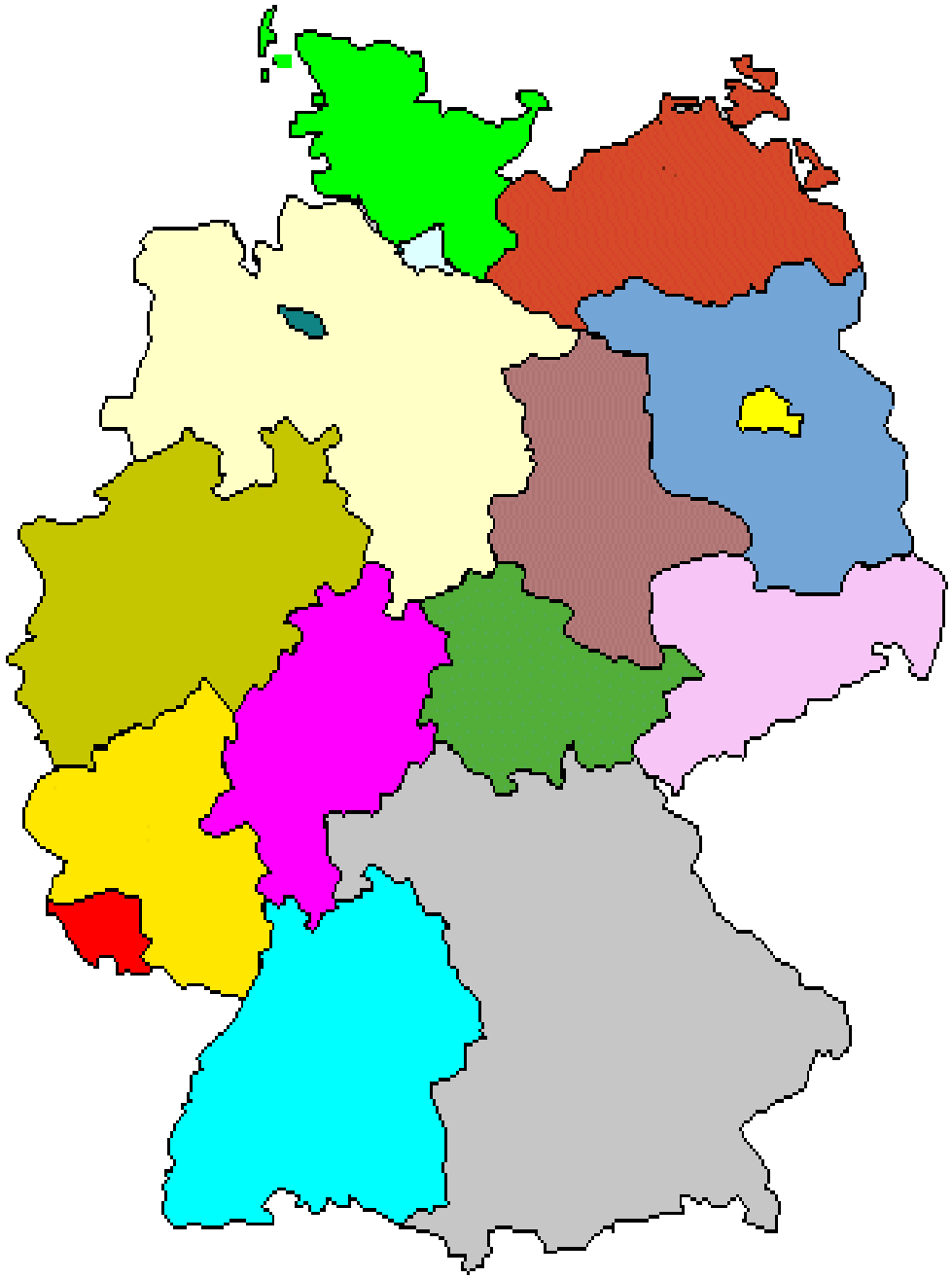
Ich erläutere jetzt ein Gebiet, zu dem Avi Widgerson maßgebliche Beiträge geleistet hat und das bei sicherheitsrelevanten Aktivitäten (z. B. in der Kryptographie) in Zukunft von großer Bedeutung sein wird. Ich erkläre das im Rahmen des folgenden Szenarios:

Ein **Beweiser** (namens **B**) hat Kenntnis über einen Sachverhalt (ein Geheimnis) und will einen **Verifizierer** (**V**) davon überzeugen, dass er das Geheimnis kennt, ohne das Geheimnis selbst zu verraten.

