Karlsruher Institut für Technologie

Algorithmen II
Übung am 27.11.2012

INSTITUT FÜR THEORETISCHE INFORMATIK · PROF. DR. DOROTHEA WAGNER

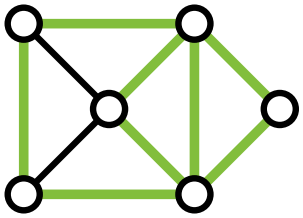
Kreisbasen

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

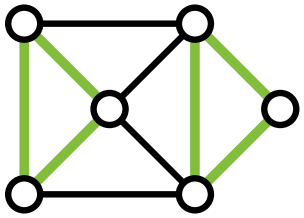
Kreise in Graphen

Definition: Kreis **(Definition 5.1)**

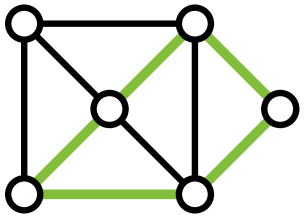
Ein Teilgraph $C = (V_C, E_C)$ von $G = (V, E)$ (d.h. $V_c \subseteq V, E_c \subseteq E$) heißt *Kreis* in G, falls alle Knoten aus V_C in C geraden Grad haben. Falls C zusammenhängend ist und alle Knoten aus V_C Grad zwei haben, so heißt C *einfacher Kreis*.



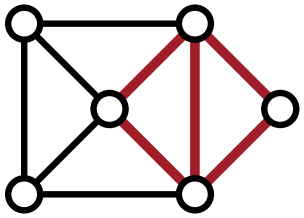
Kreis



Kreis



einfacher Kreis

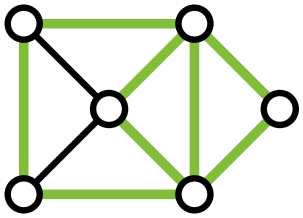


kein Kreis

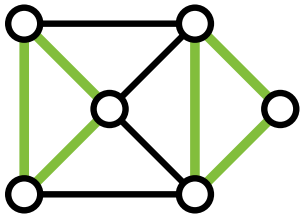
Kreise in Graphen

Definition: Kreis **(Definition 5.1)**

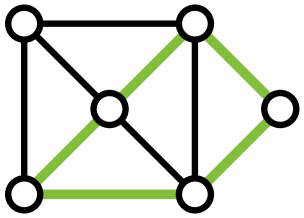
Ein Teilgraph $C = (V_C, E_C)$ von $G = (V, E)$ (d.h. $V_c \subseteq V, E_c \subseteq E$) heißt *Kreis* in G, falls alle Knoten aus V_C in C geraden Grad haben. Falls C zusammenhängend ist und alle Knoten aus V_C Grad zwei haben, so heißt C *einfacher Kreis*.



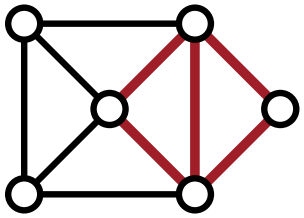
Kreis



Kreis



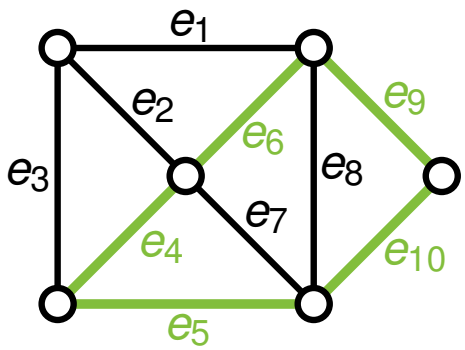
einfacher Kreis



kein Kreis

Fasse Kreis als Kantenmenge $E' \subseteq E = \{e_1, \ldots, e_m\}$ auf und kodiere E' als Vektor $X^{E'}$ mit

$$X_i^{E'} := \begin{cases} 1, & \text{falls } e_i \in E' \\ 0, & \text{sonst} \end{cases}$$



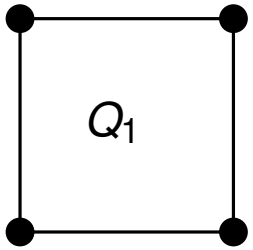
$$X^{E'} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \\ e_{10} \end{matrix}$$

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.

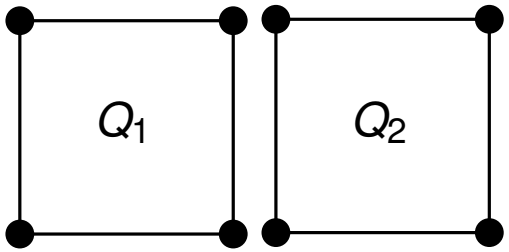
Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



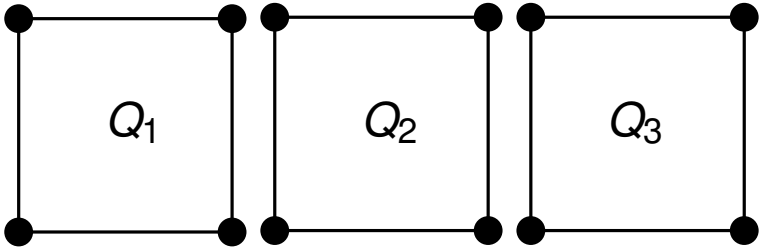
G_1

$|\mathcal{C}_1| = 1$



G_2

$|\mathcal{C}_2| = 3$



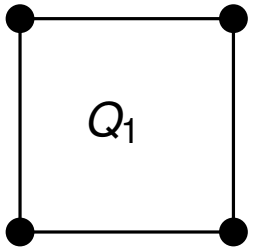
G_3

$|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

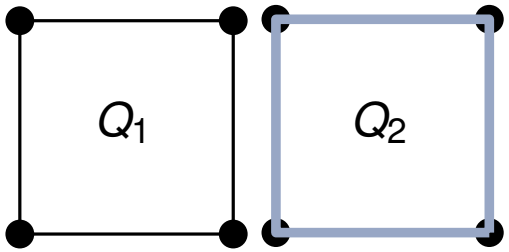
Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



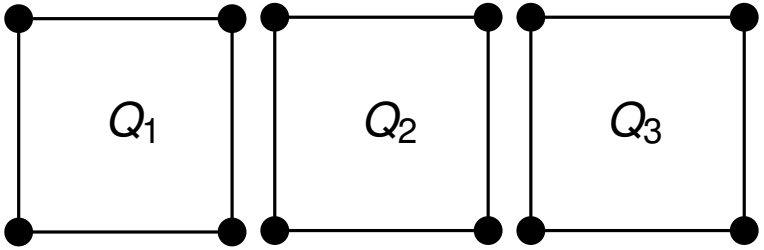
G_1

$|\mathcal{C}_1| = 1$



G_2

$|\mathcal{C}_2| = 3$



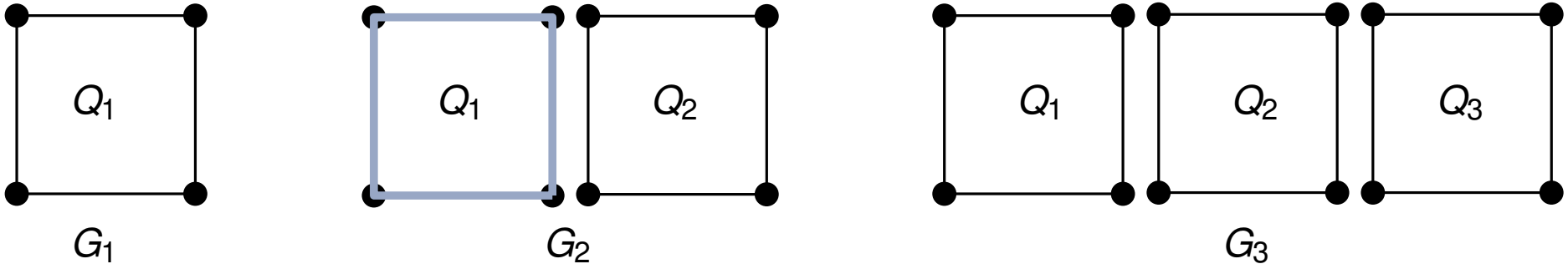
G_3

$|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



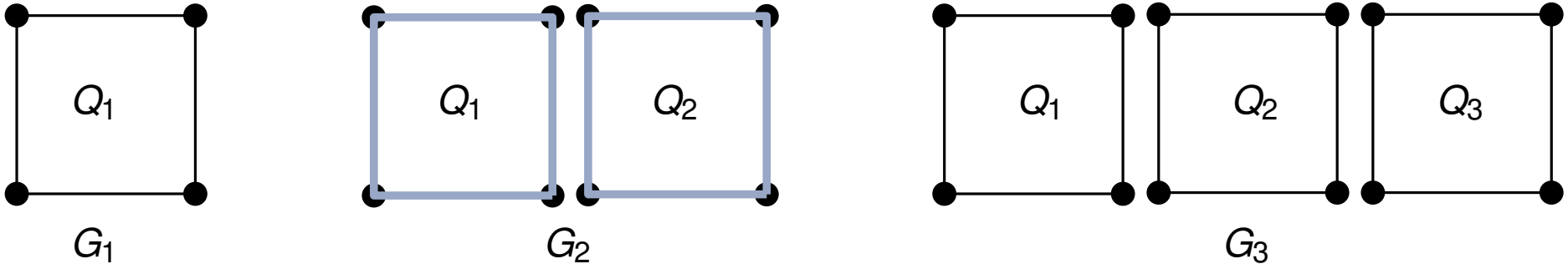
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



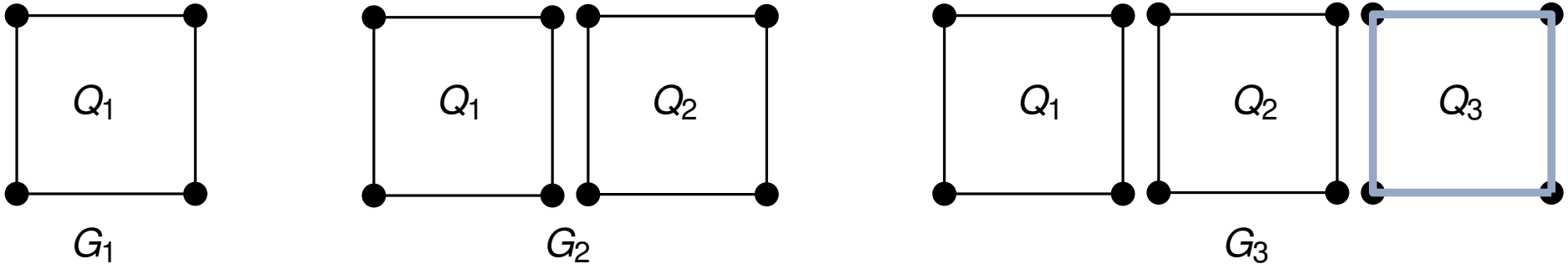
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



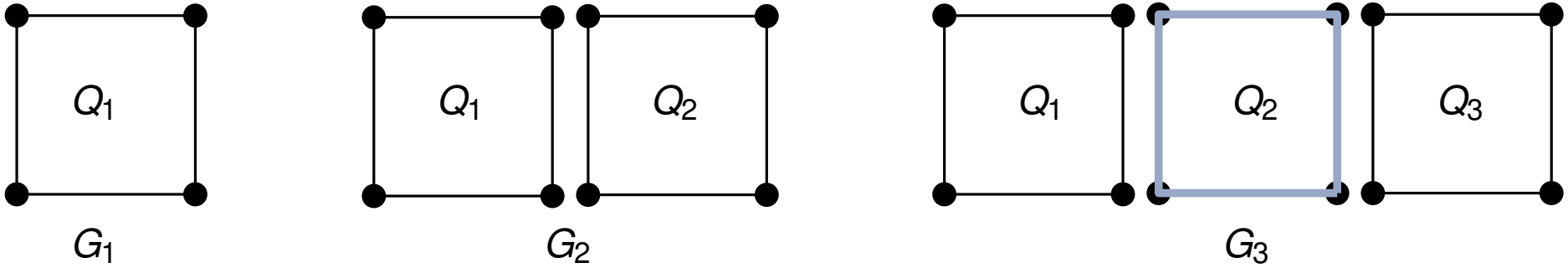
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



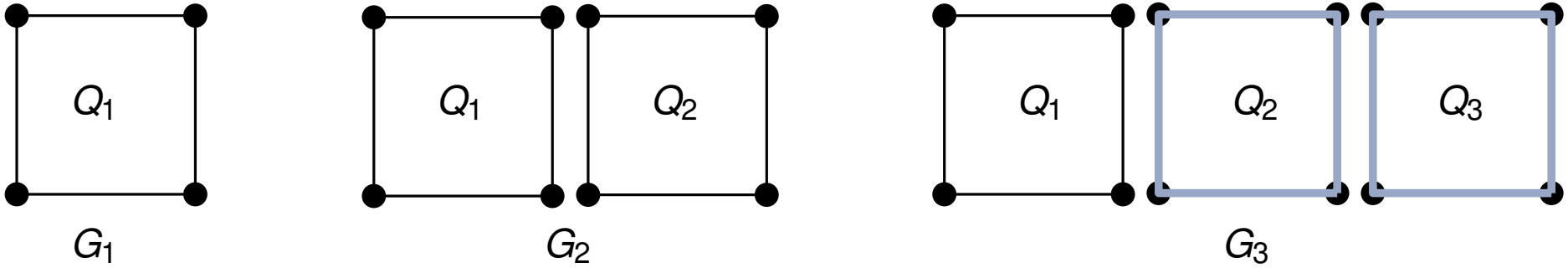
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



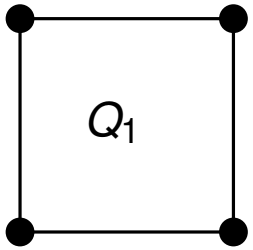
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

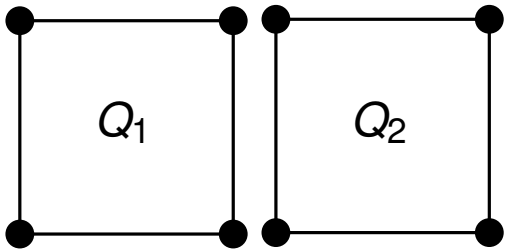
Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



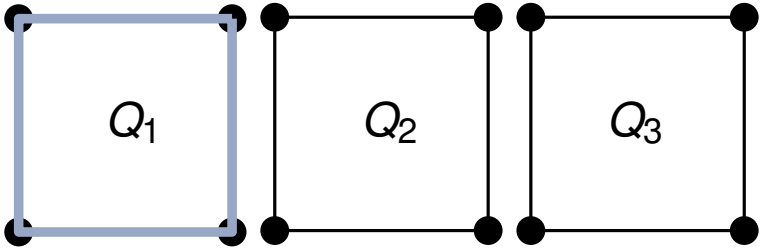
G_1

$|\mathcal{C}_1| = 1$



G_2

$|\mathcal{C}_2| = 3$



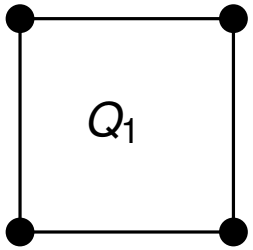
G_3

$|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

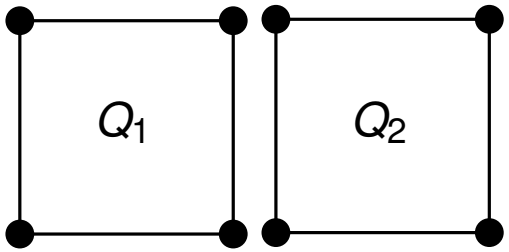
Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



