Tutorium: Diskrete Mathematik

Vorbereitung der Bonusklausur am 19.01.2018 (Teil 1)

10. Januar 2018

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

© 2018 Steven Köhler

Relationen

© 2018 Steven Köhler

Definition I

Bei einer *n-stelligen Relation* handelt es sich um eine Teilmenge des kartesischen Produkts der Mengen $A_1, \ldots, A_n$. Die Mengen $A_1, \ldots, A_n$ müssen hierbei nicht verschieden sein.

Bei einer *binären* oder *zweistelligen Relation* handelt es sich um eine Teilmenge

$$R \subseteq A_1 \times A_2.$$

Bei einer *binären* oder *zweistelligen Relation über der Menge A* handelt es sich um eine Teilmenge

$$R \subseteq A \times A.$$

Bei einer *ternären* oder *dreistelligen Relation* handelt es sich um eine Teilmenge

$$R \subseteq A_1 \times A_2 \times A_3.$$

© 2018 Steven Köhler

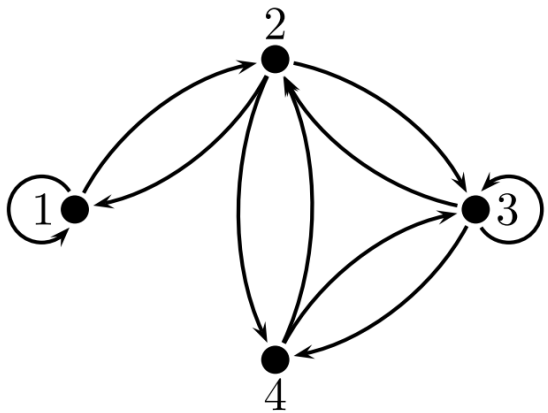
Definition II

Relationen können auf verschiedene Arten dargestellt werden, z.B. als Menge, als gerichtete Graphen oder mithilfe von Matrizen.

Es sei $A = \{1, 2, 3, 4\}$ eine Menge und $R \subseteq A \times A$ eine Relation über A:

$$R = \{(1,1), (1,2), (2,1), (2,3), (2,4), (3,2), (3,3), (3,4), (4,2), (4,3)\}$$

1	1	0	0
1	0	1	1
0	1	1	1
0	1	1	0



© 2018 Steven Köhler

Eigenschaften von Relationen I

Es sei R eine Relation über einer Menge A. Die Relation ist

- *symmetrisch*, falls gilt:

$$\forall a, b \in A : (a, b) \in R \rightarrow (b, a) \in R.$$

- *nicht symmetrisch*, falls gilt:

$$\exists a, b \in A : (a, b) \in R \rightarrow (b, a) \notin R.$$

- *antisymmetrisch*, falls gilt:

$$\forall a, b \in A, a \neq b : (a, b) \in R \rightarrow (b, a) \notin R.$$

- *nicht antisymmetrisch*, falls gilt:

$$\exists a, b \in A, a \neq b : (a, b) \in R \rightarrow (b, a) \in R.$$

© 2018 Steven Köhler

Eigenschaften von Relationen II

Es sei R eine Relation über einer Menge A. Die Relation ist

- *reflexiv*, falls gilt:

$$\forall a \in A : (a, a) \in R.$$

- *nicht reflexiv*, falls gilt:

$$\exists a \in A : (a, a) \notin R.$$

- *irreflexiv*, falls gilt:

$$\forall a \in A : (a, a) \notin R.$$

- *nicht irreflexiv*, falls gilt:

$$\exists a \in A : (a, a) \in R.$$

© 2018 Steven Köhler

Eigenschaften von Relationen III

Es sei R eine Relation über einer Menge A. Die Relation ist

- *transitiv*, falls gilt:

$$\forall a, b, c \in A : (a, b) \in R \land (b, c) \in R \rightarrow (a, c) \in R.$$

- *intransitiv*, falls gilt:

$$\exists a, b, c \in A : (a, b) \in R \land (b, c) \in R \rightarrow (a, c) \notin R.$$

- *antitransitiv*, falls gilt:

$$\forall a, b, c \in A : (a, b) \in R \land (b, c) \in R \rightarrow (a, c) \notin R.$$

© 2018 Steven Köhler

Aufgabe 1

Es sei R die folgende auf der Menge $A = \{a, b, c, d\}$ definierte Relation:

$$R = \{(a, a), (a, b), (b, b), (c, a), (d, a), (b, a), (a, d), (d, d)\}.$$

Entscheide, welche der folgenden Eigenschaften auf die Relation zutreffen. Gib jeweils eine kurze Begründung.

(i) symmetrisch

(ii) antisymmetrisch

(iii) reflexiv

(iv) irreflexiv

(v) transitiv

© 2018 Steven Köhler

Aufgabe 2

Es sei $A = \{1, 2, 3, 4\}$.

a) Gib eine Relation R_a über der Menge A an, die reflexiv, aber nicht transitiv ist.

b) Gib eine Relation R_b über der Menge A an, die symmetrisch, transitiv und nicht irreflexiv ist.

c) Gib eine Relation R_c über der Menge A an, die irreflexiv und weder symmetrisch noch antisymmetrisch ist. Dabei soll $|R_c| \geq 5$ gelten.

d) Gib eine Relation R_d über der Menge A an, die sowohl symmetrisch als auch antisymmetrisch ist.

© 2018 Steven Köhler

Äquivalenzrelation I

Man nennt eine Relation R über einer Menge A eine *Äquivalenzrelation*, falls gilt:

R ist symmetrisch, reflexiv und transitiv.