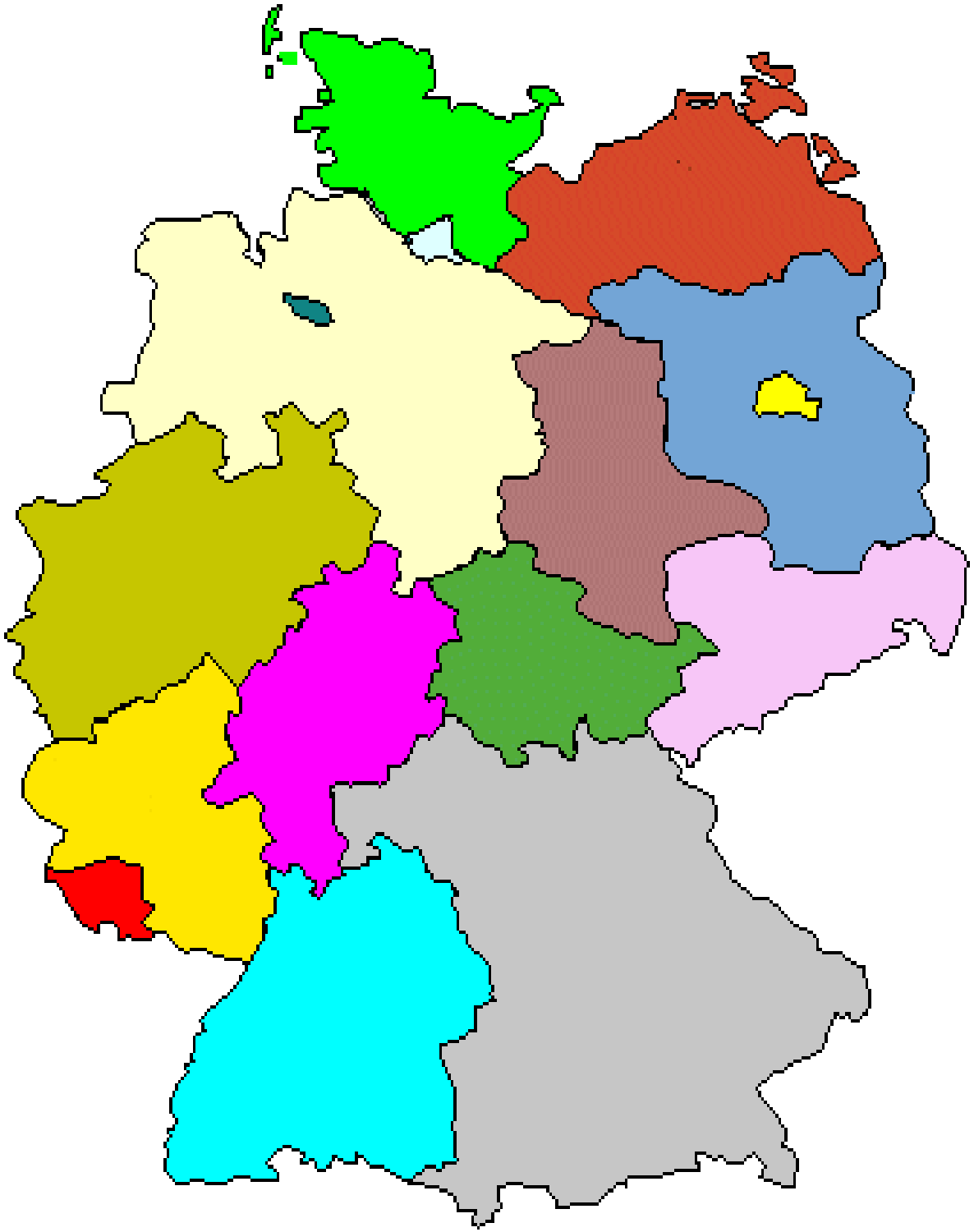
Der Überzeugungsvorgang verläuft **interaktiv**. Bei jedem Schritt wird die Wahrscheinlichkeit für den Verifizierer größer, dass B das Geheimnis tatsächlich kennt. V beendet die Interaktion, wenn er keine Zweifel mehr hat, obwohl er keine Information über das Geheimnis erhalten hat.

Ich erläutere die Beweistechnik anhand des Knotenfärbungsproblems in der Graphentheorie.