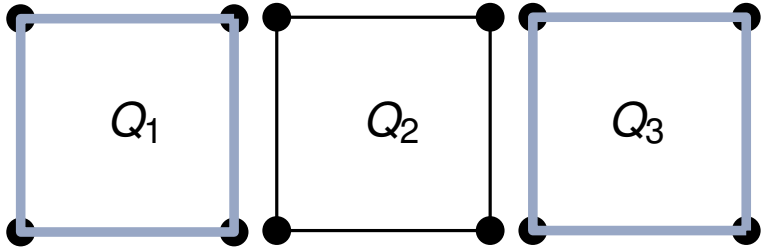
G_1

$|\mathcal{C}_1| = 1$



G_2

$|\mathcal{C}_2| = 3$



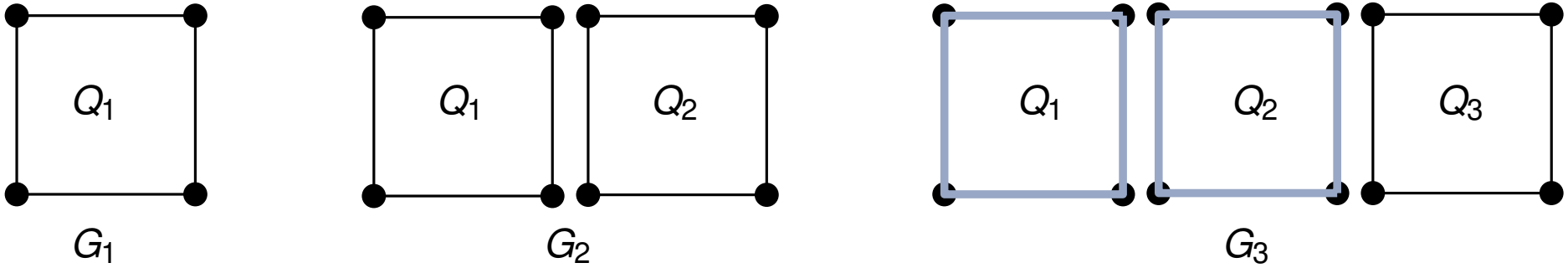
G_3

$|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



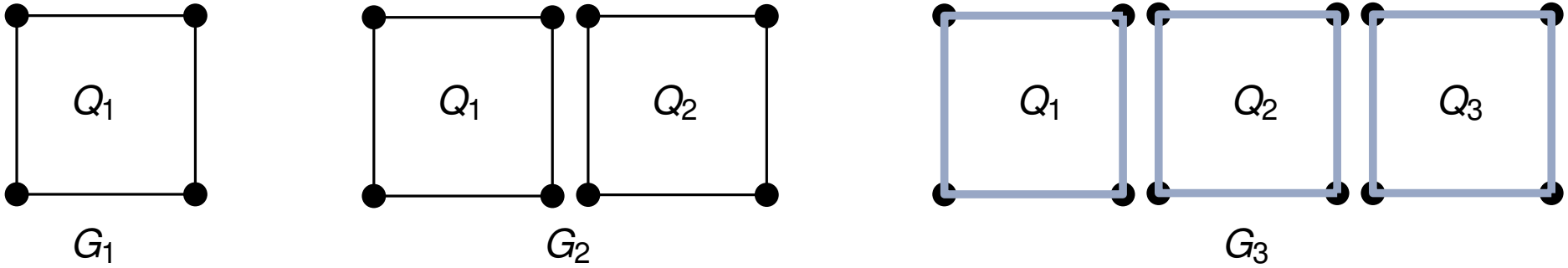
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



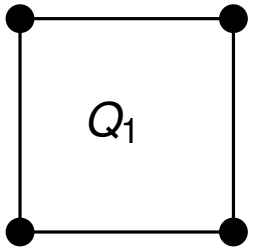
G_1 G_2 G_3

$|\mathcal{C}_1| = 1$ $|\mathcal{C}_2| = 3$ $|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

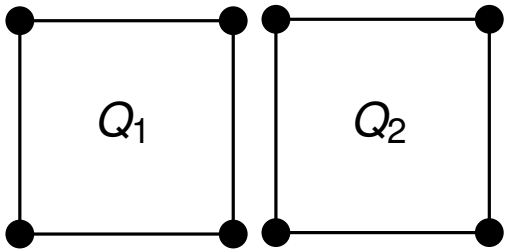
Problem 3

(a) Gesucht: Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **exponentiell** in $|E_i|$.



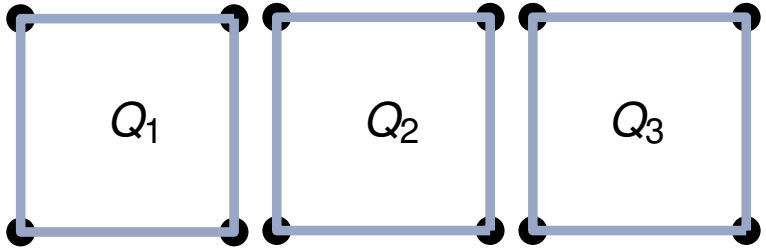
G_1

$|\mathcal{C}_1| = 1$



G_2

$|\mathcal{C}_2| = 3$



G_3

$|\mathcal{C}_3| = 7$

$G_i = i$ Kopien eines einfachen Kreises Q mit 4 Knoten. (Anzahl Kanten steigt linear)

Ein Kreis C in G_i setzt sich aus einer beliebigen Kombination von $Q_1, \ldots, Q_i$ zusammen:

Für alle $j = 1 \ldots, i$ gilt: Entweder ganz Q_j ist in C enthalten oder gar nicht.

Beschreibe C als binären Vektor $v = (b_1, \ldots, b_i)$:

$$b_j := \begin{cases} 1 & Q_j \text{ ist in } C \text{ enthalten} \\ 0 & \textit{sonst} \end{cases}$$

Es gibt $2^i - 1$ gültige Kombinationen. Nullvektor gehört nicht dazu.

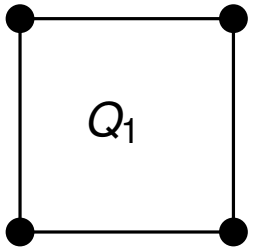
Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 3

b) Gesucht ist Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **linear** in $|E_i|$:

Problem 3

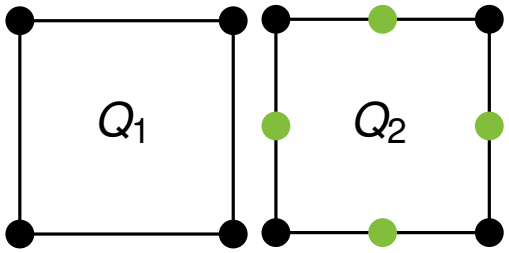
b) Gesucht ist Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **linear** in $|E_i|$:



G_1

$|\mathcal{C}_1| = 1$

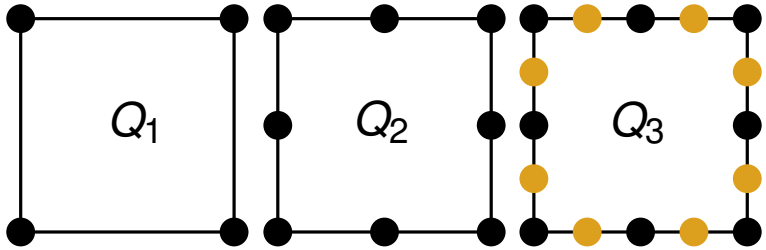
$|E_1| = 4$



G_2

$|\mathcal{C}_2| = 3$

$|E_2| = 4 + 8$



G_3

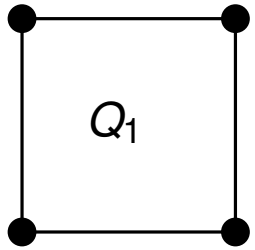
$|\mathcal{C}_3| = 7$

$|E_3| = 4 + 8 + 16$

Familie G_i der 4er-Kreis-Kopien mit Unterteilungen.

Problem 3

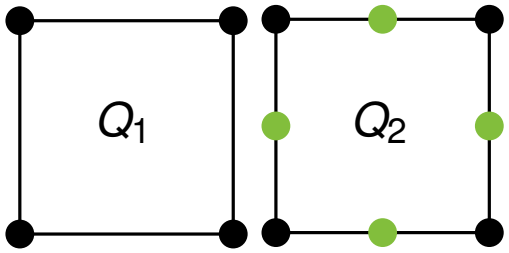
b) Gesucht ist Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **linear** in $|E_i|$:



G_1

$|\mathcal{C}_1| = 1$

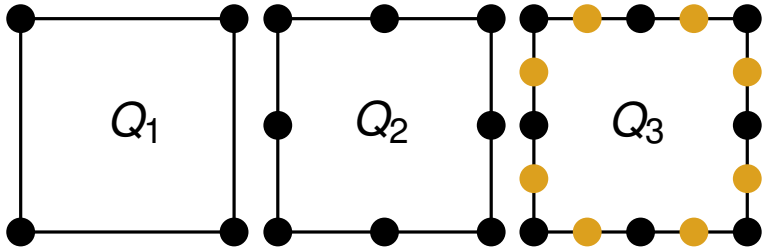
$|E_1| = 4$



G_2

$|\mathcal{C}_2| = 3$

$|E_2| = 4 + 8$



G_3

$|\mathcal{C}_3| = 7$

$|E_3| = 4 + 8 + 16$

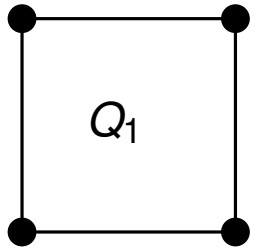
Familie G_i der 4er-Kreis-Kopien mit Unterteilungen.

$$|E_i| = \sum_{j=0}^{i-1} 4 \cdot 2^j = 4 \sum_{j=0}^{i-1} 2^j = 4(2^i - 1) = 4 \cdot 2^i - 4$$

(Verwende geometrische Reihe.)

Problem 3

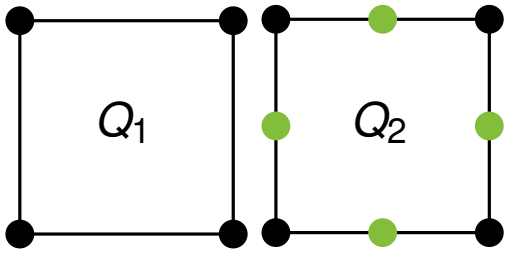
b) Gesucht ist Familie $(G_i)_{i \in \mathbb{N}}$ mit $|\mathcal{C}_i|$ **linear** in $|E_i|$:



G_1

$|\mathcal{C}_1| = 1$

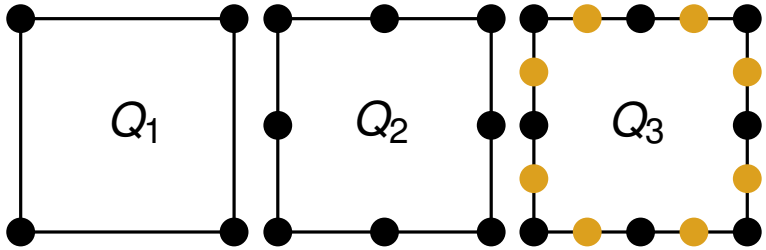
$|E_1| = 4$



G_2

$|\mathcal{C}_2| = 3$

$|E_2| = 4 + 8$



G_3

$|\mathcal{C}_3| = 7$

$|E_3| = 4 + 8 + 16$

Familie G_i der 4er-Kreis-Kopien mit Unterteilungen.

$$|E_i| = \sum_{j=0}^{i-1} 4 \cdot 2^j = 4 \sum_{j=0}^{i-1} 2^j = 4(2^i - 1) = 4 \cdot 2^i - 4$$

(Verwende geometrische Reihe.)

Ein Kreis C in G_i setzt sich weiterhin aus einer beliebigen Kombination von $Q_1, \ldots, Q_i$ zusammen:

Entweder ganz Q_i ist in C enthalten oder gar nicht.

Deshalb: $|\mathcal{C}_i| = 2^i - 1$

Kreisraum

Definition: Kreisraum
Sei $\mathcal{C}$ die Menge aller Kreise in $G = (V, E)$. Dann induziert $\mathcal{C}$ den Vektorraum der Vektoren X^c, $c \in \mathcal{C}$ über dem Körper GF(2), genannt *Kreisraum* von G.

Erinnerung: $GF(2)$ ist der Körper mit zwei Elementen $\{0, 1\}$ und den Verknüpfungen + und $\cdot$ mit

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$a_1 + \ldots + a_k = 1 \Leftrightarrow$ **ungerade** Anzahl a_i auf 1 gesetzt.
$a_1 + \ldots + a_k = 0 \Leftrightarrow$ **gerade** Anzahl a_i auf 1 gesetzt.

Kreisraum

Definition: Kreisraum

Sei $\mathcal{C}$ die Menge aller Kreise in $G = (V, E)$. Dann induziert $\mathcal{C}$ den Vektorraum der Vektoren X^c, $c \in \mathcal{C}$ über dem Körper GF(2), genannt *Kreisraum* von G.

Erinnerung: $GF(2)$ ist der Körper mit zwei Elementen $\{0, 1\}$ und den Verknüpfungen + und · mit

+	0	1
0	0	1
1	1	0

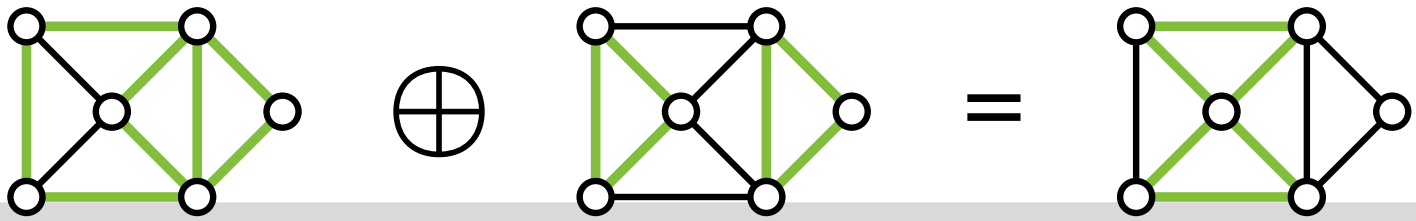
·	0	1
0	0	0
1	0	1

$a_1 + \ldots + a_k = 1 \Leftrightarrow$ **ungerade** Anzahl a_i auf 1 gesetzt.

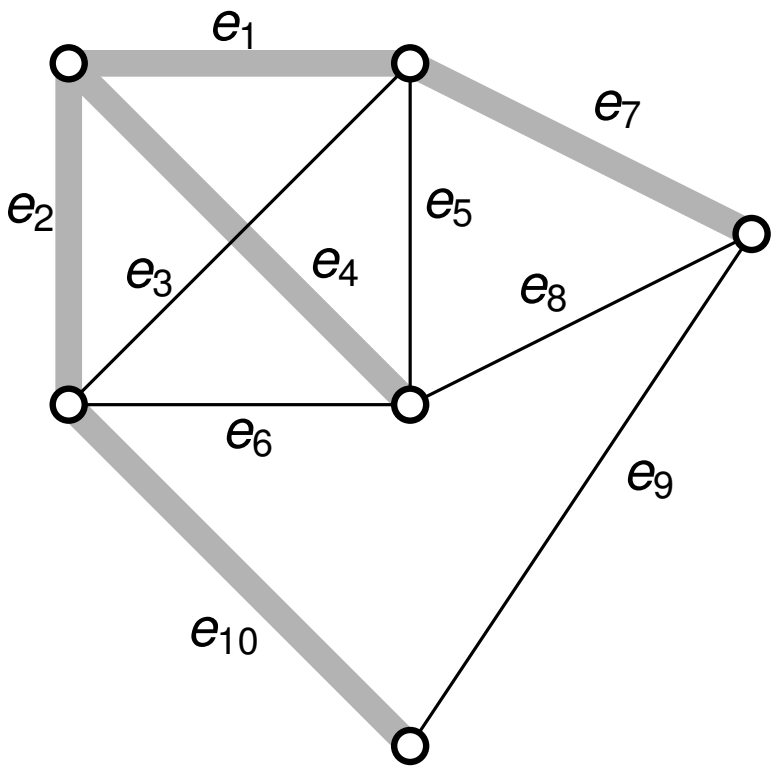
$a_1 + \ldots + a_k = 0 \Leftrightarrow$ **gerade** Anzahl a_i auf 1 gesetzt.