© 2018 Steven Köhler

Äquivalenzrelation II

Zu jeder Äquivalenzrelation gehört eine eindeutig bestimmte *Partition*, die die Menge A in disjunkte Teilmengen $A_1, \ldots, A_n$ aufteilt, so dass gilt:

$$A = A_1 \cup \ldots \cup A_n$$

$$A_i \cap A_j = \emptyset \quad (\text{für } i \neq j).$$

Bei den Teilmengen $A_1, \ldots, A_n$ handelt es sich um die *Äquivalenzklassen* der Relation.

- Stehen zwei Elemente in Relation, so sind sie in derselben Äquivalenzklasse.
- Elemente aus verschiedenen Äquivalenzklassen stehen niemals in Relation.

© 2018 Steven Köhler

Ordnungsrelation I

Man nennt eine Relation R über einer Menge A eine *Ordnungsrelation*, falls gilt:

R ist antisymmetrisch, reflexiv und transitiv.

© 2018 Steven Köhler

Ordnungsrelation II

Bei einem *Hasse-Diagramm* handelt es sich um eine Möglichkeit, eine Ordnungsrelation grafisch darzustellen. Für die bessere Übersichtlichkeit gilt:

- Kanten sind stets nach oben gerichtet, Pfeilspitzen werden weggelassen;
- reflexive Kanten werden nicht aufgezeichnet;
- transitive Kanten werden nicht aufgezeichnet.

© 2018 Steven Köhler

Aufgabe 3

Sei $A = \{a, b, c\}$. Auf der Menge $\mathcal{P}(A)$ betrachtet man die Inklusion $\subseteq$, also die Relation

$$\Big\{(X, Y) : X, Y \in \mathcal{P}(A) \wedge X \subseteq Y\Big\}.$$

Stelle $\subseteq$ auf $\mathcal{P}(A)$ als Hasse-Diagramm dar.

© 2018 Steven Köhler

Reflexive Hülle I

Gegeben sei eine Relation R über einer Menge A. Falls R nicht reflexiv ist, so kann man R in eine reflexive Relation R' überführen, indem man für alle $a \in A$ das Paar (a, a) zu R hinzufügt:

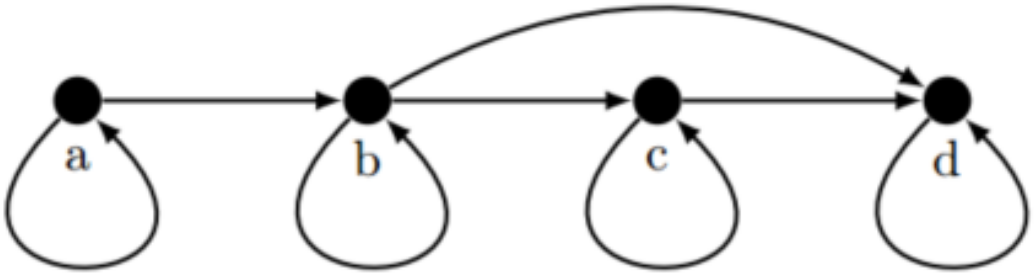
$$R' = R \cup \Big\{(a, a) : a \in A\Big\}.$$

R' ist hierbei die kleinste reflexive Relation, die R umfasst. Man bezeichnet R' als *reflexive Hülle* von R.

© 2018 Steven Köhler

Reflexive Hülle II

Relation R



reflexive Hülle R'

© 2018 Steven Köhler

Transitive Hülle I

Gegeben sei eine Relation R über einer Menge A. Falls R nicht transitiv ist, so kann man R in eine transitive Relation R^+ überführen, indem man für $a, b, c \in A$ mit $(a, b) \in R$ und $(b, c) \in R$ das Paar (a, c) zu R hinzufügt und dies solange wiederholt, bis keine weiteren Kanten mehr hinzugefügt werden können.

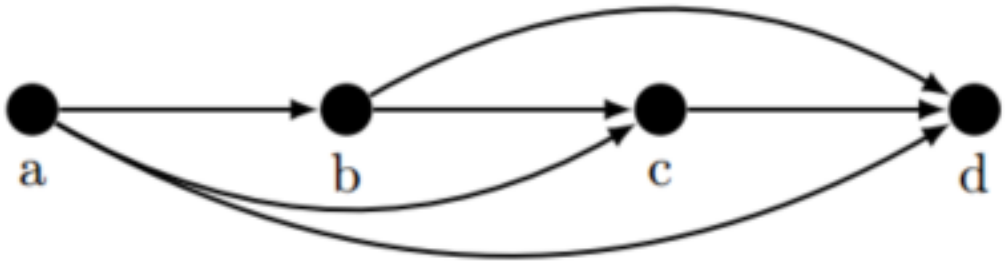
$$R^+ = R \cup \Big\{ (a, b) : \text{Es gibt } n \geq 2 \text{ und } a_1, \ldots, a_n \in A \text{ mit } a_1 = a,\ a_n = b \text{ und } (a_1, a_2), (a_2, a_3), \ldots, (a_{n-1}, a_n) \in R. \Big\}$$

R^+ ist hierbei die kleinste transitive Relation, die R umfasst. Man bezeichnet R^+ als *transitive Hülle* von R.