Zwei Deutschland-Karten



16 Farben
+ Umgebung



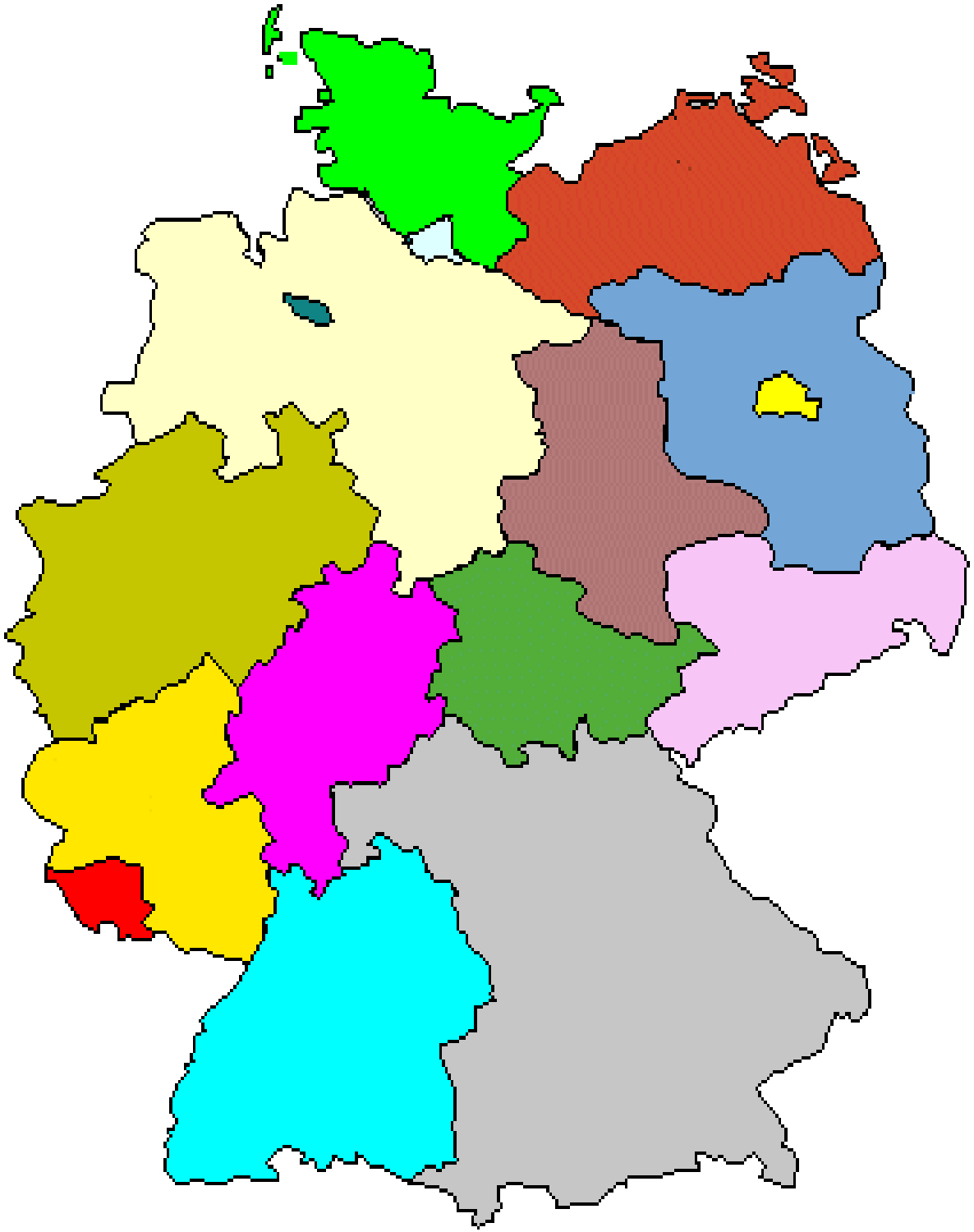
Die Bundesländer

16 Farben

+ Umgebung

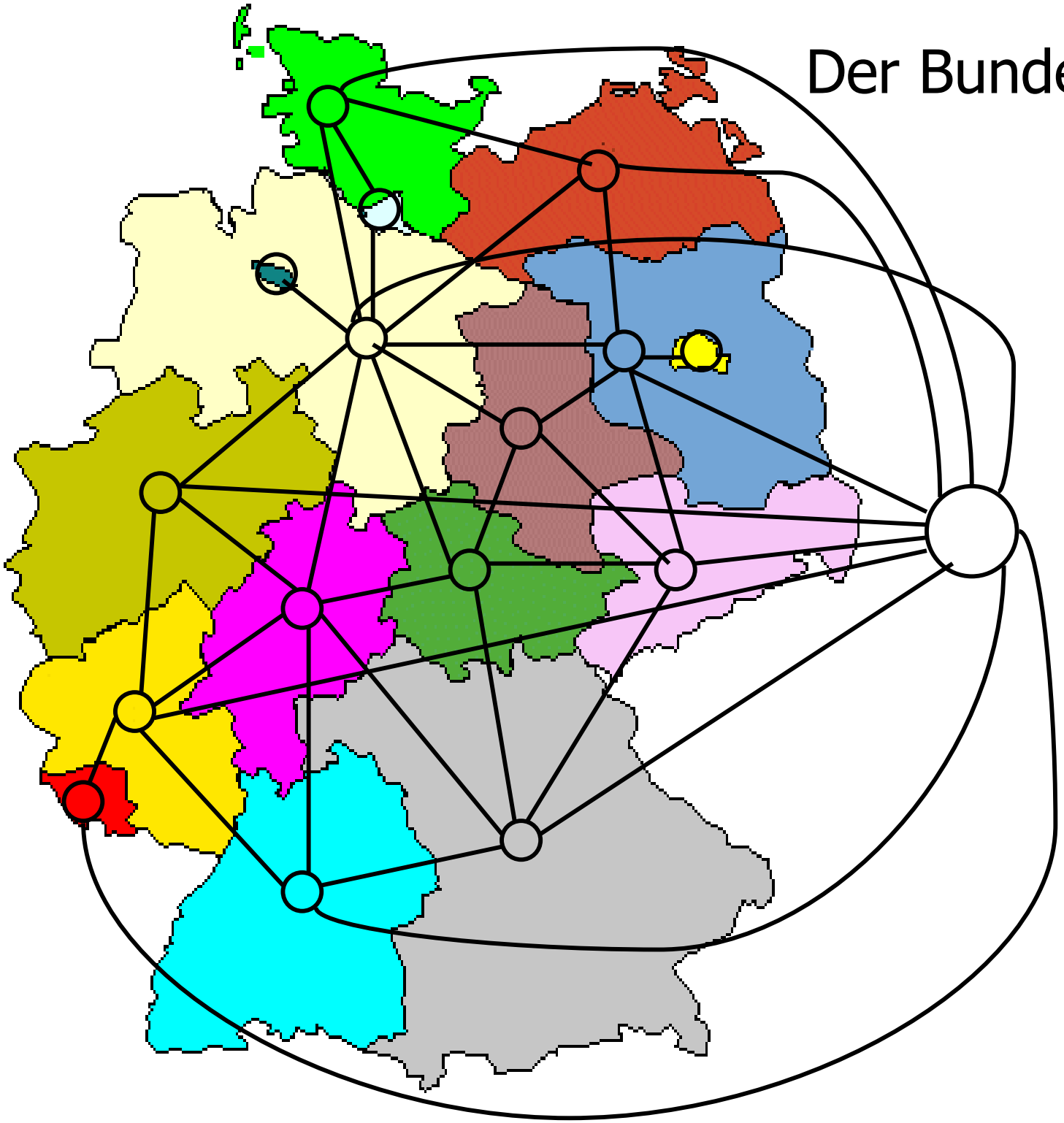
= 17 Farben

Geht das auch mit weniger Farben?