Definition: Summe von Kreisen – symmetrische Differenz

Die Addition im Kreisraum von G induziert eine Operation $\oplus$ auf C durch $c_1 \oplus c_2 = (E_{c_1} \cup E_{c_2}) \setminus (E_{c_1} \cap E_{c_2})$. Dies ist die *symmetrische Differenz* beider Kantenmengen.

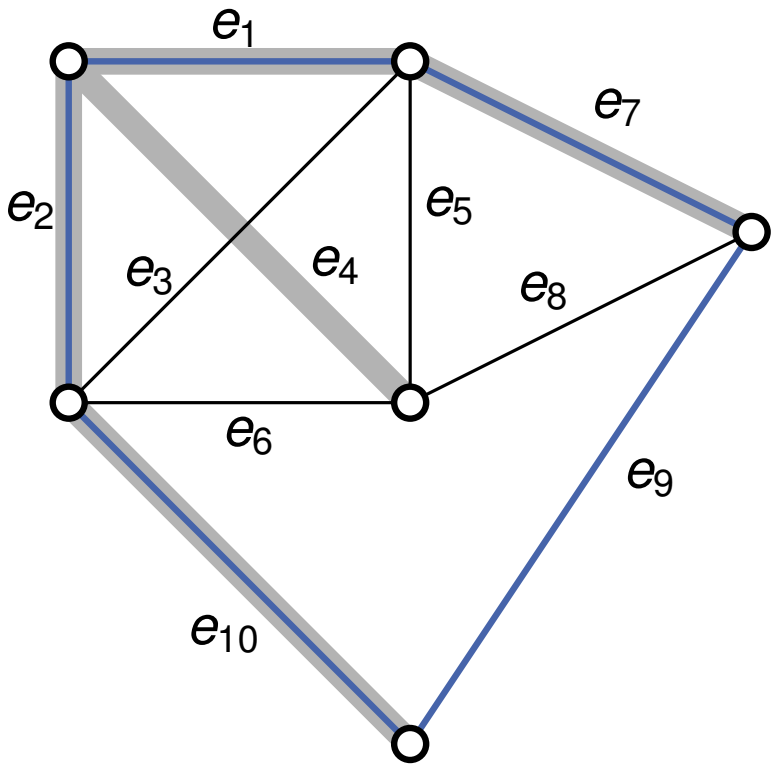


Fundamentalbasis



Spannbaum T:

Fundamentalbasis

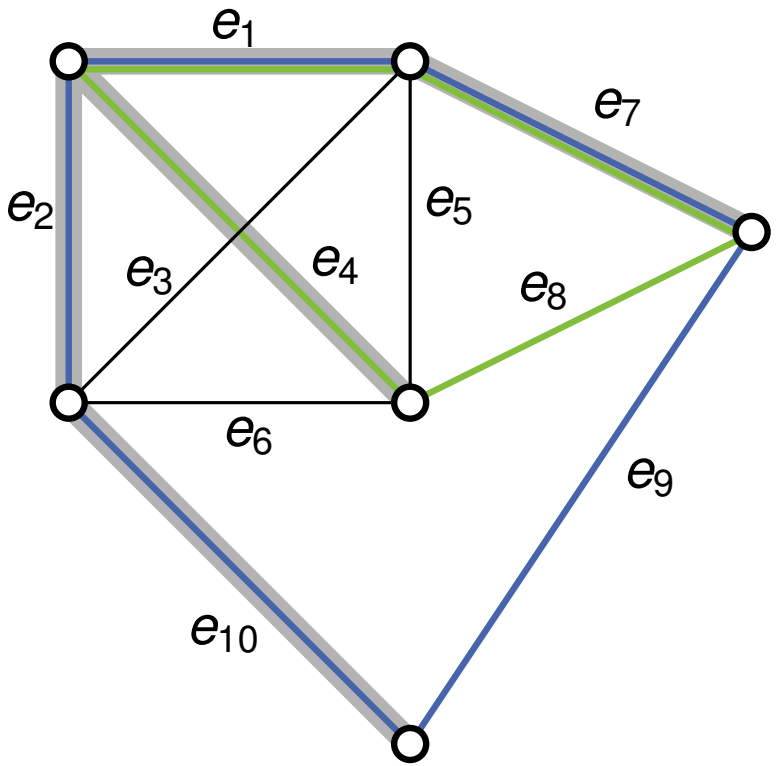


Spannbaum T:

Kante e_9 induziert Kreis:

$C_1 = e_1 - e_7 - e_9 - e_{10} - e_2$

Fundamentalbasis



Spannbaum T:

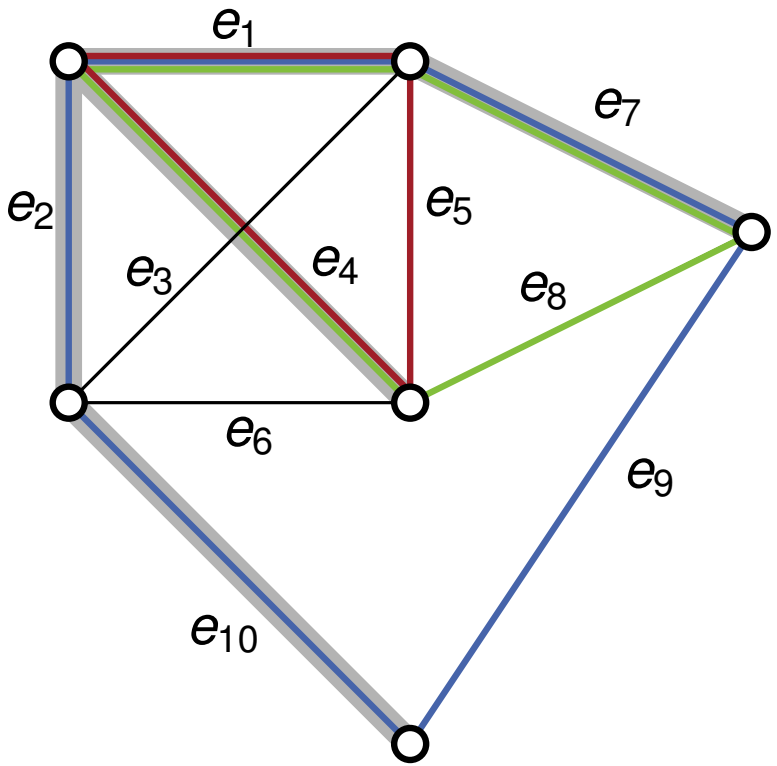
Kante e_9 induziert Kreis:

$C_1 = e_1 - e_7 - e_9 - e_{10} - e_2$

Kante e_8 induziert Kreis:

$C_2 = e_1 - e_7 - e_8 - e_4$

Fundamentalbasis



Spannbaum T:

Kante e_9 induziert Kreis:

$C_1 = e_1 - e_7 - e_9 - e_{10} - e_2$

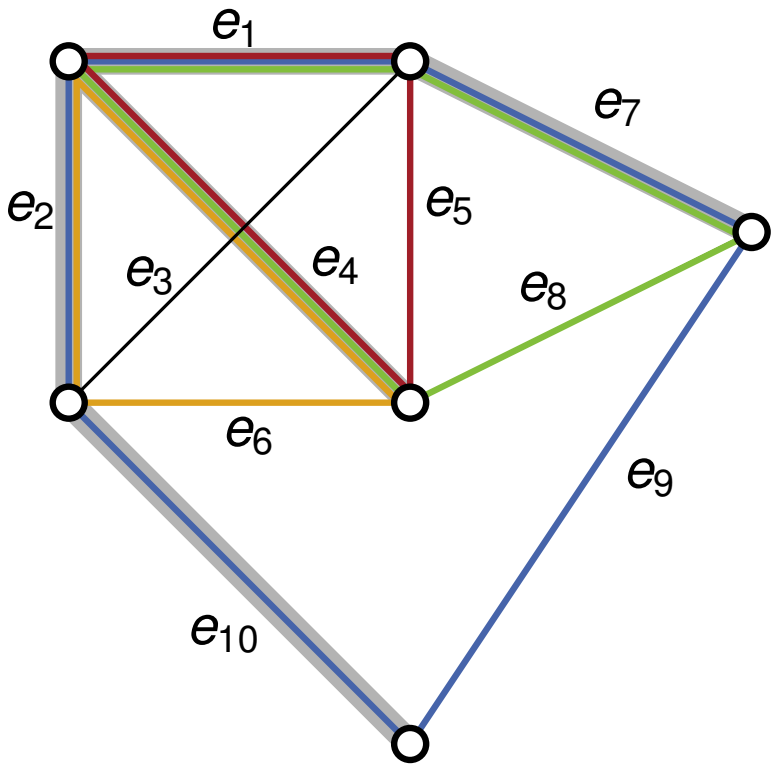
Kante e_8 induziert Kreis:

$C_2 = e_1 - e_7 - e_8 - e_4$

Kante e_5 induziert Kreis:

$C_3 = e_1 - e_5 - e_4$

Fundamentalbasis



Spannbaum T:

Kante e_9 induziert Kreis:

$C_1 = e_1 - e_7 - e_9 - e_{10} - e_2$

Kante e_8 induziert Kreis:

$C_2 = e_1 - e_7 - e_8 - e_4$

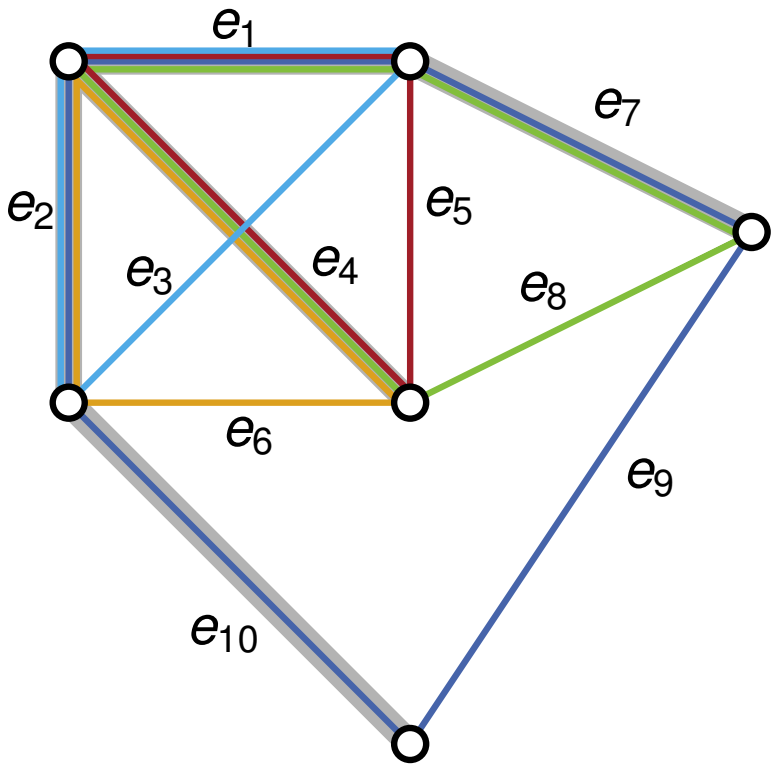
Kante e_5 induziert Kreis:

$C_3 = e_1 - e_5 - e_4$

Kante e_6 induziert Kreis:

$C_4 = e_2 - e_4 - e_6$

Fundamentalbasis



Spannbaum T:

Kante e_9 induziert Kreis:

$C_1 = e_1 - e_7 - e_9 - e_{10} - e_2$

Kante e_8 induziert Kreis:

$C_2 = e_1 - e_7 - e_8 - e_4$

Kante e_5 induziert Kreis:

$C_3 = e_1 - e_5 - e_4$

Kante e_6 induziert Kreis:

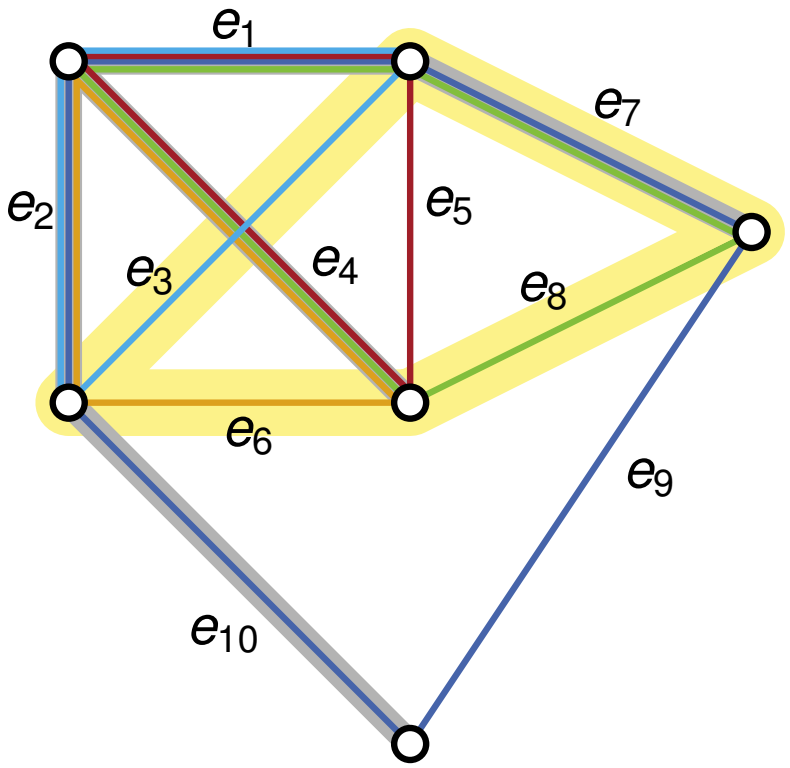
$C_4 = e_2 - e_4 - e_6$

Kante e_3 induziert Kreis:

$C_5 = e_1 - e_3 - e_2$

C_1, C_2, C_3, C_4 und C_5 bilden Fundamentalbasis.

Fundamentalbasis



Spannbaum T:

Kante e_9 induziert Kreis:

$C_1 = e_1 - e_7 - e_9 - e_{10} - e_2$

Kante e_8 induziert Kreis:

$C_2 = e_1 - e_7 - e_8 - e_4$

Kante e_5 induziert Kreis:

$C_3 = e_1 - e_5 - e_4$

Kante e_6 induziert Kreis:

$C_4 = e_2 - e_4 - e_6$

Kante e_3 induziert Kreis:

$C_5 = e_1 - e_3 - e_2$

C_1, C_2, C_3, C_4 und C_5 bilden Fundamentalbasis.

Darstellung anderer Kreise bezüglich der gewählten Basis:

$e_3 - e_7 - e_8 - e_6 = e_1 - e_7 - e_8 - e_4 \oplus e_2 - e_4 - e_6 \oplus e_1 - e_3 - e_2$

2. Problem

Gegeben:

- ungerichteter, zusammenhängender Graph $G = (V, E)$
- aufspannender Baum $T = (V, E_T)$ in G

Fundamentalbasis B_t des Kreisraumes $\mathcal{C}$ von G definiert als

$$B_T := \{C_e \mid e \in E \setminus E_T,\ C_e \in \mathcal{C},\ \textit{mit}$$
$$E_{C_e} = \{e = \{u, v\}\} \cup \{\text{Pfadkanten von } u \text{ nach } v \text{ in } T\}\}$$

2. Problem

Gegeben:

- ungerichteter, zusammenhängender Graph $G = (V, E)$
- aufspannender Baum $T = (V, E_T)$ in G

Fundamentalbasis B_t des Kreisraumes $\mathcal{C}$ von G definiert als

$$B_T := \{C_e \mid e \in E \setminus E_T,\ C_e \in \mathcal{C},\ mit$$
$$E_{C_e} = \{e = \{u, v\}\} \cup \{\text{Pfadkanten von } u \text{ nach } v \text{ in } T\}\}$$

1. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ linear unabhängig ist.