© 2018 Steven Köhler

Transitive Hülle II

Relation R



transitive Hülle R^+

© 2018 Steven Köhler

Reflexive, transitive Hülle I

Gegeben sei eine Relation R auf einer Menge A. Man nennt die Relation

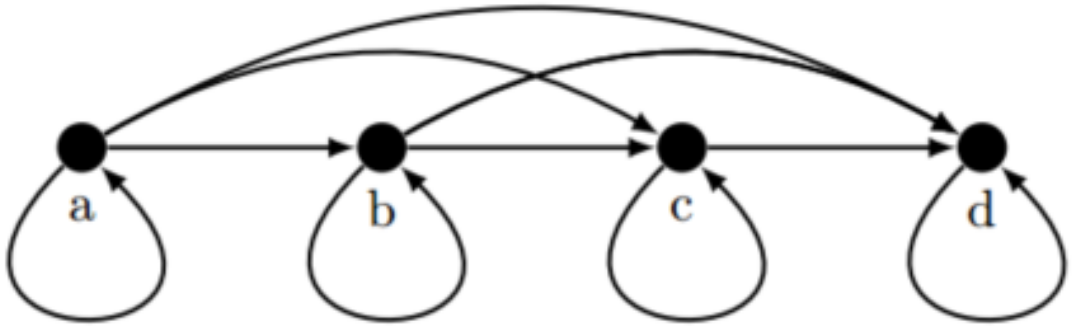
$$R^* = R^+ \cup R'$$

die *reflexive, transitive Hülle* von R. Bei R^* handelt es sich um die kleinste reflexive und transitive Relation, die R umfasst.

© 2018 Steven Köhler

Reflexive, transitive Hülle II

Relation R



reflexive, transitive Hülle R^*

© 2018 Steven Köhler

Graphentheorie

© 2018 Steven Köhler

Ungerichteter Graph

Bei einem *ungerichteten Graphen* G handelt es sich um ein Paar $G = (V, E)$:

- V ist die *Knotenmenge* des Graphen;
- E ist die *Kantenmenge* des Graphen

$$E \subseteq \Big\{ \{x, y\} : x, y \in V, x \neq y \Big\}.$$

© 2018 Steven Köhler

Ungerichteter Multigraph

Bei einem *ungerichteten Mutligraphen* G handelt es sich um ein Tripel $G = (V, E, f)$:

- V ist die *Knotenmenge* des Graphen;
- E ist die *Kantenmenge* des Graphen;
- f ist eine Abbildung, die jedem Element von E eine ein- oder zweielementige Teilmenge von V zuordnet.

Kanten mit demselben Start- und Endknoten heißen *Schlingen*. Existieren Kanten $e_1, e_2 \in E$ mit $f(e_1) = f(e_2)$, so handelt es sich um *Mehrfachkanten*.

© 2018 Steven Köhler

Gerichteter Graph

Bei einem *gerichteten Graphen* G handelt es sich um ein Paar $G = (V, E)$:

- V ist die *Knotenmenge* des Graphen;
- E ist die *Kantenmenge* des Graphen

$$E \subseteq \Big\{ (x, y) : x, y \in V \Big\} = V \times V.$$

© 2018 Steven Köhler

Grad eines Knotens

Unter dem *Grad* $d(v)$ eines Knotens v versteht man die Anzahl der zu v inzidenten Kanten.

Es gilt stets (*Handshaking Lemma*):

$$\sum_{v \in V} d(v) = 2 \cdot |E|.$$

© 2018 Steven Köhler

Aufgabe 4

Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Der Graph H_n sei wie folgt definiert: Die Knotenmenge von H_n sei die Menge aller n-Tupel $(x_1, \ldots, x_n)$ mit $x_i \in \{0, 1, 2\}$ (für $i = 1, \ldots, n$). Zwei Knoten seien genau dann durch eine Kante verbunden, wenn sie sich an genau 2 Stellen unterscheiden.

a) Wie viele Knoten besitzt der Graph H_n?

b) Wie viele Kanten besitzt der Graph H_n?

© 2018 Steven Köhler

Zusammenhang eines Graphen I

Ein ungerichteter Graph $G = (V, E)$ heißt *zusammenhängend*, falls es für alle Knoten $v, w \in V$ einen ungerichteten Weg von v nach w gibt.

Einen maximal zusammenhängenden Teilgraphen nennt man *Komponente* oder auch *Zusammenhangskomponente*. Die Anzahl der Zusammenhangskomponenten eines Graphen G wird mit $c(G)$ bezeichnet.

© 2018 Steven Köhler

Zusammenhang eines Graphen II

Ein gerichteter Graph $G = (V, E)$ heißt *(stark) zusammenhängend von einem Knoten v aus*, falls es für alle Knoten $w \in V$ einen gerichteten Weg von v nach w gibt.

Ein gerichteter Graph $G = (V, E)$ heißt *stark zusammenhängend*, falls G von jedem Knoten $v \in V$ aus stark zusammenhängend ist.

Ein gerichteter Graph G heißt *schwach zusammenhängend*, falls der zugehörige ungerichtete Graph zusammenhängend ist.

© 2018 Steven Köhler

Eulersche Linie I

G sei ein zusammenhängender Graph oder Multigraph. Man nennt einen Kantenzug in G eine *eulersche Linie*, falls er geschlossen ist und sämtliche Kanten von G durchläuft.

© 2018 Steven Köhler

Eulersche Linie II

Für jeden zusammenhängenden Graphen oder Multigraphen G gilt: G hat genau dann eine eulersche Linie, wenn der Grad jedes Knotens gerade ist. (notwendig und hinreichend)

© 2018 Steven Köhler

Hamiltonkreis I

G sei ein Graph und C sei ein Kreis in G. Man nennt C einen *Hamiltonschen Kreis* (oder auch *Hamiltonkreis*), wenn C sämtliche Knoten von G enthält.