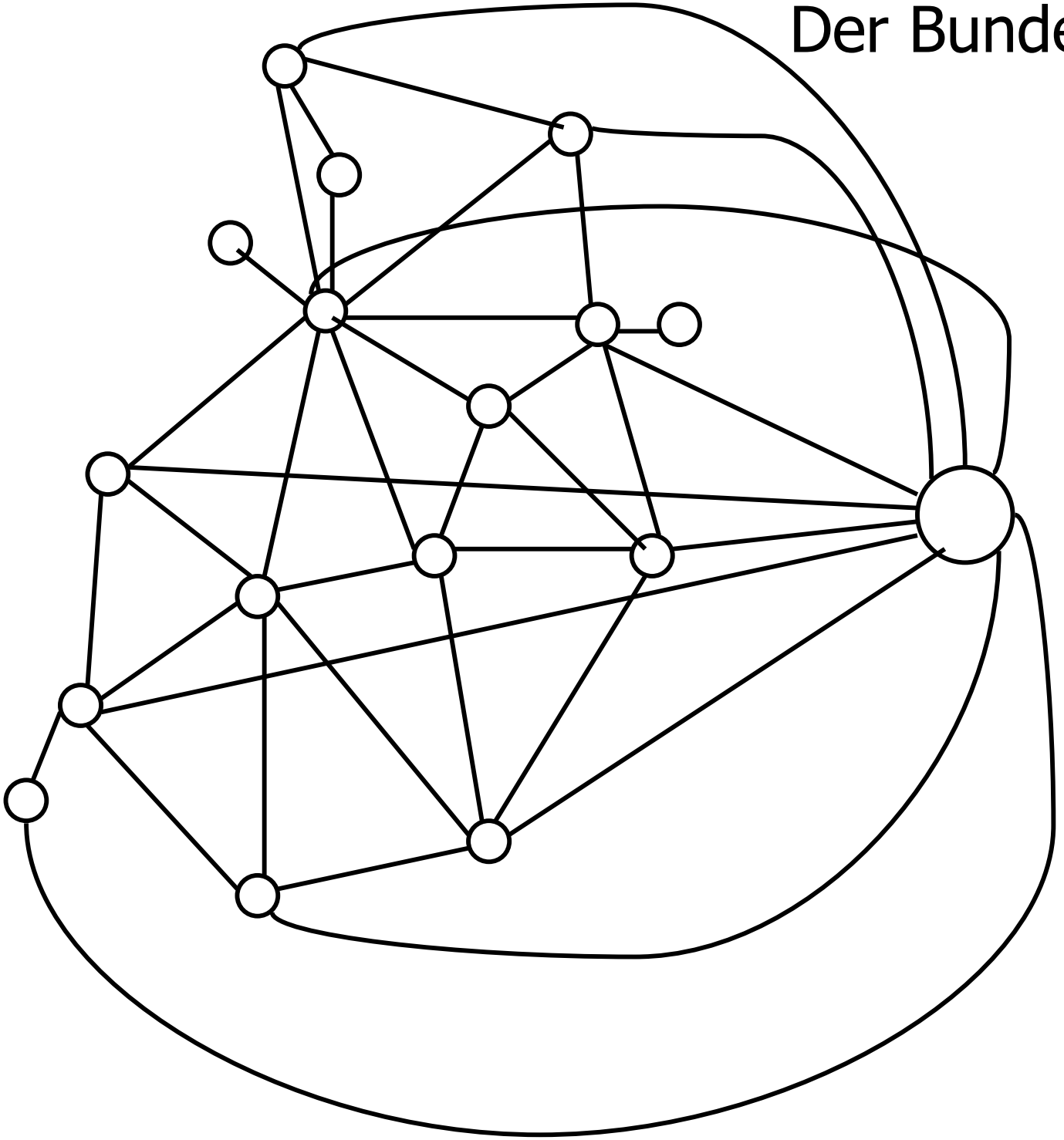


Von Bundesländern zu einem Graphen

Der Bundesländer-Graph

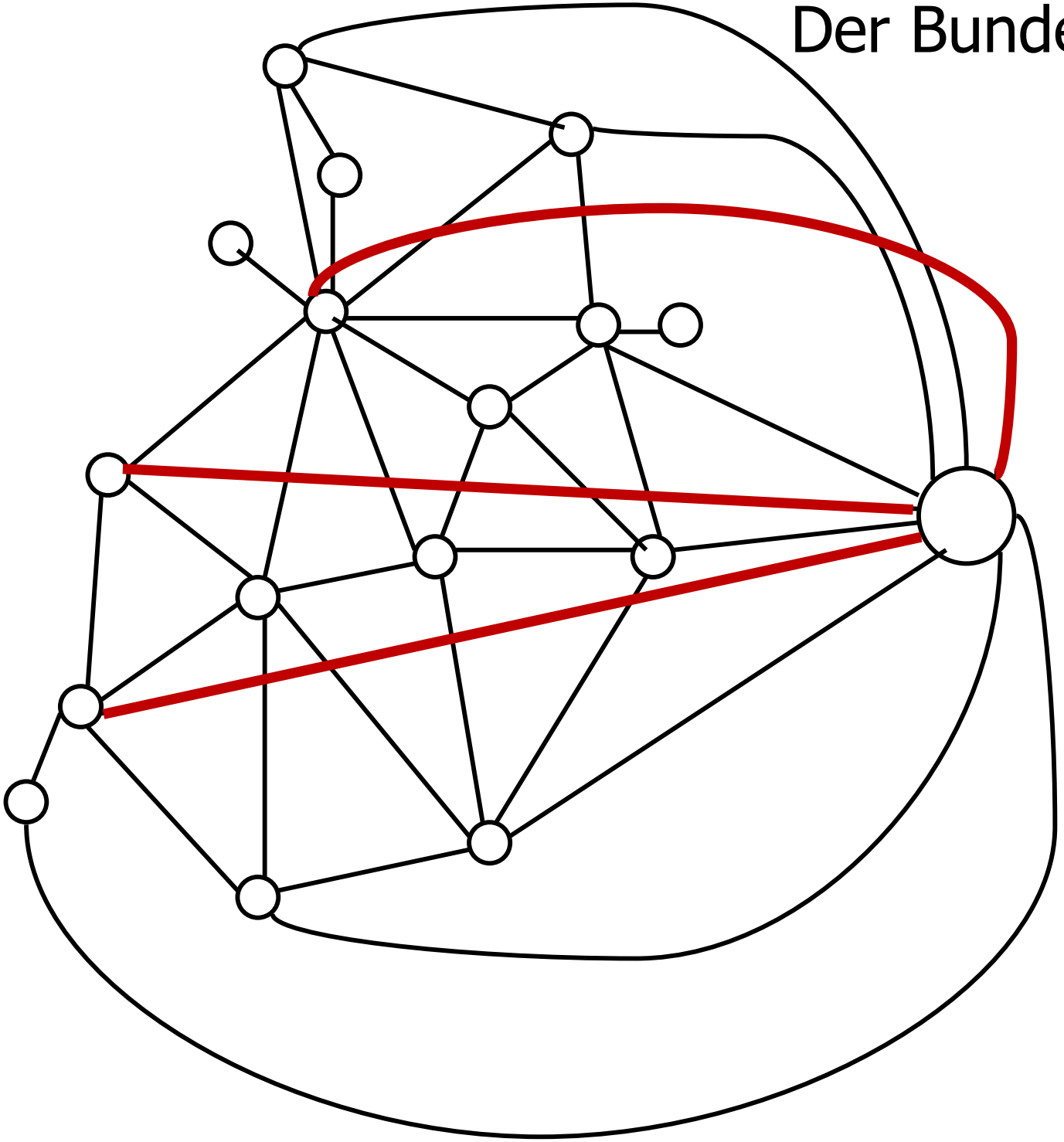


Der Bundesländer-Graph



Dieser Graph ist planar, kann also so in die Ebene gezeichnet werden, dass sich keine zwei Kanten überschneiden.

Der Bundesländer-Graph



4-Farbensatz (1852 vermutet, 175 Jahre später bewiesen)

Theorem: Die Knoten eines planaren Graphen (also auch die Länder auf einer Landkarte) können mit vier Farben so gefärbt werden, dass zwei benachbarte Knoten (durch eine Grenze aneinander stoßende Länder) verschiedene Farben haben.