Wiederholung: Eine Teilmenge $B = \{b_1, \ldots, b_n\} \subseteq V$ eines K-Vektorraums V heißt *linear unabhängig*, wenn gilt:

$$\sum_{i=1}^{i=n} a_i b_i = 0,\ a_i \in K \quad \Longleftrightarrow \quad a_i = 0 \quad \forall\, i,$$

d.h., der Nullvektor lässt sich nur als triviale Linearkombination der Vektoren in B schreiben.

2. Problem

Gegeben:

- ungerichteter, zusammenhängender Graph $G = (V, E)$
- aufspannender Baum $T = (V, E_T)$ in G

Fundamentalbasis B_t des Kreisraumes $\mathcal{C}$ von G definiert als

$$B_T := \{C_e \mid e \in E \setminus E_T,\ C_e \in \mathcal{C},\ mit$$
$$E_{C_e} = \{e = \{u, v\}\} \cup \{\text{Pfadkanten von } u \text{ nach } v \text{ in } T\}\}$$

1. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ linear unabhängig ist.

- Nach Definition von B_T: Jede Nichtbaumkante nur in einem Kreis in B_T enthalten.

2. Problem

Gegeben:

- ungerichteter, zusammenhängender Graph $G = (V, E)$
- aufspannender Baum $T = (V, E_T)$ in G

Fundamentalbasis B_t des Kreisraumes $\mathcal{C}$ von G definiert als

$$B_T := \{C_e \mid e \in E \setminus E_T,\ C_e \in \mathcal{C},\ \textit{mit}$$
$$E_{C_e} = \{e = \{u, v\}\} \cup \{\text{Pfadkanten von } u \text{ nach } v \text{ in } T\}\}$$

1. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ linear unabhängig ist.

- Nach Definition von B_T: Jede Nichtbaumkante nur in einem Kreis in B_T enthalten.
- Annahme: Sei $\sum_{e \in E \setminus E_T} a_e C_e = 0$, mit $a_{e'} \neq 0$, für mindestens ein e'.

2. Problem

Gegeben:

- ungerichteter, zusammenhängender Graph $G = (V, E)$
- aufspannender Baum $T = (V, E_T)$ in G

Fundamentalbasis B_t des Kreisraumes $\mathcal{C}$ von G definiert als

$$B_T := \{C_e \mid e \in E \setminus E_T,\ C_e \in \mathcal{C},\ mit$$
$$E_{C_e} = \{e = \{u, v\}\} \cup \{\text{Pfadkanten von } u \text{ nach } v \text{ in } T\}\}$$

1. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ linear unabhängig ist.

- Nach Definition von B_T: Jede Nichtbaumkante nur in einem Kreis in B_T enthalten.
- Annahme: Sei $\sum_{e \in E \setminus E_T} a_e C_e = 0$, mit $a_{e'} \neq 0$, für mindestens ein e'.
- Entsprechender Kreis $C_{e'}$ enthält dann die Nichtbaumkante e', die in keinem anderen Kreis aus B_T enthalten ist .

2. Problem

Gegeben:

- ungerichteter, zusammenhängender Graph $G = (V, E)$
- aufspannender Baum $T = (V, E_T)$ in G

Fundamentalbasis B_t des Kreisraumes $\mathcal{C}$ von G definiert als

$$B_T := \{C_e \mid e \in E \setminus E_T,\ C_e \in \mathcal{C},\ mit$$
$$E_{C_e} = \{e = \{u, v\}\} \cup \{\text{Pfadkanten von } u \text{ nach } v \text{ in } T\}\}$$

1. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ linear unabhängig ist.

- Nach Definition von B_T: Jede Nichtbaumkante nur in einem Kreis in B_T enthalten.
- Annahme: Sei $\sum_{e \in E \setminus E_T} a_e C_e = 0$, mit $a_{e'} \neq 0$, für mindestens ein e'.
- Entsprechender Kreis $C_{e'}$ enthält dann die Nichtbaumkante e', die in keinem anderen Kreis aus B_T enthalten ist .
- Kann nicht zu Null summiert werden, da die hier betrachtete Verknüpfung die *symmetrische Differenz* ist.

Annahme ist widerlegt.

2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

2. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ ein Erzeugendensystem von $\mathcal{C}$ ist.

Hinweis:

Gehen Sie dabei konstruktiv vor und beschreiben Sie, wie ein beliebiger Kreis durch eine Linearkombination von Elementen aus B_T gebildet werden kann.

2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

2. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ ein Erzeugendensystem von $\mathcal{C}$ ist.

Hinweis:
Gehen Sie dabei konstruktiv vor und beschreiben Sie, wie ein beliebiger Kreis durch eine Linearkombination von Elementen aus B_T gebildet werden kann.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

Wdh.: C_e ist eindeutiger Kreis in gegebener Fundamentalbasis B_T über Nichtbaumkante e.

2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

2. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ ein Erzeugendensystem von $\mathcal{C}$ ist.

Hinweis:
Gehen Sie dabei konstruktiv vor und beschreiben Sie, wie ein beliebiger Kreis durch eine Linearkombination von Elementen aus B_T gebildet werden kann.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

Wdh.: C_e ist eindeutiger Kreis in gegebener Fundamentalbasis B_T über Nichtbaumkante e.

Betrachte Linearkombination $\sum_{e \in E_C \setminus E_T} C_e$ und zeige für beliebige Kante $e \in E$:

- Falls $e \in E_C$: e bleibt in Linearkombination erhalten.
- Falls $e \notin E_C$: e bleibt in Linearkombination nicht erhalten.

2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

2. Zeigen Sie, dass $B_T \subseteq GF(2)^m$ ein Erzeugendensystem von $\mathcal{C}$ ist.

Hinweis:
Gehen Sie dabei konstruktiv vor und beschreiben Sie, wie ein beliebiger Kreis durch eine Linearkombination von Elementen aus B_T gebildet werden kann.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

Wdh.: C_e ist eindeutiger Kreis in gegebener Fundamentalbasis B_T über Nichtbaumkante e.

Betrachte Linearkombination $\sum_{e \in E_C \setminus E_T} C_e$ und zeige für beliebige Kante $e \in E$:

- Falls $e \in E_C$: e bleibt in Linearkombination erhalten.
- Falls $e \notin E_C$: e bleibt in Linearkombination nicht erhalten.

Betrachte die Fälle:

1. e ist Nichtbaumkante in C: $e \in E_C \setminus E_T$
2. e ist Baumkante in C: $e \in E_C \cap E_T$
3. e ist Nichtbaumkante außerhalb von C: $e \in E \setminus (E_C \cup E_T)$
4. e ist Baumkante außerhalb von C: $e \in E_T \setminus E_C$

2. Problem

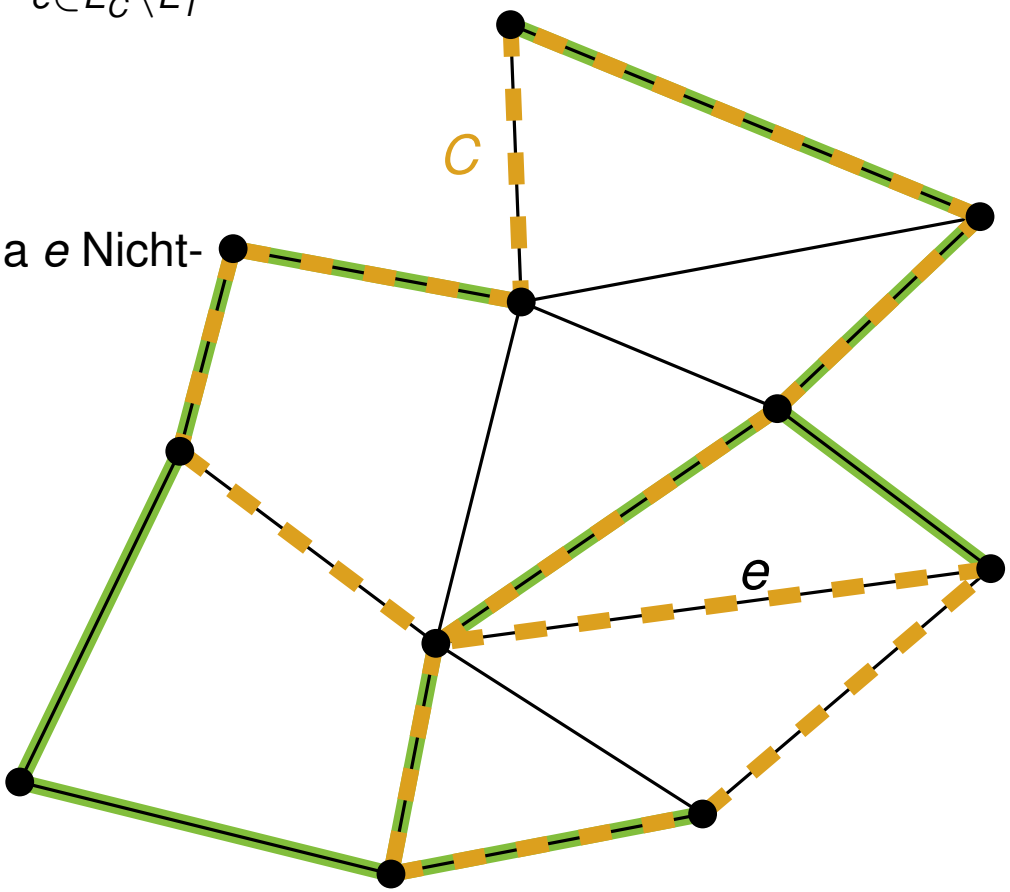
E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

1. Fall: $e \in E_C \setminus E_T$

- C_e kommt als Summand vor.
- e kommt nur einmal in Summe vor, da e Nichtbaumkante ist.

$\Rightarrow$ Summe erhält e.

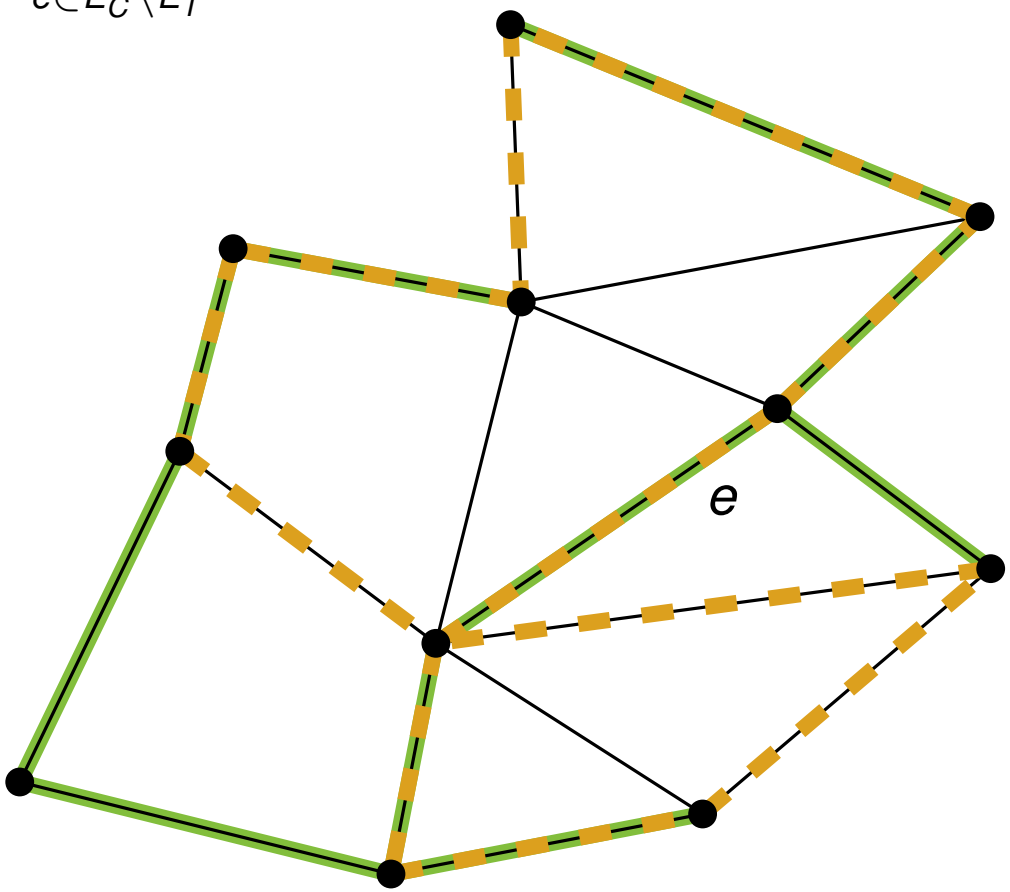


2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

2. Fall: $e \in E_C \cap E_T$



2. Problem

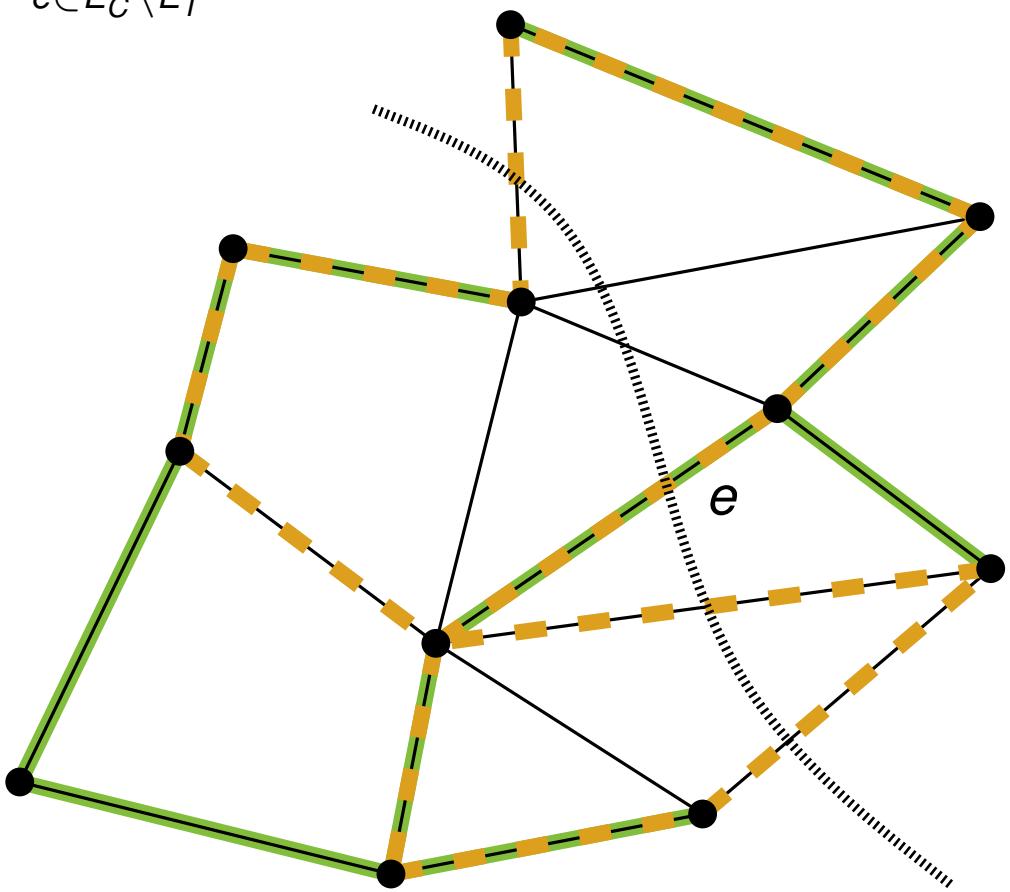
E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

2. Fall: $e \in E_C \cap E_T$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist **gerade**:

  Gilt für jeden Schnitt und Kreis.