© 2018 Steven Köhler

Hamiltonkreis II

Hat ein Graph $G = (V, E)$ einen Hamiltonkreis, so gilt für alle $A \subseteq V$ stets $c(G - A) \leq |A|$. (notwendig)

Gilt $d(v) \geq \lceil \frac{n}{2} \rceil$ für alle $v \in V$, so besitzt der Graph $G = (V, E)$ mit $|V| = n$ einen Hamiltonkreis. (*Satz von Dirac*, hinreichend)

Gilt $d(v) + d(u) \geq n$ für alle nichtadjazenten Knoten $u, v \in V$, so besitzt der Graph $G = (V, E)$ mit $|V| = n$ einen Hamiltonkreis. (*Satz von Ore*, hinreichend)

© 2018 Steven Köhler

Aufgabe 5

Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Der ungerichtete Graph H bestehe aus zwei Zusammenhangskomponenten H_1 und H_2. Der Teilgraph H_1 sei ein vollständiger Graph mit n Knoten, der Teilgraph H_2 sei ein Baum mit n Knoten. Der Graph G entsteht aus H dadurch, dass man weitere Kanten wie folgt zu H hinzufügt: Man verbindet jeden Knoten von H_1 mit jedem Knoten von H_2 durch eine Kante.

a) Wie viele Kanten besitzt der Graph G?

b) Besitzt der Graph G einen Hamiltonkreis? Gib eine kurze Begründung.

c) Begründe, weshalb der Graph G im Allgemeinen keine eulersche Linie besitzt.

© 2018 Steven Köhler

Aufgabe 6

Unter einem *Hyperwürfel* Q_n versteht man den folgenden Graphen: Knotenmenge von Q_n ist die Menge aller n-Tupel $(x_1, \ldots, x_n)$ mit $x_i \in \{0, 1\}$ für $i = 1, \ldots, n$. Zwei Knoten von Q_n sind genau dann durch eine Kante verbunden, wenn sich die entsprechenden n-Tupel an genau einer Stelle unterscheiden.

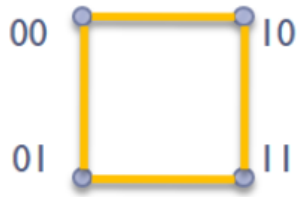
Beweise durch vollständige Induktion, dass der Hyperwürfel Q_n für jedes $n \in \mathbb{N}$ mit $n \geq 2$ einen Hamiltonkreis besitzt.

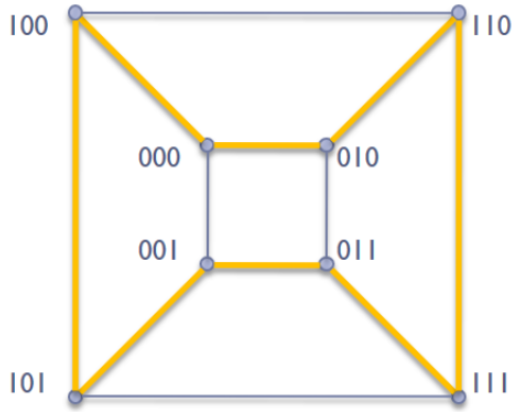
© 2018 Steven Köhler

Aufgabe 6 – Lösung I

Induktionsanfang:

Die Hyperwürfel Q_2 und Q_3 besitzen Hamiltonkreise.





© 2018 Steven Köhler

Aufgabe 6 – Lösung II

Induktionsannahme:

Für ein fest gewähltes $n \in \mathbb{N}$ besitzt der Hyperwürfel Q_n einen Hamiltonkreis.

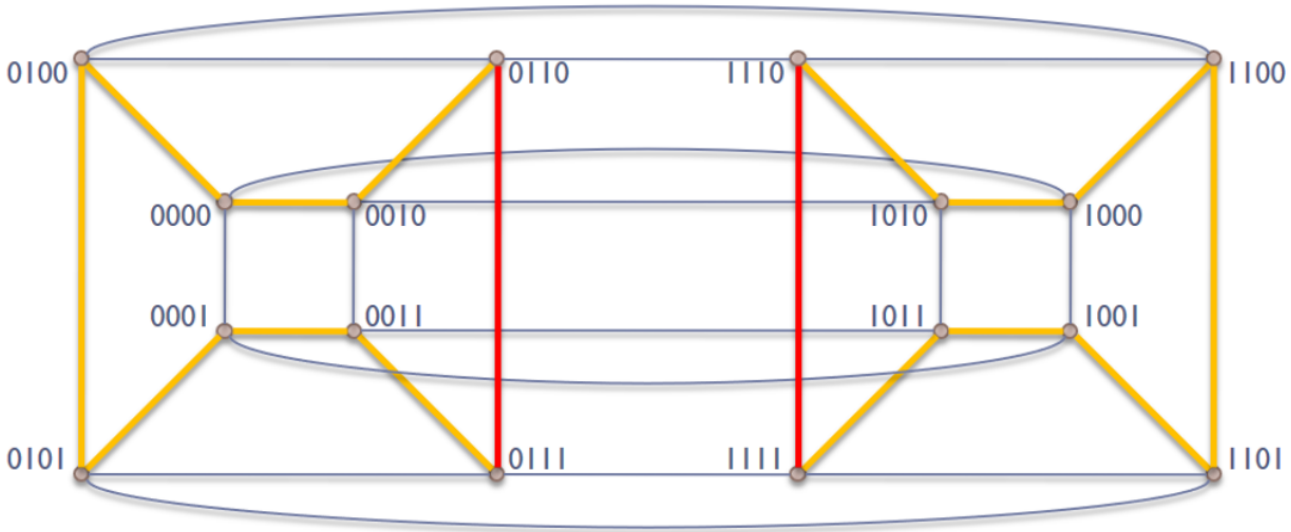
Induktionsschritt:

Der Hyperwürfel Q_{n+1} entsteht aus Q_n, indem man Q_n verdoppelt (und die Kopie spiegelt), die mit den Knoten assoziierten Tupel um 0 bzw. 1 ergänzt und die entsprechenden Verbindungskanten hinzufügt.