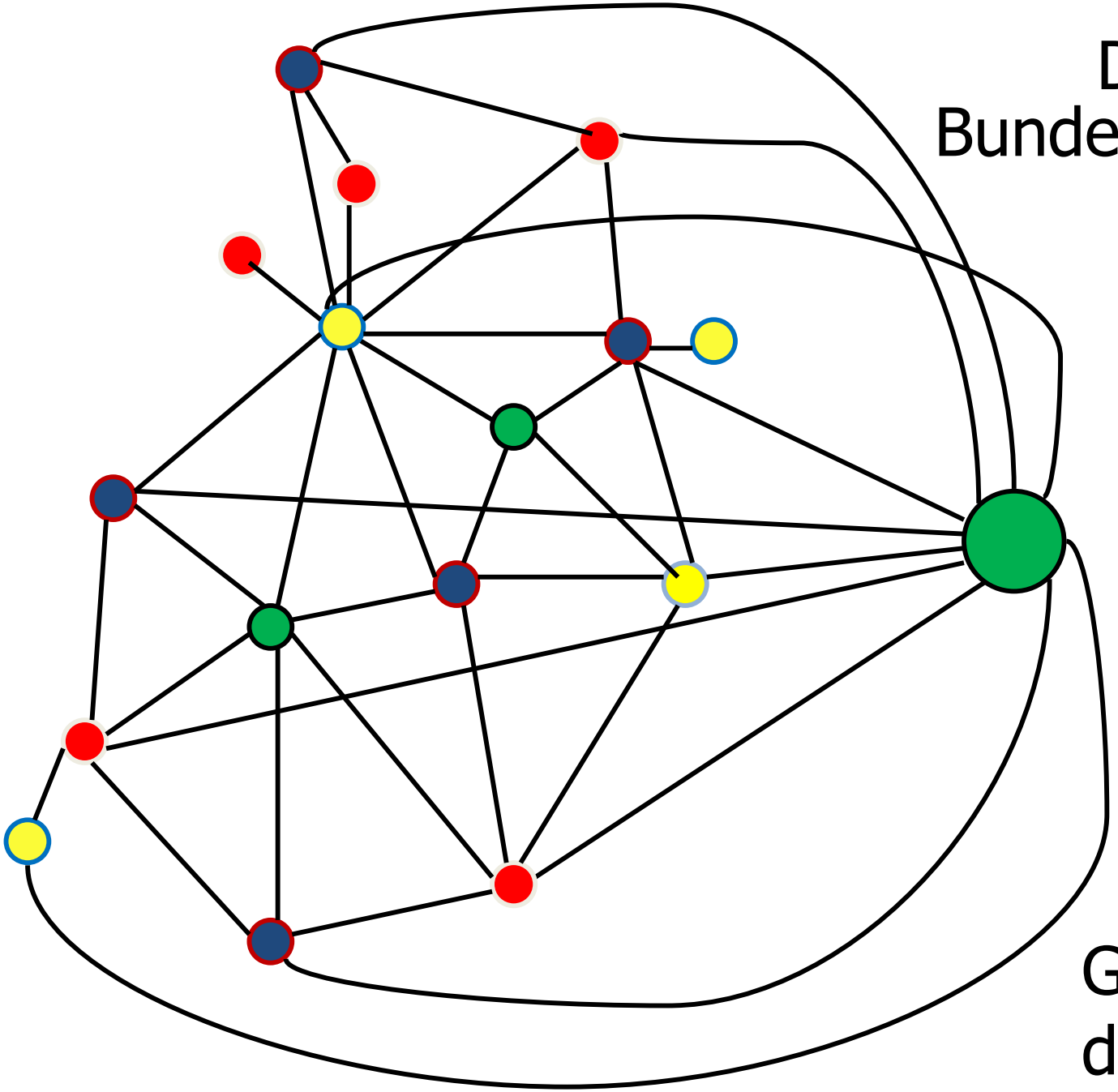
K. Appel and W. Haken, *Every planar map is four colorable*. Bulletin AMS Bd. 82, 1976, S. 711

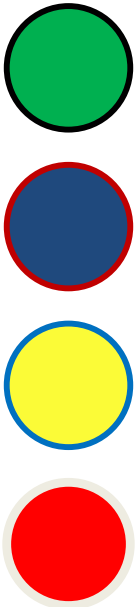
K. Appel and W. Haken, *Every planar map is four colorable. Part I. Discharging*, Illinois J. Math. 21 (1977), 429-490.

K. Appel, W. Haken and J. Koch, *Every planar map is four colorable. Part II. Reducibility*, Illinois J. Math. 21 (1977), 491--567.

1996 Neil Robertson, Daniel Sanders, Paul Seymour und Robin Thomas:
modifizierter Computerbeweis mit 633 Fällen.
(allgemein akzeptiert)

Der vierfarbige Bundesländer-Graph





Geht es auch mit drei Farben?

Überraschung

Das Problem, einen Graphen mit drei Farben zu färben, ist schwer.
Das gilt auch für den Spezialfall von planaren Graphen.

Spezielle Situation (Idee kopiert von Avi Widgerson)

Es liegt ein wichtiger großer planarer Graph vor. Jemand (die Bank, der Geheimdienst, das Militär), für uns **Herr V**, muss unbedingt wissen, ob der Graph mit drei Farben färbbar ist.