2. Problem

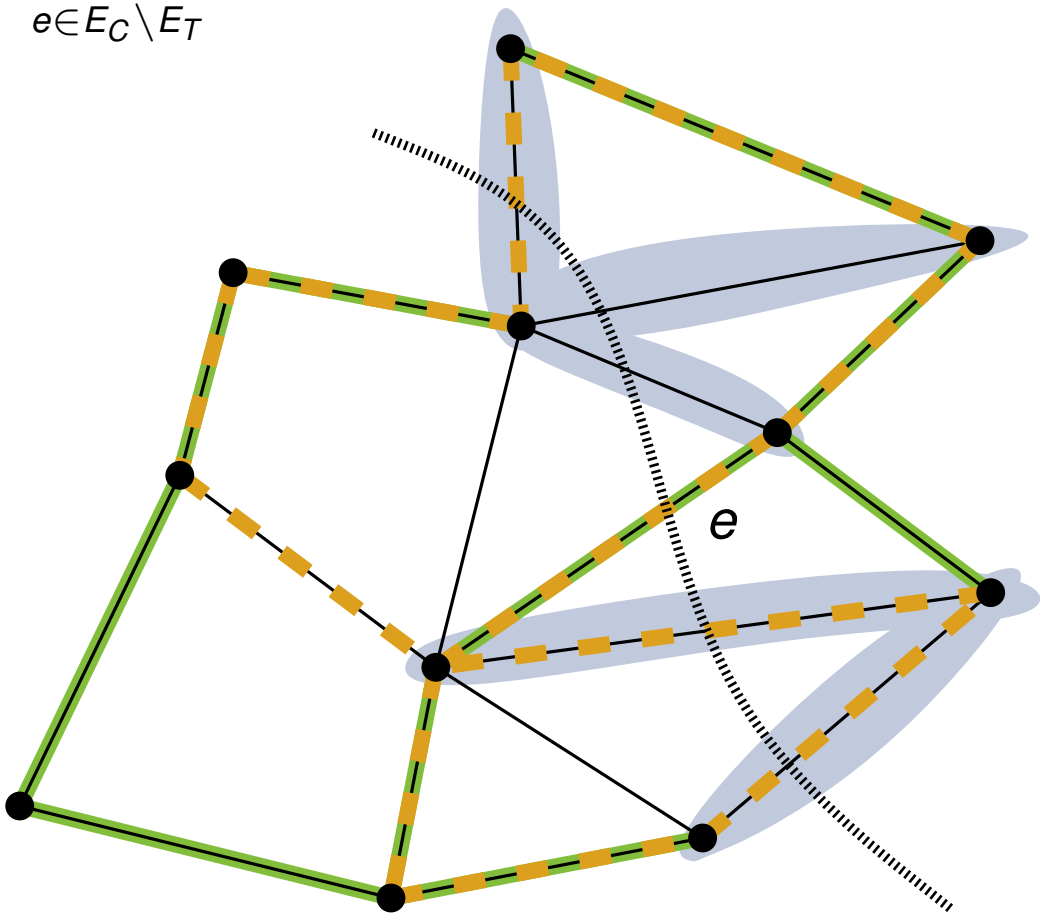
E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

2. Fall: $e \in E_C \cap E_T$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist **gerade**:

  Gilt für jeden Schnitt und Kreis.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.



2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

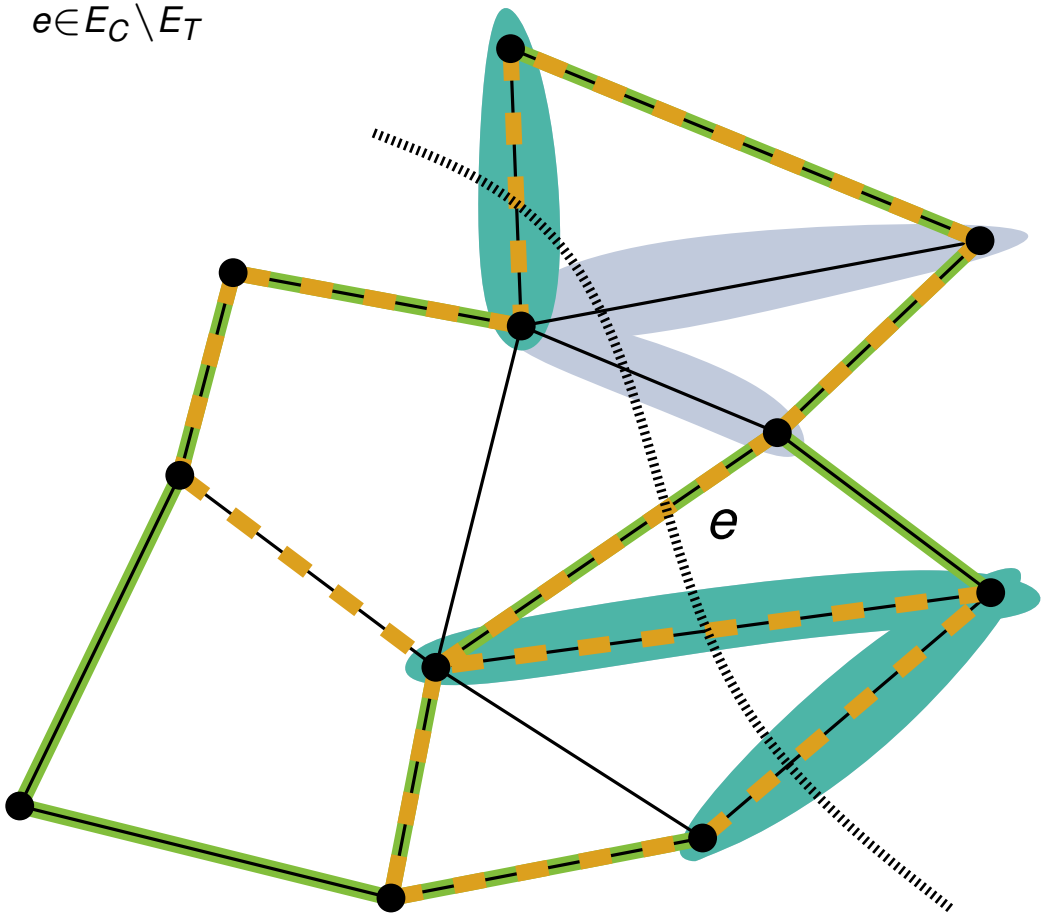
Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

2. Fall: $e \in E_C \cap E_T$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist **gerade**:

  Gilt für jeden Schnitt und Kreis.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.

$\Rightarrow$ E_C hat **ungerade** Anzahl an Nichtbaumkanten E', die Schnitt kreuzen.



2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

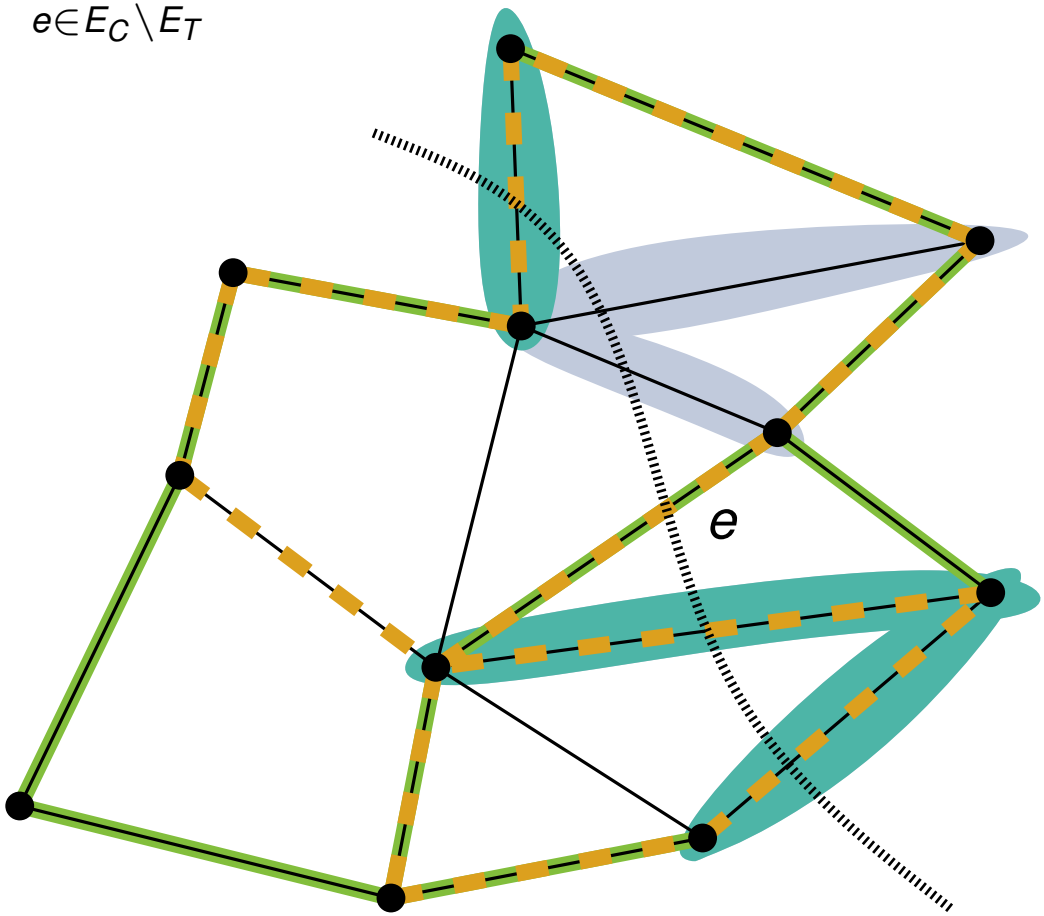
2. Fall: $e \in E_C \cap E_T$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist **gerade**:

  Gilt für jeden Schnitt und Kreis.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.

$\Rightarrow$ E_C hat **ungerade** Anzahl an Nichtbaumkanten E', die Schnitt kreuzen.

$\Rightarrow$ E' bilden gerade die Kreise in B_T, die e enthalten.



2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

2. Fall: $e \in E_C \cap E_T$

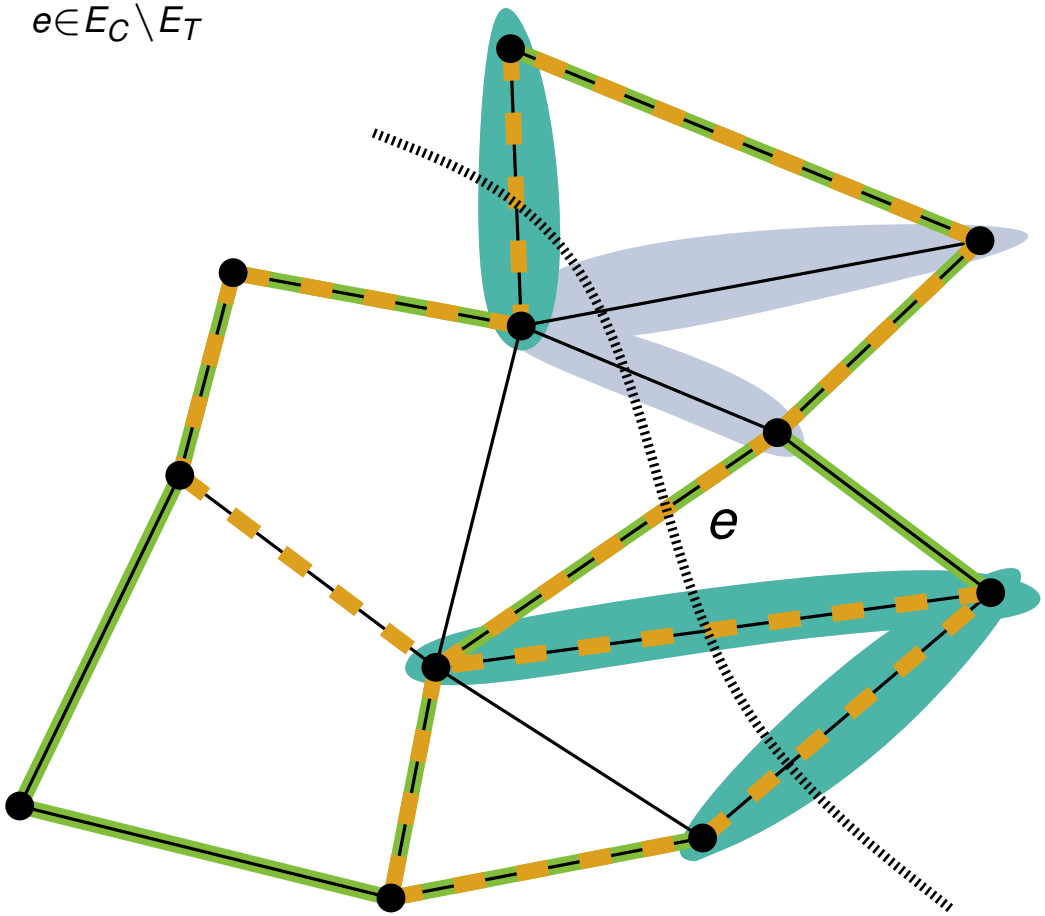
- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist **gerade**:

  Gilt für jeden Schnitt und Kreis.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.

$\Rightarrow$ E_C hat **ungerade** Anzahl an Nichtbaumkanten E', die Schnitt kreuzen.

$\Rightarrow$ E' bilden gerade die Kreise in B_T, die e enthalten.

$\Rightarrow$ e wird nicht zu 0 summiert.



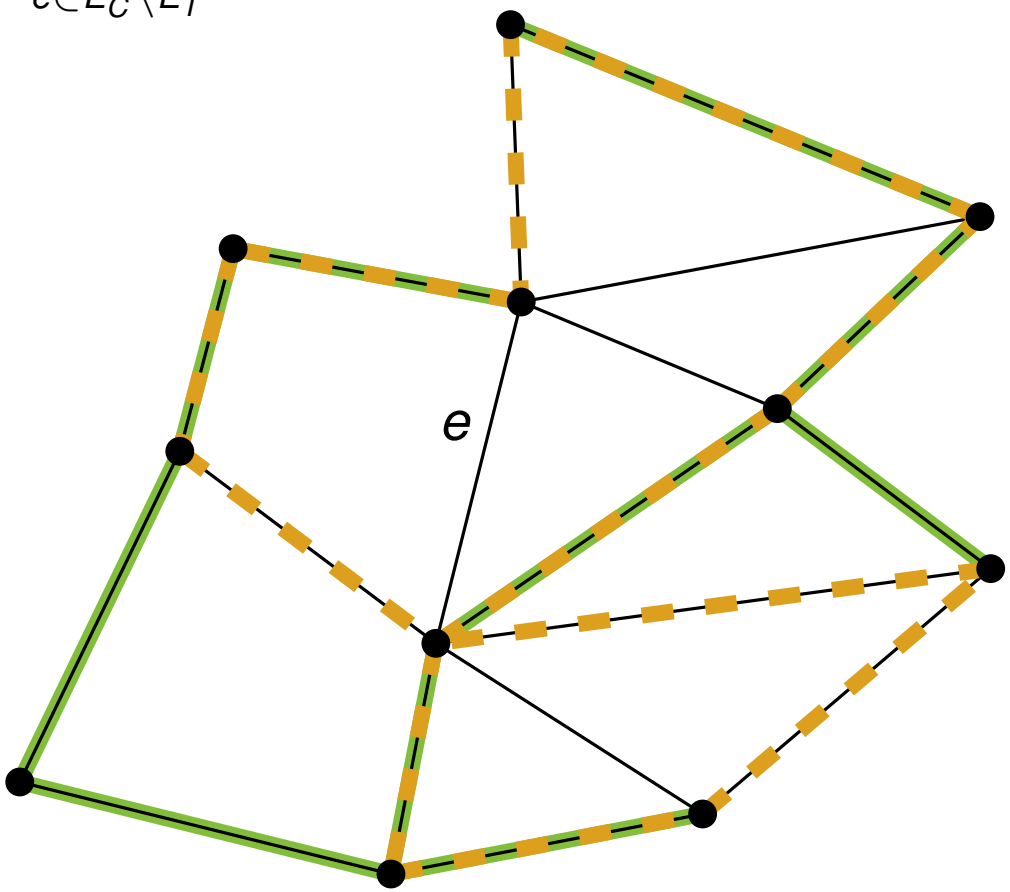
2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

3. Fall: $e \in E \setminus (E_C \cup E_T)$

- Da e Nichtbaumkante, gibt es genau einen Kreis C_e in B_T.
- Da $e \notin E_C$ kommt C_e nicht in Summe vor.