© 2018 Steven Köhler

Aufgabe 6 – Lösung III

Demonstration am Beispiel von Q_4:

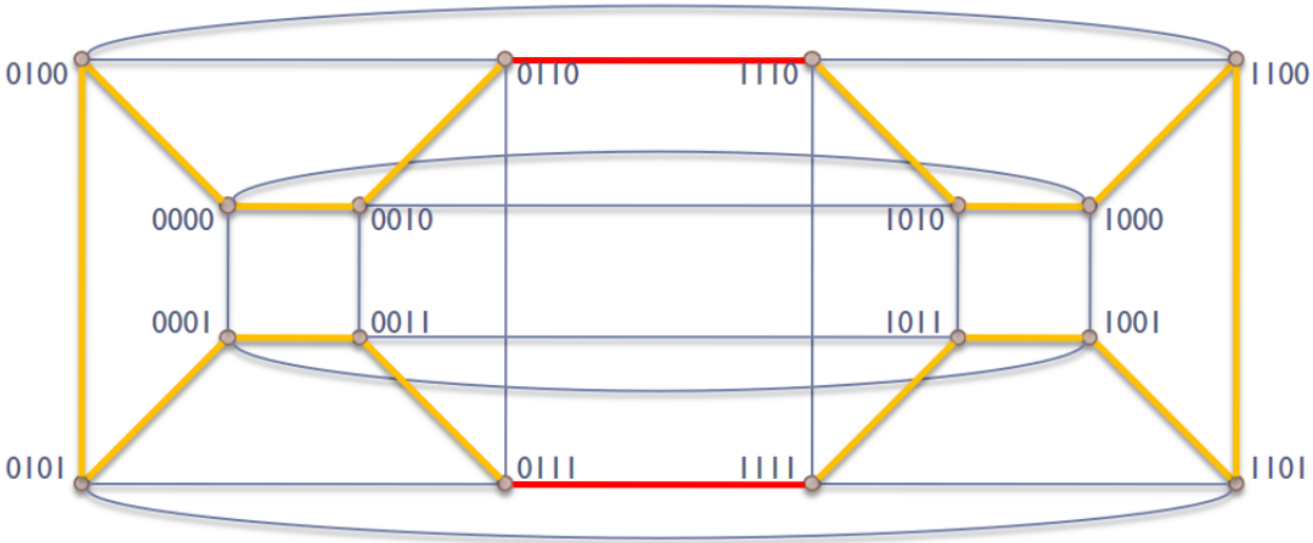


Die orangenen (bzw. roten) Kanten sind die Hamiltonkreise der beiden enthaltenen Hyperwürfel Q_3. Die beiden roten Kanten werden aus den Hamiltonkreisen „entfernt“, die orangenen Kantenzüge werden neu verbunden.

© 2018 Steven Köhler

Aufgabe 6 – Lösung IV

Es entsteht der Hamiltonkreis des Q_4:



Auf analoge Art lässt sich ein Hamiltonkreis für jeden Hyperwürfel Q_{n+1} aus den (nach der Induktionsannahme existierenden) Hamiltonkreisen der beiden Hyperwürfel Q_n konstruieren. □

© 2018 Steven Köhler

Aufgabe 7

Wahr oder falsch? Gib jeweils eine (kurze) Begründung.

(i) Jeder vollständige Graph besitzt einen Hamiltonkreis.

(ii) In einem Graphen ist die Summe aller Knotengrade stets gerade.

(iii) Ein ungerichteter Graph besitzt genau dann eine eulersche Linie, wenn jeder Knoten einen geraden Grad besitzt.

(iv) Es existiert kein ungerichteter Graph mit n Knoten und n^2 Kanten.

(v) Das „Haus des Nikolaus“ besitzt eine eulersche Linie.

(vi) Es sei $G = (V, E)$. Gilt $c(G - A) < |A|$ für alle Teilmengen $A \subseteq V$, so besitzt der Graph G einen Hamiltonkreis.

© 2018 Steven Köhler

Isomorphie

Zwei Graphen G und H heißen *isomorph* (oder *strukturgleich*), wenn es eine bijektive Abbildung φ gibt, die die Knoten von G auf die Knoten von H abbildet, so dass gilt:

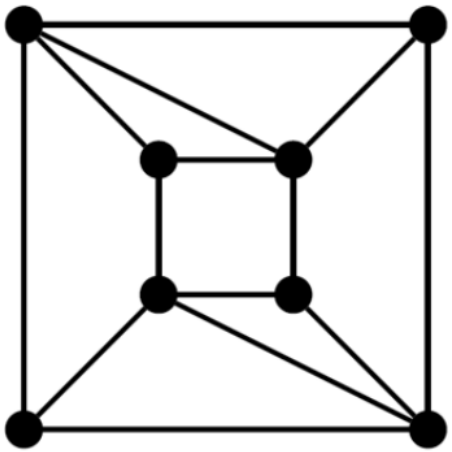
$$\forall u, v \in V(G) : \{u, v\} \in E(G) \Leftrightarrow \{\varphi(u), \varphi(v)\} \in E(H).$$

Die Abbildung φ heißt *Isomorphismus*.

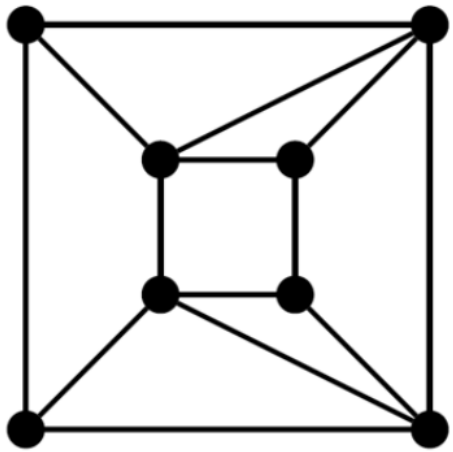
© 2018 Steven Köhler

Aufgabe 8

Sind die folgenden beiden Graphen isomorph? Gib eine (kurze) Begründung für deine Antwort!