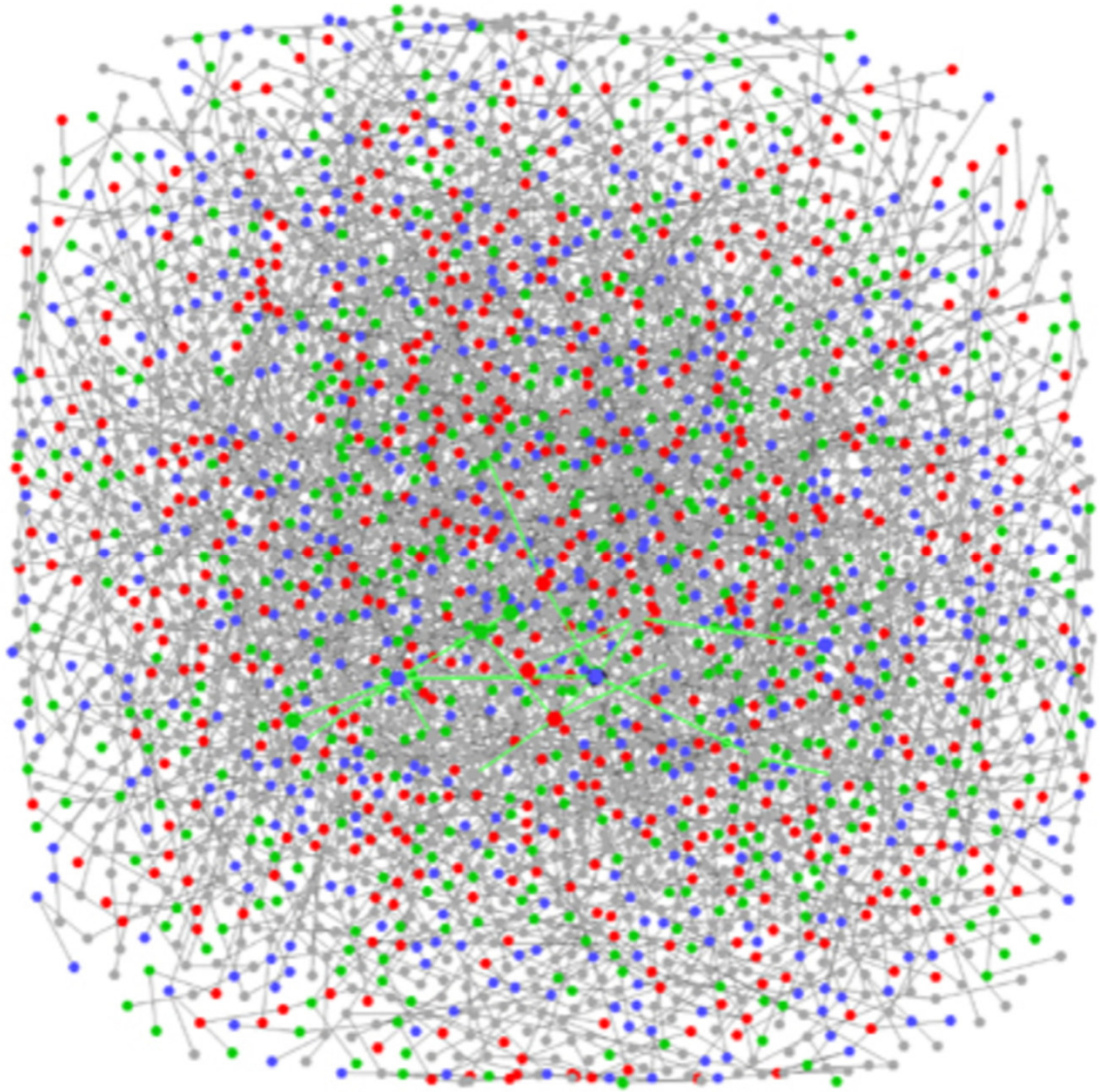
Der Beweiser **B** behauptet, dass er eine Dreifärbung kennt. Er möchte für seine Lösung eine Million Dollar haben. Herr V ist bereit, diese Summe zu bezahlen. B will ihm die Lösung aber erst übergeben, wenn er das Geld erhalten habe.

- **Wie überzeugt B Herrn V davon, dass er tatsächlich eine Lösung hat, und wie tut er das so, dass V aus den Informationen, die B ihm gibt, die Dreifärbung nicht selbst konstruieren kann?**

Das ist der wesentliche Punkt eines **Zero-Knowledge-Proofs**.

Der Zero-Knowledge-Beweis

V kennt den Graphen G, weiß also, welche Knoten mit welchen benachbart sind. In der Praxis könnte der Graph wie folgt aussehen:



Wie verläuft die Interaktion?

1. B legt auf jeden Knoten einen geschlossenen Umschlag. In diesem Umschlag ist die Farbe des Knoten verzeichnet.
2. V darf für jeweils zwei Knoten benennen, sagen wir p und q, und B öffnet die zu den Knoten p und q gehörigen Briefumschläge.
3. Sind p und q nicht benachbart, ist die Knotenfärbung irrelevant.
4. Sind p und q benachbart und haben sie die gleichen Farben, ist B als Lügner entlarvt.
5. Sind p und q benachbart und haben p und q verschiedene Farben, so ist das ein Hinweis auf die Korrektheit der Behauptung.

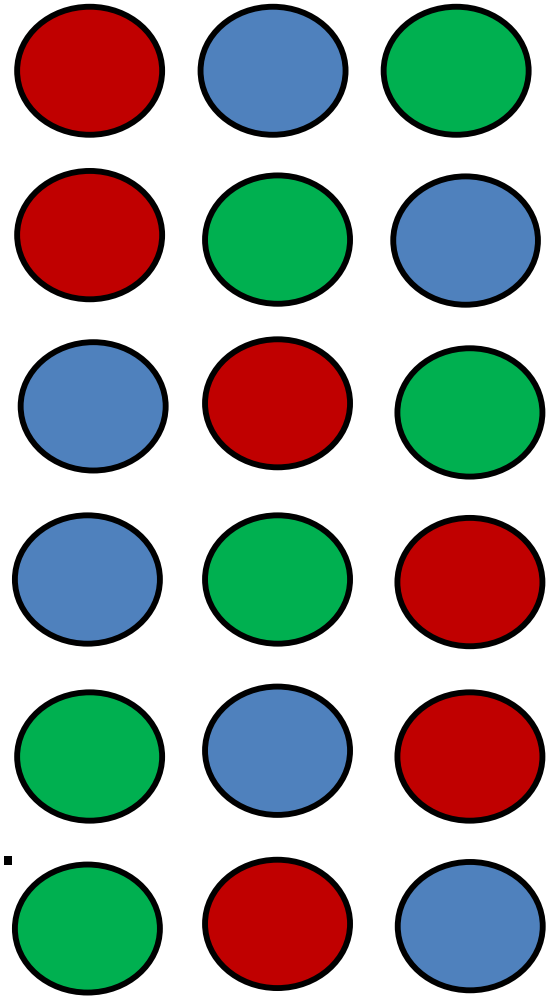
Nun könnte V im Prinzip die Umschläge für alle benachbarten Knoten überprüfen, aber dann hätte er die Dreifärbung entdeckt. Das ist kein Zero-Knowledge-Proof.

Was ist zu tun?

Wie verläuft die Interaktion?