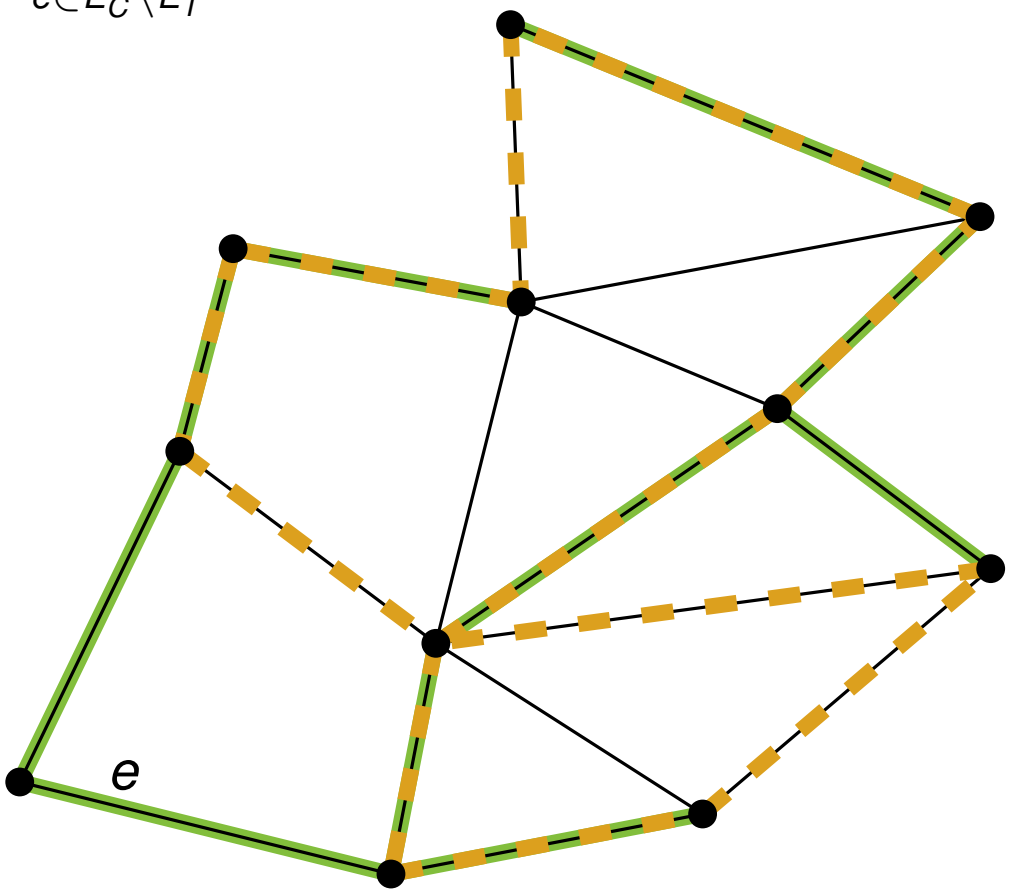


2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

4. Fall: $e \in E_T \setminus E_C$



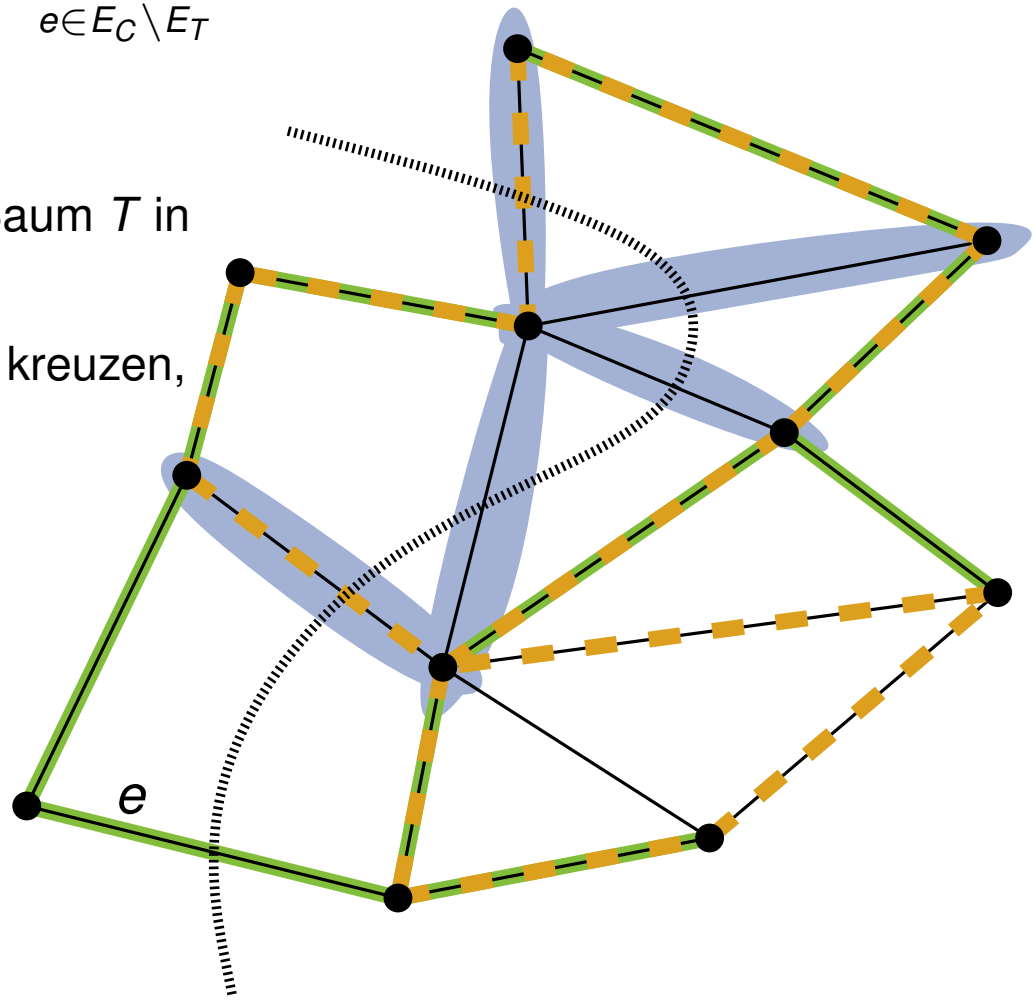
2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

4. Fall: $e \in E_T \setminus E_C$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.



Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

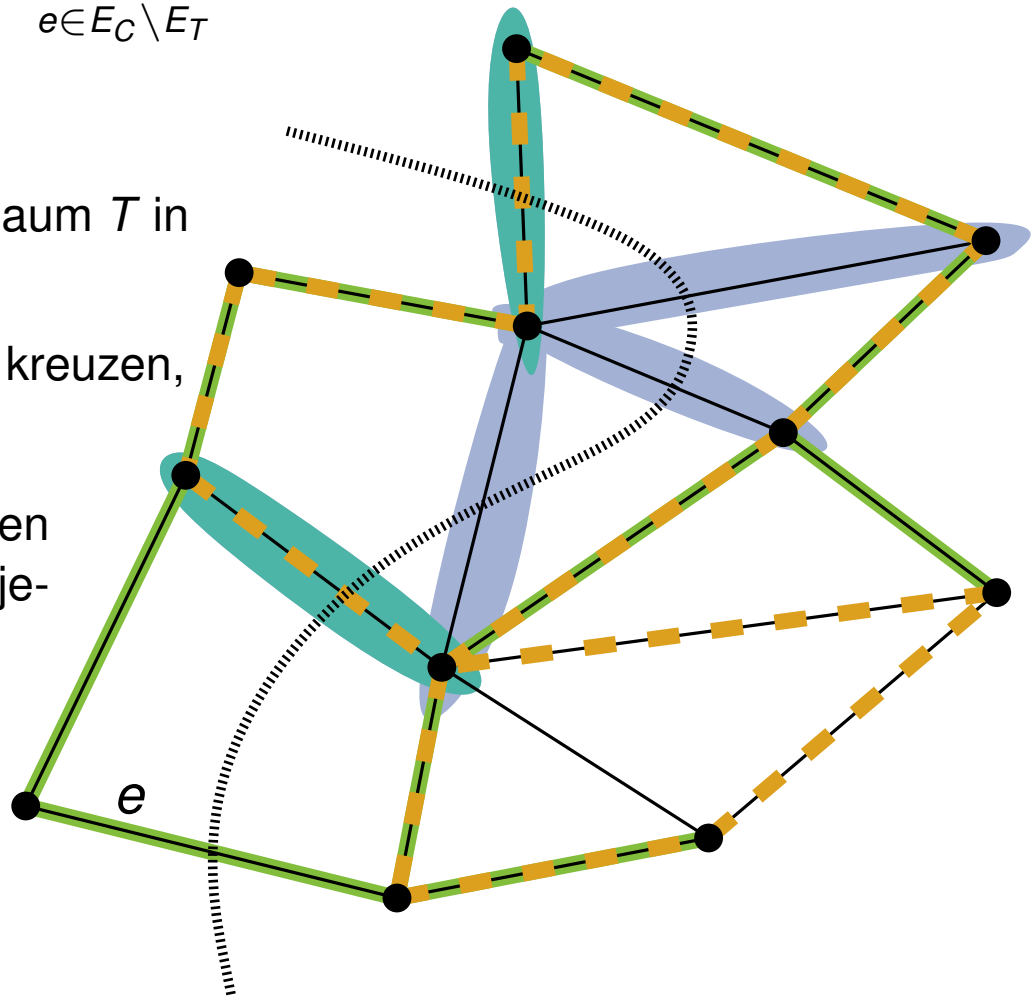
2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

4. Fall: $e \in E_T \setminus E_C$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist gerade: Gilt für jeden Kreis und Schnitt.



2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

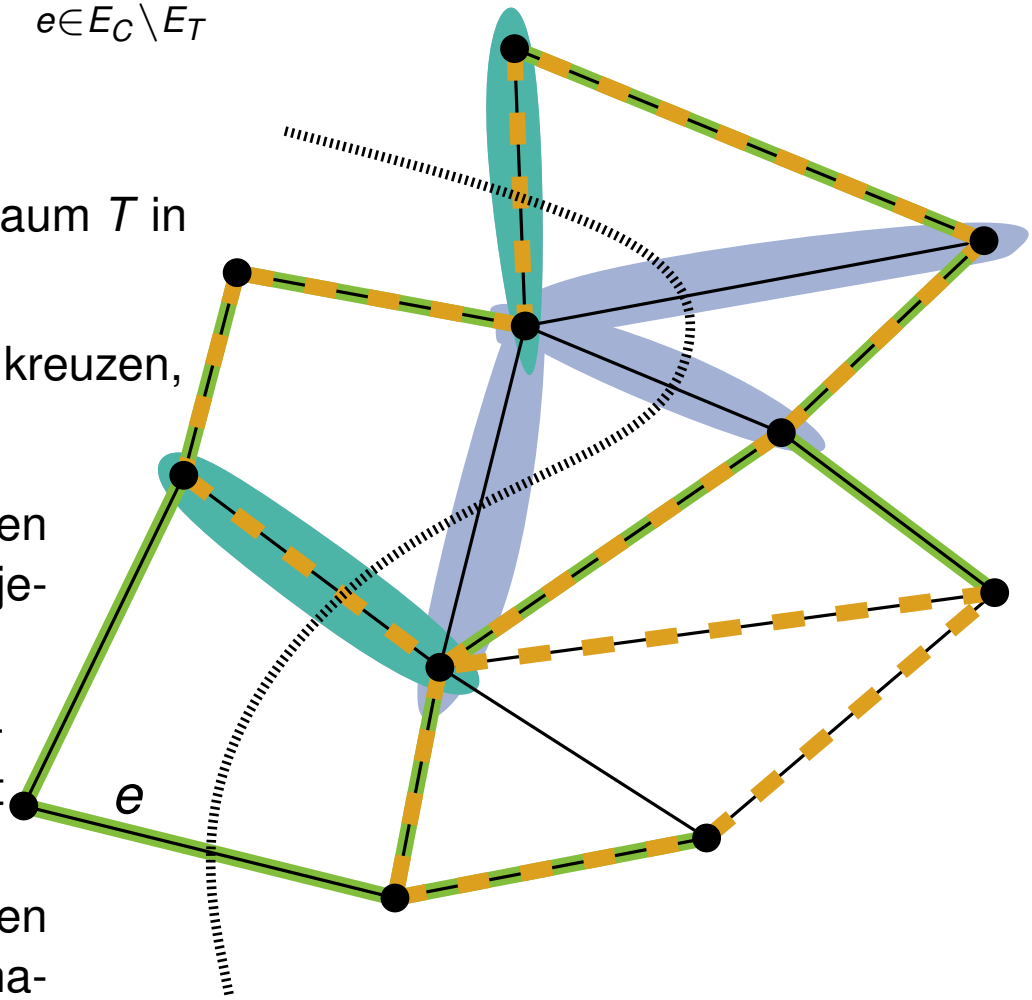
Behauptung: Für jeden Kreis C in G gilt: $C = \sum_{e \in E_C \setminus E_T} C_e$

4. Fall: $e \in E_T \setminus E_C$

- e induziert einen Schnitt, da e den Baum T in zwei Teile zertrennt.
- Alle Kanten außer e, die den Schnitt kreuzen, sind Nichtbaumkanten.
- Die Anzahl der Kanten aus E_C, die den Schnitt kreuzen, ist gerade: Gilt für jeden Kreis und Schnitt.

$\Rightarrow$ Wegen $e \notin E_C$ ist Anzahl der Nichtbaumkanten E' in E_C die Schnitt kreuzen **gerade**.

$\Rightarrow$ Die Nichtbaumkanten E' entsprechen gerade der Kreise in Linearkombination, die e enthalten.



Folglich: e wird zu 0 aufsummiert.