G



G'

© 2018 Steven Köhler

Aufgabe 9

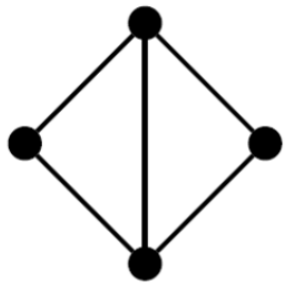
G sei ein vollständiger Graph mit genau 8 Knoten.

a) Wie viele Kanten hat G?

b) Wie viele verschiedene Kreise der Länge 3 enthält G?

c) Wie viele verschiedene Kreise der Länge 4 enthält G?

d) Wie viele verschiedene Teilgraphen, die isomorph zum abgebildeten Graphen sind, enthält G?



© 2018 Steven Köhler

Tiefensuche I

1. Markiere den Knoten v und setze $a := v$. In diesem Schritt sei B der Baum, dessen einziger Knoten die Wurzel v ist.
2. Falls es einen unmarkierten Knoten $u \in V$ gibt, so dass $(a, u) \in E$ gilt, so wählte ein solches u, füge u und die Kante (a, u) zum Baum B hinzu, markiere u und setze $a := u$. Diesen Schritt bezeichnet man als den *Vorwärtsschritt* (*advance step*).

© 2018 Steven Köhler

Tiefensuche II

3. Falls es keinen unmarkierten Knoten $u \in V$ gibt, so dass $(a, u) \in E$ gilt, und falls a nicht die Wurzel von B ist, so geht man zurück zum Vater w von a in B und setzt $a := w$. Diesen Schritt bezeichnet man als den *Rückwärtsschritt* (*back-tracking step*). Nun fährt man mit Schritt (2) fort.
4. Falls es keinen unmarkierten Knoten $u \in V$ gibt, so dass $(a, u) \in E$ gilt, und falls a die Wurzel von B ist, so endet der Algorithmus. Die von v aus erreichbaren Knoten sind genau die markierten Knoten. Das sind auch genau die Knoten von B.

© 2018 Steven Köhler

Breitensuche I

1. Markiere den Knoten v und setze $a := v$. In diesem Schritt sei B der Baum, dessen einziger Knoten die Wurzel v ist.
2. Falls es einen unmarkierten Knoten $u \in V$ gibt, so dass $(a, u) \in E$ gilt, so wähle ein solches u, füge u und die Kante (a, u) zum Baum B hinzu und markiere u. Im Unterschied zur Tiefensuche bleibt in diesem Schritt der ursprüngliche Knoten a der aktuelle Knoten.