6. Nun entfernt B alle Umschläge und legt für alle Knoten neue aus.
7. V benennt wieder zwei Knoten und es geht so fort wie vorher.

Der „Kniff" besteht darin, dass es zu jeder Dreifärbung fünf weitere Dreifärbungen gibt.



Bei jedem Wechsel der Briefumschläge wird eine andere korrekte Dreifärbung „gezeigt".

Wenn immer dieselbe Dreifärbung benutzt würde, könnte V Zug um Zug die Farben der Knoten lernen. Wird jedoch vor jeder neuen Frage eine der sechs Dreifärbungen **zufällig** ausgewählt, so kann V aus den Antworten keine Information über die Dreifärbung ableiten.

Das ist ein „Zero-Knowledge Proof".

Wieso ist V überzeugt?

Der vorgeführte Beweis ist kein Beweis im gewohnten Sinn, bei dem am Beweisende die Korrektheit glasklar demonstriert ist.

Der vorgeführte Beweis ist ein **probabilistischer Beweis**.

- Der Verifizierer V hat die Möglichkeit, so oft die Farben von zwei Knoten abzufragen, wie er will.
- Wenn er auf jede Abfrage eine korrekte Antwort erhält, so erhöht sich die Wahrscheinlichkeit Zug um Zug, dass B tatsächlich eine Dreifärbung kennt.
- V hört dann mit den Abfragen auf, wenn er aus seiner Sicht hinreichend (z. B. zu 99,99…%) überzeugt ist.

Die tiefliegendste Erkenntnis

Ich habe ein Beispiel für einen Zero-Knowledge-Beweis anhand der Dreifärbung von Graphen vorgeführt. Ich bin auf einige formale Details (wie das Interaktionsprotokoll) nicht eingegangen.

Auf Erkenntnisse vieler anderer aufbauend haben **Goldreich, Micali und Widgerson** unter gewissen technischen Voraussetzungen das folgende völlig verblüffende Theorem bewiesen.

Theorem. Für alle mathematischen Aussagen, die einen Beweis besitzen, gibt es auch einen Zero-Knowledge-Beweis.

Anwendungsbeispiel: Jemand, der eine extrem nützliche neue mathematische Theorie entwickelt hat, könnte sie der Allgemeinheit zur Verfügung stellen, ihre Korrektheit überzeugend darstellen, aber verschleiern, warum sie richtig ist.

Verschlüsselung

Das RSA-Verfahren ist eine der bei Verschlüsselungen am häufigsten verwendeten Methoden. Es basiert (wie auch weitere Verfahren) darauf dass es, für eine Zahl z, die Produkt zweier großer Primzahlen p und q ist (z=p●q), schwer ist, die beiden Primfaktoren p und q schnell zu bestimmen.

- Der seit rund 25 Jahren bekannte Shor-Algorithmus könnte diese Aufgabe schnell erledigen, aber dafür werden funktionierende Quantencomputer benötigt.

- Wenn jemand, sagen wir eine Zahlentheoretikerin, einen schnellen Faktorisierungsalgorithmus auf einem konventionellen Computer finden würde, wäre das ein interessanter Anwendungsfall für einen Zero-Knowledge-Beweis.

P = BPP, etc.

Widgerson hat tiefliegende Erkenntnisse zu den Hierarchieklassen der Komplexitätstheorie beigetragen. Die Darstellung erfordert sehr detaillierten technischen Aufwand. Mir ist es nicht gelungen, die Beiträge so aufzubereiten, dass sie in wenigen Minuten einigermaßen verständlich erläutert werden können. Um die Schwierigkeit anzudeuten, nenne ich einige wichtige Hierarchieklassen:

- **R** berechenbar, **RE** beweisbar durch endliche Algorithmen (**R≠RE**)
- Komplexitätsklassen: **P, NP, BPP, EXP, NEXP, PSPACE** (**P=NP**?)
- **PCP** Probabilistically Checkable Proofs (**PCP=NP**)
- **IP** Interactive Proofs (**IP=PSPACE**) (polynomial number of interactions)
- **2IP** Two Prover Interactive Proofs (**2IP=NEXP**)
- **IP*** Quantum Verifier Interactive Proofs (**IP*=PSPACE**)
- **MIP*** Multiple Quantum Verifier Interactive Proofs (**MIP*=RE**)

Gliederung

1. Abel und der Abel-Preis
2. Der Abel-Preis und die International Mathematical Union
3. Veranstaltungen anlässlich der Verleihung
4. Graphentheorie & Komplexitätstheorie (ein paar Begriffe)
5. Die Preisträger 2021
6. László Lovász: Perfekte Graphen und davon ausgehende Entwicklungen, der LLL-Algorithmus
7. Avi Wigderson: 3-Färbungen und Zero-Knowledge-Proofs, P=BPP
8. Zusammenfassung

Vielen Dank für Ihre Aufmerksamkeit

Der Abel-Preis:
Die Preisverleihung
und eine Skizze einiger Aspekte
des Werks der Preisträger von 2021

Martin Grötschel

Tag der Mathematik, FU Berlin
30.04.2022

- Institut für Mathematik, Technische Universität Berlin (TUB) (1991-2015, im Ruhestand)
- Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB) (1991-2015)
- DFG-Forschungszentrum "Mathematik für Schlüsseltechnologien" (MATHEON) (2002-2014)
- Berlin-Brandenburgische Akademie der Wissenschaften (2015-2020)

groetschel@bbaw.de
http://www.zib.de/groetschel