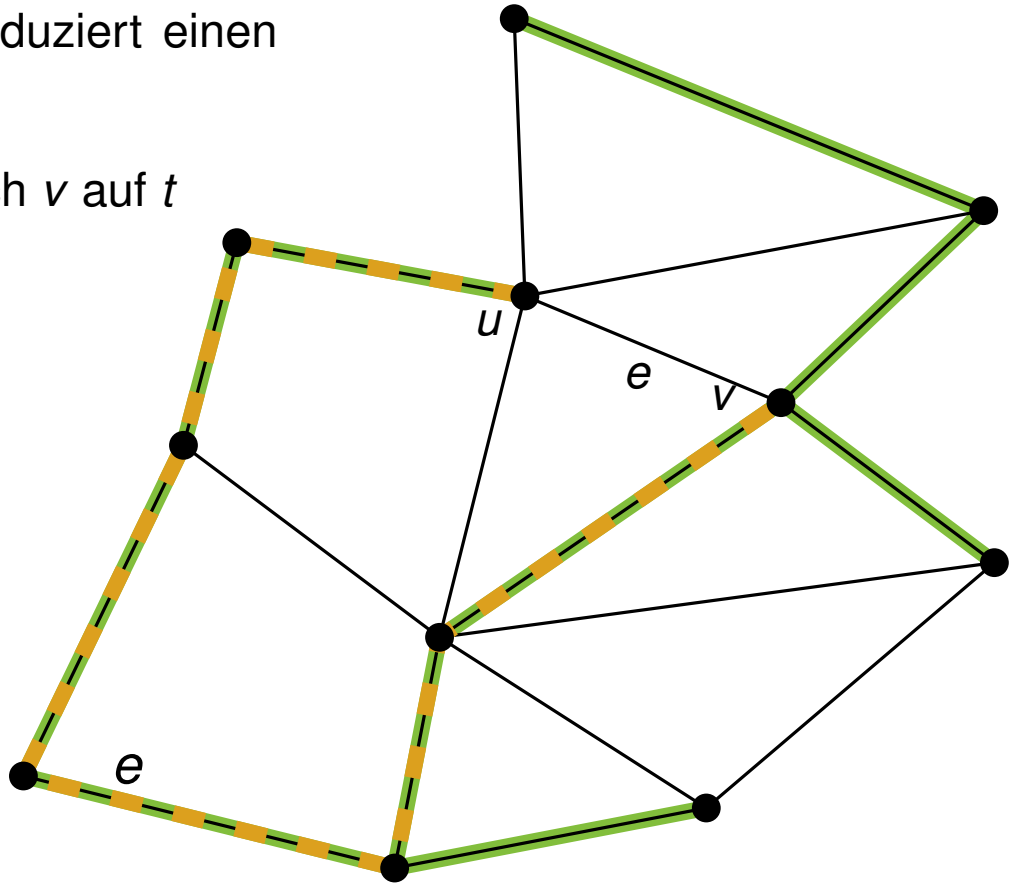
2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

3. Zeigen Sie, dass $|B_T| = m - n + 1$ gilt.

Beob.: Jede Nichtbaumkante $e = \{u, v\}$ induziert einen eindeutigen Kreis C_e:

$\{u, v\}$ + einfacher Weg von u nach v auf t



2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

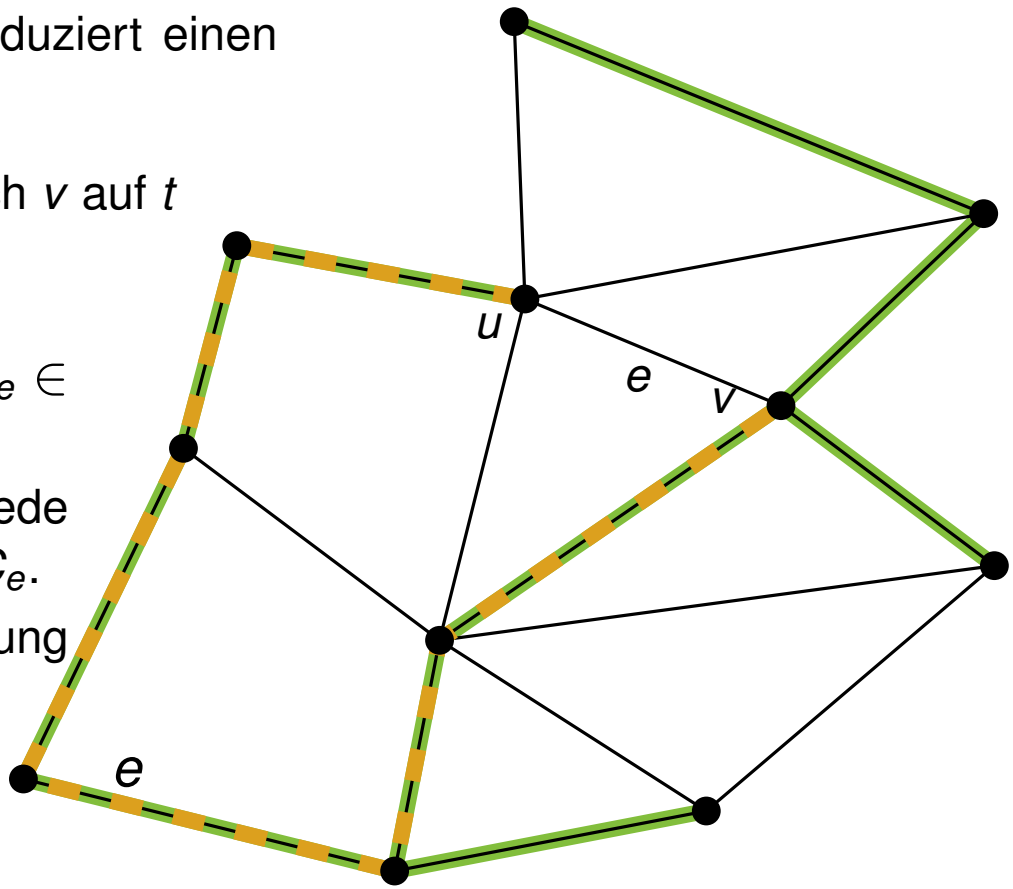
3. Zeigen Sie, dass $|B_T| = m - n + 1$ gilt.

Beob.: Jede Nichtbaumkante $e = \{u, v\}$ induziert einen eindeutigen Kreis C_e:

$\{u, v\}$ + einfacher Weg von u nach v auf t

- Wir zeigen zuerst: $|B_T| = |E \setminus E_T|$
  - Nach Konstruktion enthält jeder Kreis $C_e \in B_T$ genau eine Nichtbaumkante.
  - Wegen obiger Beobachtung induziert jede Nichtbaumkante e genau einen Kreis C_e.

  $\Rightarrow$ wegen bijektiver Mengenentsprechung folgt $|B_T| = |E \setminus E_T|$



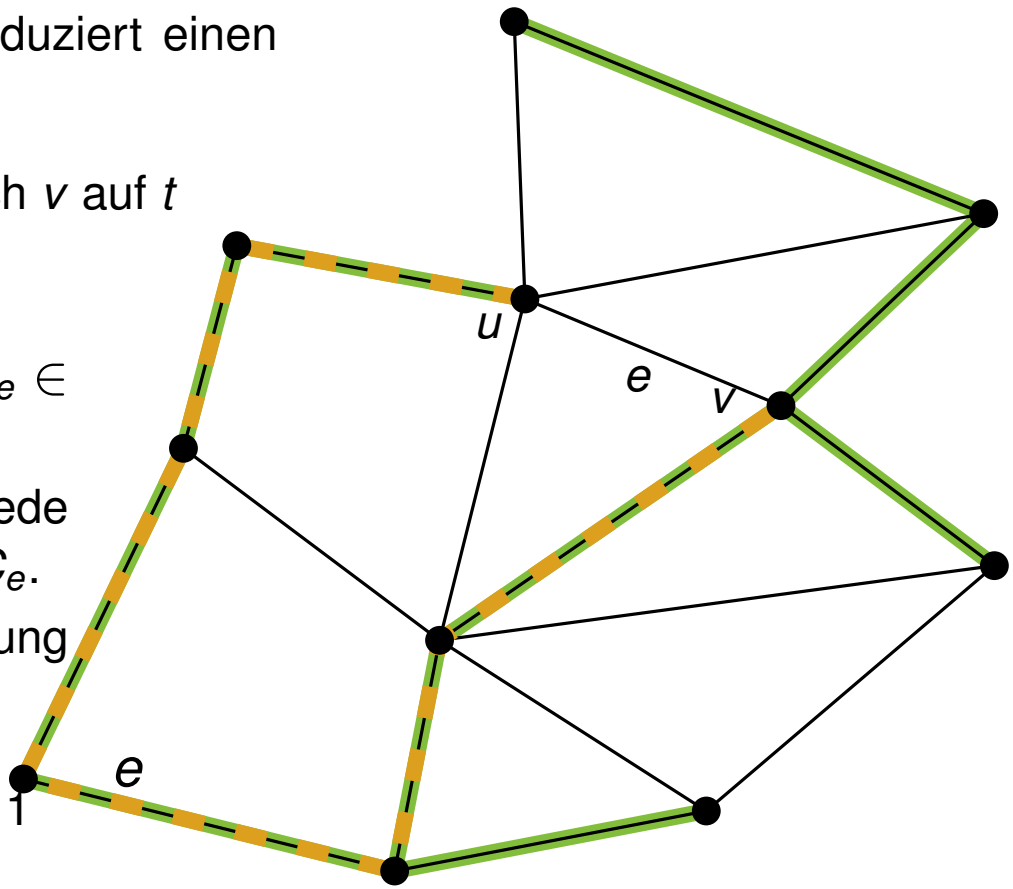
2. Problem

E_C= Kanten im Kreis C.
E_T= Kanten im aufspannenden Baum T.

3. Zeigen Sie, dass $|B_T| = m - n + 1$ gilt.

Beob.: Jede Nichtbaumkante $e = \{u, v\}$ induziert einen eindeutigen Kreis C_e:

$\{u, v\}$ + einfacher Weg von u nach v auf t



- Wir zeigen zuerst: $|B_T| = |E \setminus E_T|$
  - Nach Konstruktion enthält jeder Kreis $C_e \in B_T$ genau eine Nichtbaumkante.
  - Wegen obiger Beobachtung induziert jede Nichtbaumkante e genau einen Kreis C_e.

  $\Rightarrow$ wegen bijektiver Mengenentsprechung folgt $|B_T| = |E \setminus E_T|$

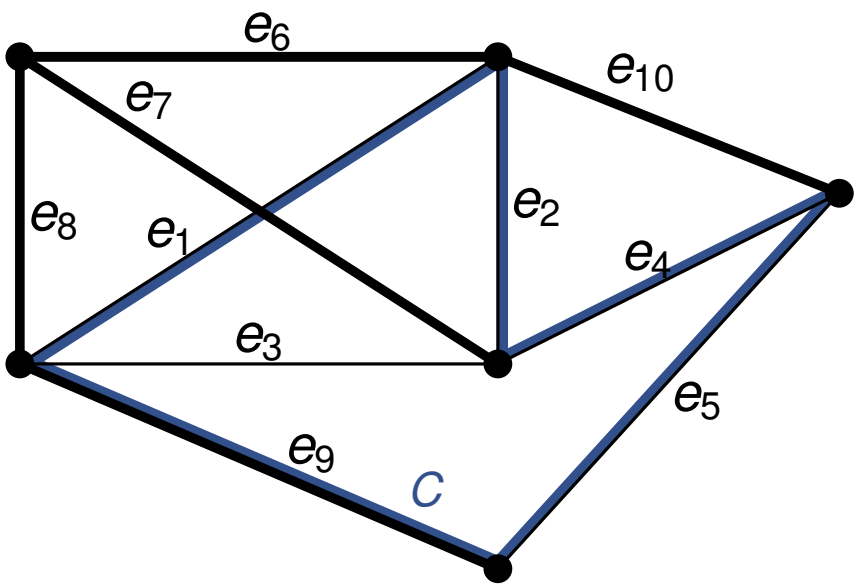
- Aufspannender Baum in Graph hat $n - 1$ Kanten. Damit gilt

$$|B_T| = |E \setminus E_T| = m - n + 1$$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Algorithmus von De Pina

Betrachte Kreise als Inzidenzvektoren über E mit Einschränkung auf die Nichtbaumkanten $\{e_1, \ldots, e_N\}$.



Beispiel: Kreise werden mithilfe der Nichtbaumkanten e_1, e_2, e_3, e_4 und e_5 beschrieben.

$$C = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \begin{matrix} e_1 \\ \\ \vdots \\ \\ e_5 \end{matrix}$$

Kreis C kann mithilfe der Fundamentalkreise C_i (C_i=Fundamentalkreis der Nichtbaumkante e_i) rekonstruiert werden.

$$C = C_1 \oplus C_2 \oplus C_4 \oplus C_5$$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Algorithmus von de Pina

Eingabe: Graph $G = (V, E)$, aufspannenden Baum $T = \{e_1, \ldots, e_N\}$

Ausgabe: MCB von G

for $i = 1$ *bis* N **do**
  $S_i \leftarrow \{e_i\}$

for $k = 1$ *bis* N **do**
  Finde einen kürzesten Kreis C_k mit $\langle C_k, S_k \rangle = 1$
  for $i = k + 1$ *bis* N **do**
    if $\langle C_k, S_i \rangle = 1$ **then**
      $S_i \leftarrow S_i \oplus S_k$

Ausgabe ist: $\{C_1, \ldots, C_N\}$

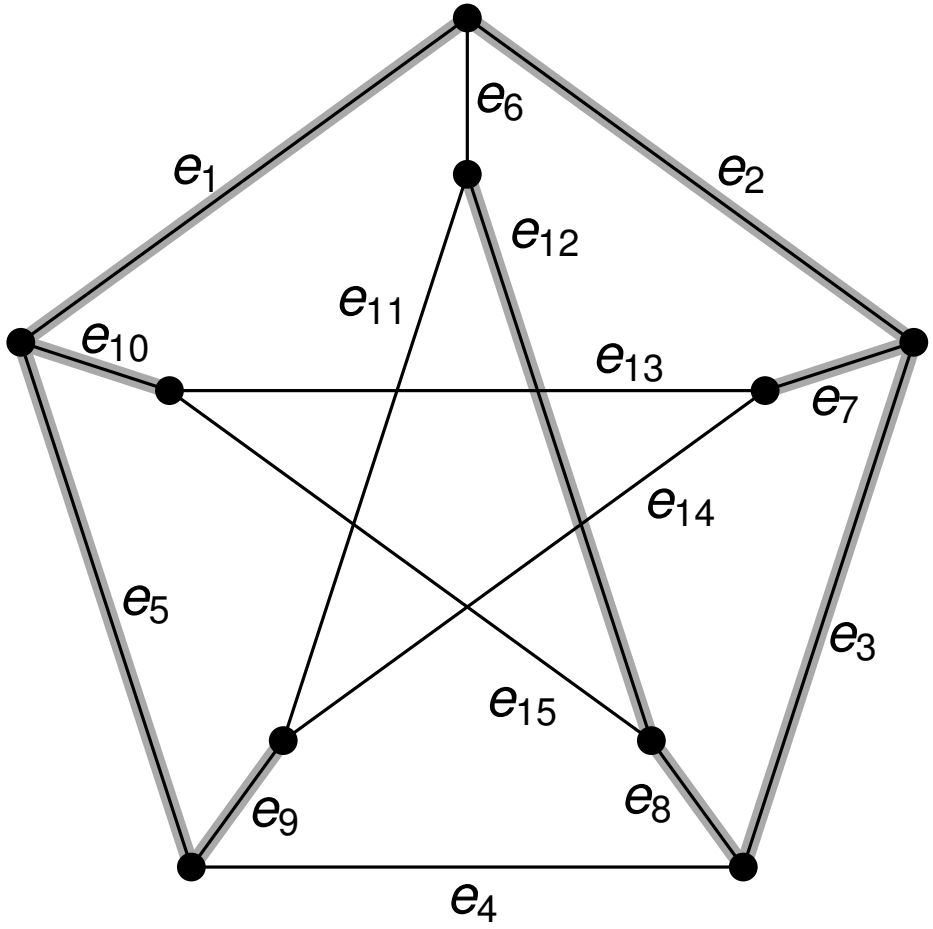
Definiere Bilinearform zweier Vektoren C und S: $\langle C, S \rangle := \sum_{i=1}^{N} (c_i \cdot s_i)$

Produkt und Summe sind über GF(2) definiert.

C und S sind *orthogonal* zueinander genau dann, wenn $\langle C, S \rangle = 0$.

$\langle C, S \rangle = 1$ genau dann, wenn C eine ungerade Anzahl Einträge (Kreise) mit S gemeinsam hat.