© 2018 Steven Köhler

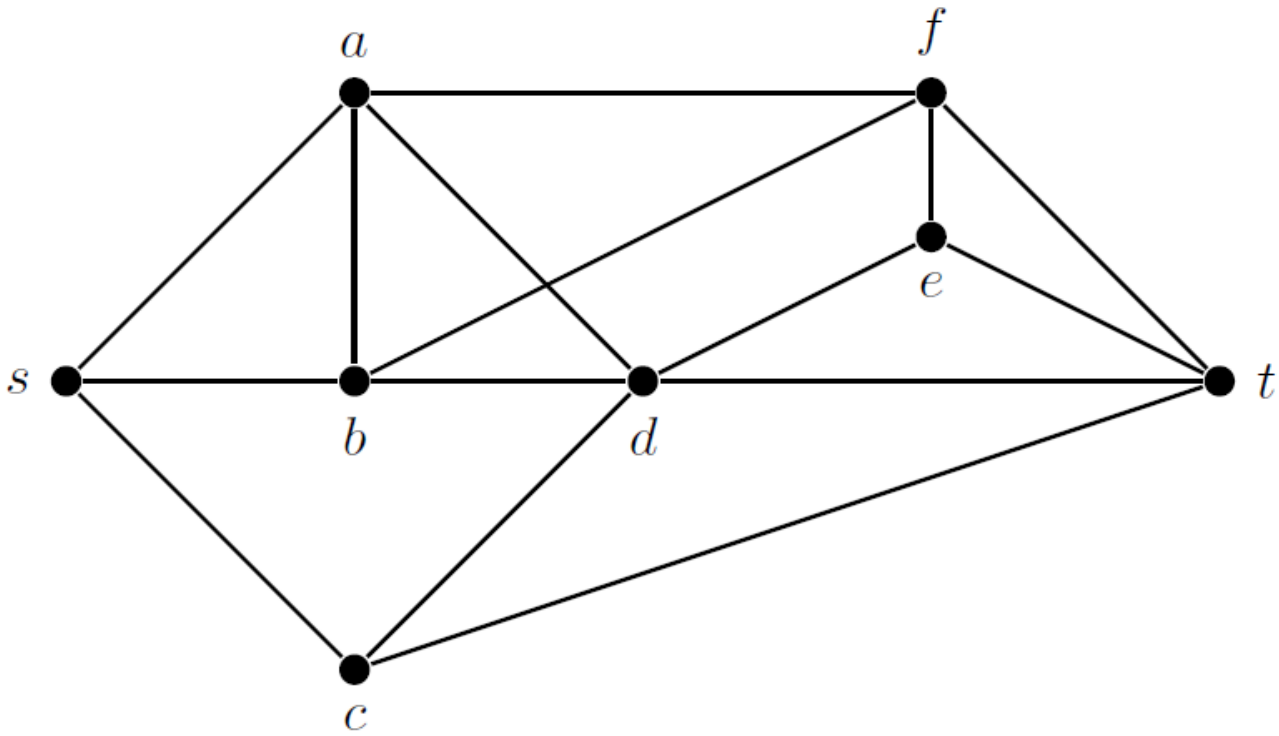
Breitensuche II

3. Falls es keinen unmarkierten Knoten $u \in V$ gibt, so dass $(a, u) \in E$ gilt, und falls es einen Knoten b in B gibt, von dem aus es eine Kante (b, u) zu einem unmarkierten Knoten u gibt, so wähle aus allen solchen Knoten b denjenigen aus, der schon am längsten im Baum B ist und setze $a := b$. Der Knoten b wird also der neue aktuelle Knoten und der Algorithmus fährt mit Schritt (2) fort.
4. Falls es keine Kante (a, u) vom aktuellen Knoten zu einem unmarkierten Knoten gibt und auch kein Knoten b in B existiert, der zu einem unmarkierten Knoten benachbart ist, so stoppt der Algorithmus.

© 2018 Steven Köhler

Aufgabe 10

Führe für den folgenden Graphen G eine Breiten- sowie eine Tiefensuche durch. In beiden Fällen soll der Knoten a als Startknoten gewählt werden. Stelle den jeweils erhaltenen Baum in einer Zeichnung dar. Gibt es mehrere Möglichkeiten, einen Nachbarknoten auszuwählen, so entscheidet die alphabetische Reihenfolge.



© 2018 Steven Köhler

Modulare Arithmetik

© 2018 Steven Köhler

Square-and-Multiply-Verfahren

Das *Square-and-Multiply-Verfahren* ist eine sehr effiziente Methode zum Berechnen von natürlichen Potenzen, also von Ausdrücken der Form a^n mit natürlichem Exponenten n.

Es gilt

$$a^n = \begin{cases} \left(a^{\frac{n}{2}}\right)^2 & \text{, für gerade } n \\ a^{n-1} \cdot a & \text{, für ungerade } n. \end{cases}$$

© 2018 Steven Köhler

Kleiner Satz von Fermat

Es sei p eine Primzahl und a sei eine ganze Zahl, für die $\mathrm{ggT}(a, p) = 1$ gilt; a und p sind also teilerfremd. Dann gilt:

$$a^{p-1} \equiv 1 \pmod{p}.$$

© 2018 Steven Köhler

Aufgabe 11

a) Bestimme den ganzzahligen Rest der Division von 5^{948} durch 23.

b) Bestimme den ganzzahligen Rest der Division von 4^{153} durch 42.

© 2018 Steven Köhler

Restklassenring I

Wir betrachten die Kongruenzrelation $\equiv$ modulo m. Es handelt es sich um eine Äquivalenzrelation, bei deren Äquivalenzklassen es sich um die Restklassen $[0]_m, [1]_m, \ldots, [m-1]_m$ handelt.

Man definiert die Menge $\mathbb{Z}_m$ (oder $\mathbb{Z}/m\mathbb{Z}$) als die Menge der Äquivalenzklassen der Kongruenzrelation modulo m:

$$\mathbb{Z}_m = \left\{ [0]_m, [1]_m, \ldots, [m-1]_m \right\}.$$

Wenn klar ist, dass es sich um Elemente aus $\mathbb{Z}_m$ handelt, kann anstelle von $[0]_m, [1]_m, \ldots, [m-1]_m$ stellvertretend auch einfach $0, 1, \ldots, m-1$ geschrieben werden.

© 2018 Steven Köhler

Restklassenring II

Für alle $x, y \in \mathbb{Z}$ seien die Operationen $\oplus$ und $\odot$ wie folgt definiert:

$$[x]_m \oplus [y]_m = [x + y]_m$$
$$[x]_m \odot [y]_m = [x \cdot y]_m$$

Anstelle von $\oplus$ und $\odot$ wird oft auch nur $+$ und $\cdot$ geschrieben.

Es handelt sich bei $(\mathbb{Z}_m, \oplus, \odot)$ bzw. $(\mathbb{Z}_m, +, \cdot)$ um einen kommutativen Ring.

© 2018 Steven Köhler

Restklassenring III

Für beliebige $[a]_m, [b]_m, [c]_m \in \mathbb{Z}_m$ gilt:

(I) $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$

$[a]_m \odot [b]_m = [b]_m \odot [a]_m$

(II) $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$

$([a]_m \odot [b]_m) \odot [c]_m = [a]_m \odot ([b]_m \odot [c]_m)$

(III) $[a]_m \oplus [0]_m = [a]_m$

$[a]_m \odot [1]_m = [a]_m$

(IV) $[a]_m \odot ([b]_m \oplus [c]_m) = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m)$

(V) $[a]_m \oplus [-a]_m = [0]_m$

© 2018 Steven Köhler

Multiplikatives Inverses

Es sei $[a]_m \in \mathbb{Z}_m$. Ein Element $[x]_m \in \mathbb{Z}_m$ heißt *multiplikatives Inverses* von $[a]_m$, falls gilt:

$$[a]_m \odot [x]_m = [1]_m.$$

Besitzt $[a]_m$ ein multiplikatives Inverses, so nennt man $[a]_m$ *invertierbar*.

Hinweis: Per Konvention wird für das multiplikative Inverse stets der kleinste, nichtnegative Vertreter der entsprechenden Restklasse angegeben.

© 2018 Steven Köhler

Erweiterter Euklidischer Algorithmus

Zum Bestimmen des *multiplikativen Inversen* von x in $\mathbb{Z}_m$ kann der *erweiterte Euklidische Algorithmus* verwendet werden.

- Bestimmen von $\mathrm{ggT}(x, m)$.
- Gilt $\mathrm{ggT}(x, m) \neq 1$, so existiert kein multiplikatives Inverses von x in $\mathbb{Z}_m$.
- Gilt $\mathrm{ggT}(x, m) = 1$, so kann das multiplikatives Inverse durch *Rückwärtseinsetzen* bestimmt werden.

© 2018 Steven Köhler

Aufgabe 12

Bestimme, falls möglich, das multiplikative Inverse. Gib im Falle der Nicht-Existenz eine (kurze) Begründung, weshalb das multiplikative Inverse nicht existiert.

a) 23 in $\mathbb{Z}_{149}$

b) 54 in $\mathbb{Z}_{966}$

c) 1336 in $\mathbb{Z}_{1337}$

© 2018 Steven Köhler

RSA

© 2018 Steven Köhler

Eulersche φ-Funktion

Die *eulersche φ-Funktion* ist eine Funktion, die zu einer natürlichen Zahl n angibt, wie viele zu n teilerfremde natürliche Zahlen es gibt, die kleiner gleich n sind.

$$\varphi(n) = \left|\left\{a \in \mathbb{N} : 1 \leq a \leq n \wedge \mathrm{ggT}(a, n) = 1\right\}\right|$$

© 2018 Steven Köhler

Berechnung der eulerschen φ-Funktion I

Da eine Primzahl p nur durch 1 und sich selbst teilbar ist, ist sie zu den Zahlen 1 bis $p-1$ teilerfremd. Da $p \geq 2$ gilt und somit p niemals zu sich selbst teilerfremd ist, gilt stets

$$\varphi(p) = p - 1.$$

© 2018 Steven Köhler

Berechnung der eulerschen φ-Funktion II

Sind m und n zwei teilerfremde ganze Zahlen, so gilt:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

© 2018 Steven Köhler

Berechnung der eulerschen φ-Funktion III

Eine Potenz p^k einer Primzahl p besitzt als einzigen Primfaktor die Zahl p. Daher hat p^k nur mit Vielfachen von p einen von 1 verschiedenen gemeinsamen Teiler. Im Bereich $1, \ldots, p^k$ sind dies die Zahlen

$$1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p.$$

Es gibt also insgesamt p^{k-1} Zahlen, die nicht teilerfremd zu p^k sind. Für die eulersche φ-Funktion gilt folglich:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1) = p^k \cdot \left(1 - \frac{1}{p}\right).$$

© 2018 Steven Köhler

Berechnung der eulerschen φ-Funktion IV

Der Wert der eulerschen φ-Funktion lässt sich für jede natürliche Zahl n aus deren Primfaktorzerlegung berechnen. Hierbei sei

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Dann gilt

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}).$$

© 2018 Steven Köhler

Aufgabe 13

Berechne $\varphi(24)$!

Überprüfe dein Ergebnis, indem du alle zu 24 teilerfremden Zahlen a mit $1 \leq a \leq 24$ auflistest.

© 2018 Steven Köhler

Satz von Euler

Es seien a und n zwei natürliche Zahlen mit $\mathrm{ggT}(a, n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dieser Satz ist auch als *Satz von Euler-Fermat* bekannt.

© 2018 Steven Köhler

Beschreibung des RSA-Verfahrens I

Zum Erzeugen des öffentlichen und des privaten Schlüssels werden die folgenden Schritte ausgeführt:

1. Auswahl von zwei verschiedenen Primzahlen p und q.
2. Bestimmen des RSA-Moduls $N = p \cdot q$.
3. Berechnen des Werts $\varphi(N) = (p-1) \cdot (q-1)$.
4. Auswahl einer zu $\varphi(N)$ teilerfremden Zahl e mit $1 < e < \varphi(N)$.
5. Berechnen des Werts d mit $1 < d < \varphi(N)$, so dass gilt:

$$e \cdot d \equiv 1 \pmod{\varphi(N)}.$$

Man erhält den *öffentlichen Schlüssel* (e, N) sowie den *privaten Schlüssel* (d, N).

© 2018 Steven Köhler

Beschreibung des RSA-Verfahrens II

Beim *Verschlüsseln* einer Nachricht m (mit $1 \leq m < N$) kann die verschlüsselte Nachricht c (mit $1 \leq c < N$) wie folgt berechnet werden:

$$m^e \equiv c \pmod{N}.$$

Beim *Entschlüsseln* einer verschlüsselten Nachricht c kann die ursprüngliche Nachricht m wie folgt berechnet werden:

$$c^d \equiv m \pmod{N}.$$

© 2018 Steven Köhler

Aufgabe 14

Gegeben seien die beiden Primzahlen $p = 13$ und $q = 17$.

a) Bestimme den öffentlichen Schlüssel (e, N) sowie den privaten Schlüssel (d, N). Es gelte $e = 23$.

b) Verschlüssle die Nachricht $m = 42$.

c) Entschlüssle die in b) erhaltene verschlüsselte Nachricht und überprüfe, ob es sich tatsächlich wieder um die ursprüngliche Nachricht m handelt.

© 2018 Steven Köhler

Aufgabe 15

Es seien die Bezeichnungen wie in der Beschreibung des RSA-Verfahrens. Zeige, dass es sich bei c^d tatsächlich um die ursprüngliche Nachricht m handelt.

© 2018 Steven Köhler

Aufgabe 16

Es seien der öffentliche RSA-Schlüssel $(47, 253)$ sowie die verschlüsselte Nachricht $c = 42$ gegeben. Wie lautet die unverschlüsselte Nachricht m?

© 2018 Steven Köhler