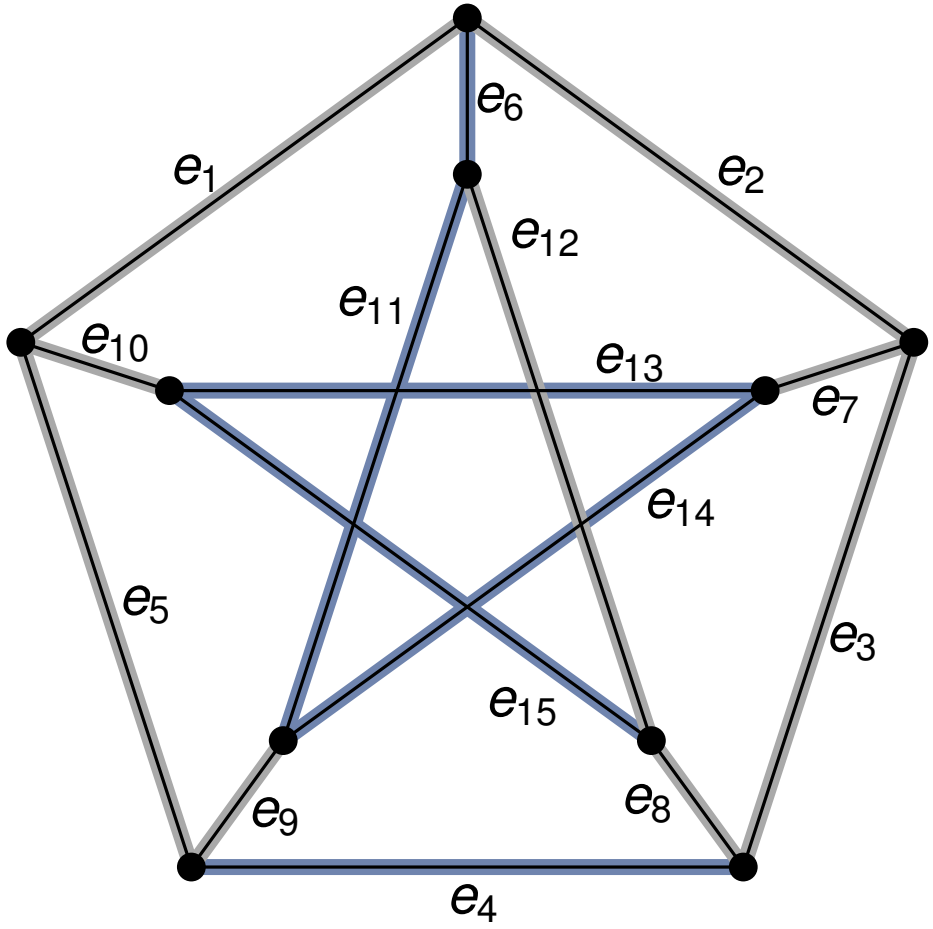
Problem 1



Peterson-Graph

Gewicht pro Kante: 3

Problem 1



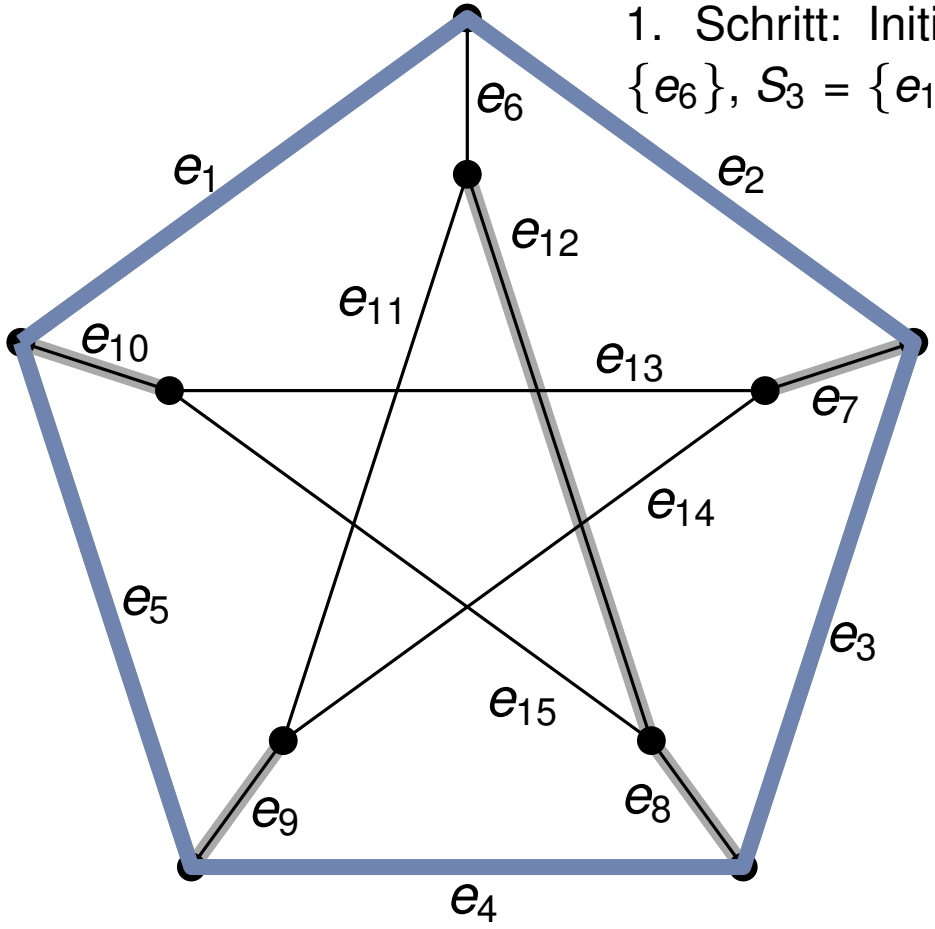
Peterson-Graph

1. Schritt: Initialisierung mit Nichtbaumkanten

$S_1 = \{e_4\}$
$S_2 = \{e_6\}$
$S_3 = \{e_{11}\}$
$S_4 = \{e_{13}\}$
$S_5 = \{e_{14}\}$
$S_6 = \{e_{15}\}$

Gewicht pro Kante: 3

Problem 1



Peterson-Graph

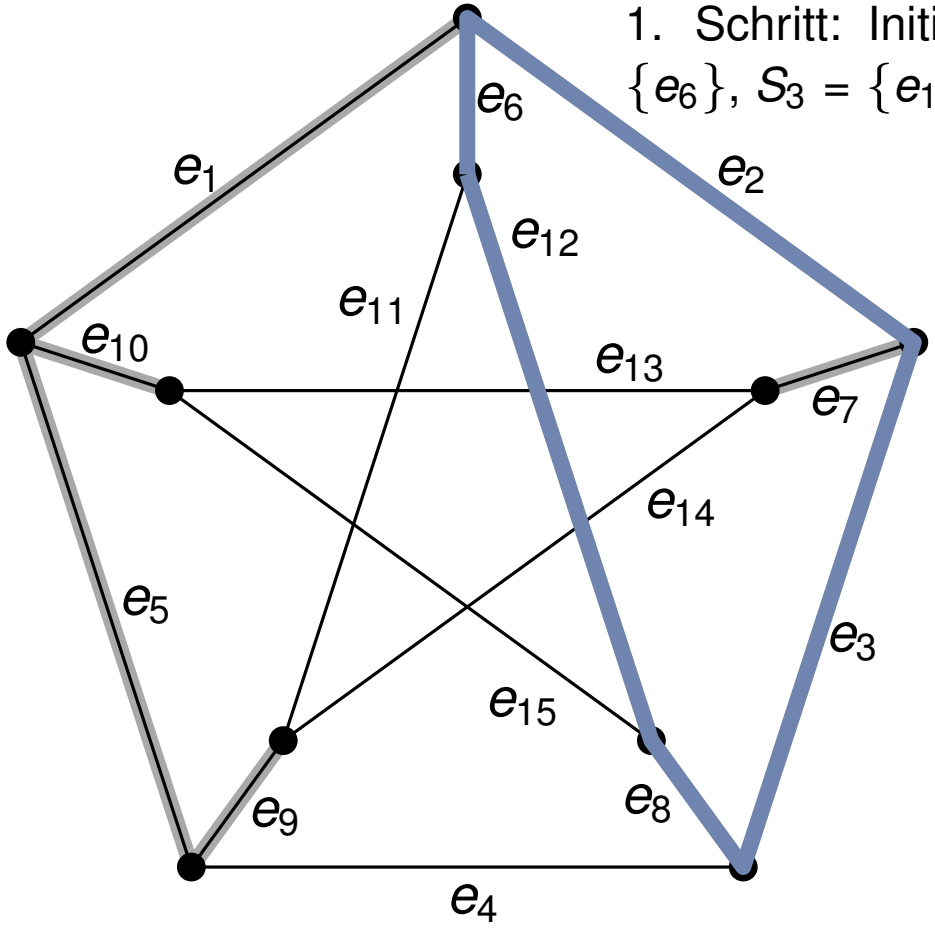
1. Schritt: Initialisierung mit Nichtbaumkanten $S_1 = \{e_4\}$, $S_2 = \{e_6\}$, $S_3 = \{e_{11}\}$, $S_4 = \{e_{13}\}$, $S_5 = \{e_{14}\}$, $S_6 = \{e_{15}\}$

k = 1: Wähle $C_1 = \{e_1, e_2, e_3, e_4, e_5\}$, $w(C_1)=15$
Für i=2...6 gibt es kein S_i mit $\langle C_1, S_i \rangle = 1$

Gewicht pro Kante: 3

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1



Peterson-Graph

1. Schritt: Initialisierung mit Nichtbaumkanten $S_1 = \{e_4\}$, $S_2 = \{e_6\}$, $S_3 = \{e_{11}\}$, $S_4 = \{e_{13}\}$, $S_5 = \{e_{14}\}$, $S_6 = \{e_{15}\}$

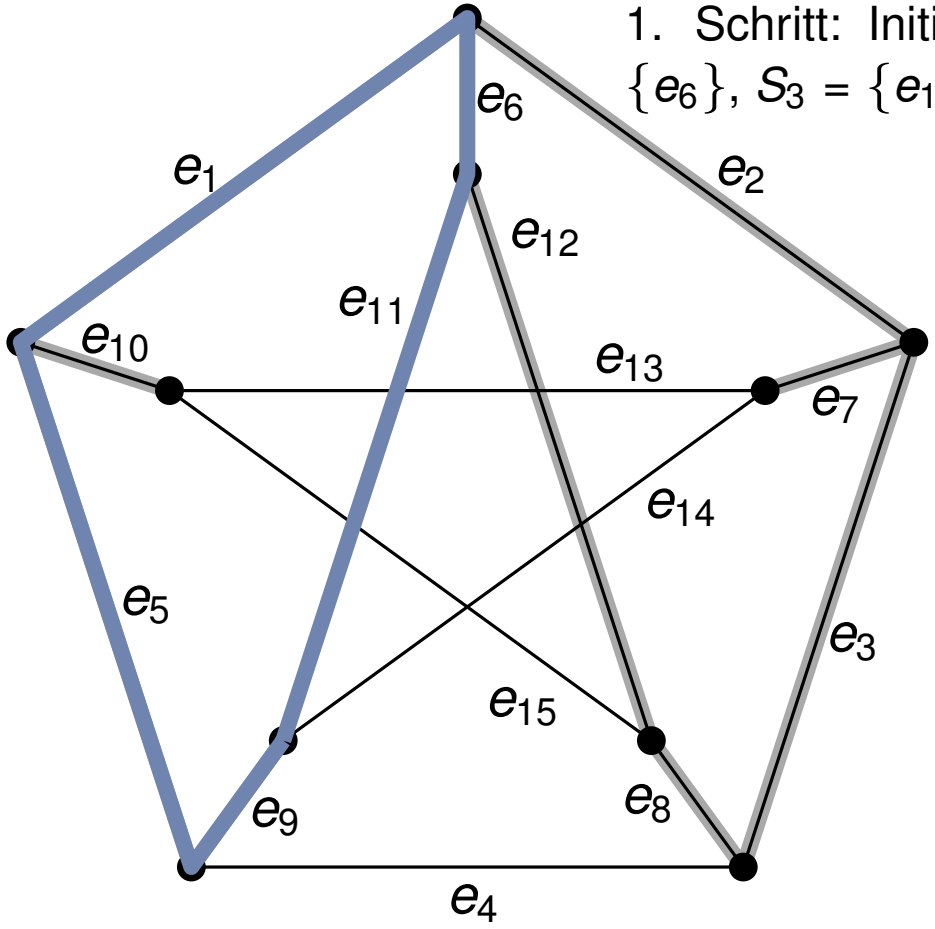
k = 1: Wähle $C_1 = \{e_1, e_2, e_3, e_4, e_5\}$, $w(C_1)$=15
Für i=2...6 gibt es kein S_i mit $\langle C_1, S_i \rangle = 1$

k = 2: Wähle $C_2 = \{e_6, e_2, e_3, e_8, e_{12}\}$, $w(C_2)$=15
Für i=3...6 gibt es kein S_i mit $\langle C_2, S_i \rangle = 1$

Gewicht pro Kante: 3

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1



Peterson-Graph

1. Schritt: Initialisierung mit Nichtbaumkanten $S_1 = \{e_4\}$, $S_2 = \{e_6\}$, $S_3 = \{e_{11}\}$, $S_4 = \{e_{13}\}$, $S_5 = \{e_{14}\}$, $S_6 = \{e_{15}\}$

k = 1: Wähle $C_1 = \{e_1, e_2, e_3, e_4, e_5\}$, $w(C_1)$=15
Für i=2...6 gibt es kein S_i mit $\langle C_1, S_i \rangle = 1$

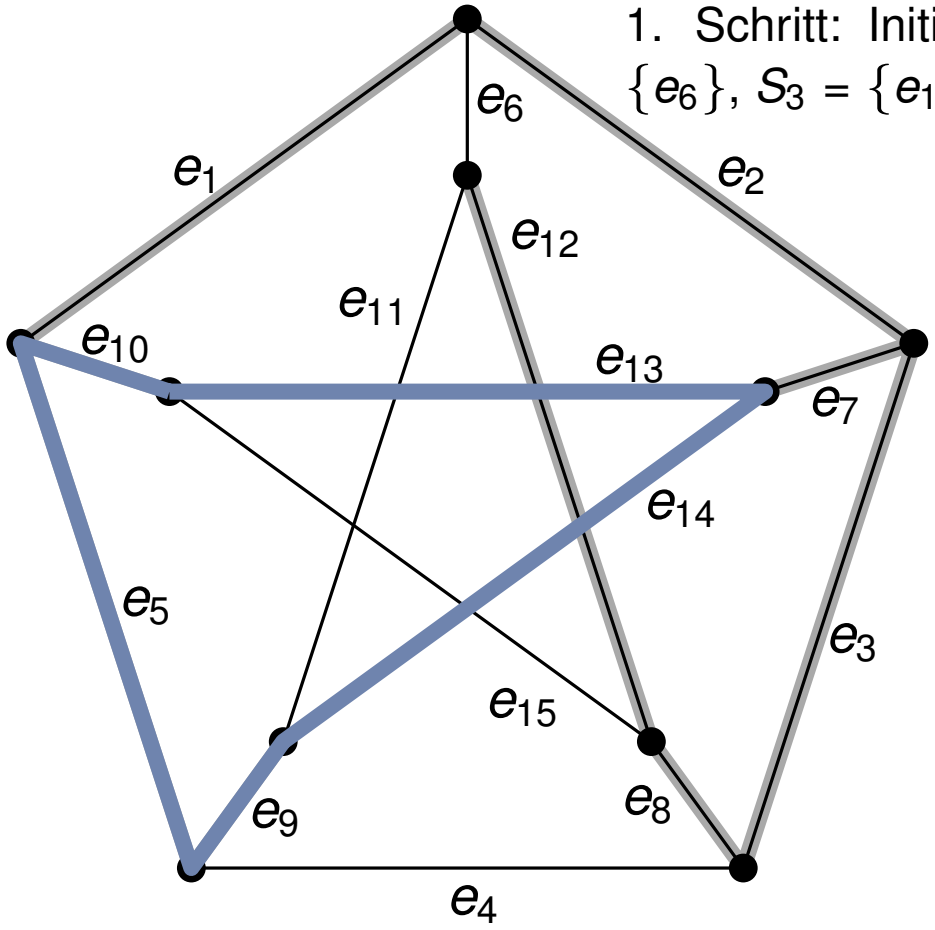
k = 2: Wähle $C_2 = \{e_6, e_2, e_3, e_8, e_{12}\}$, $w(C_2)$=15
Für i=3...6 gibt es kein S_i mit $\langle C_2, S_i \rangle = 1$

k = 3: Wähle $C_3 = \{e_{11}, e_6, e_1, e_5, e_9\}$, $w(C_3)$=15
Für i=4...6 gibt es kein S_i mit $\langle C_3, S_i \rangle = 1$

Gewicht pro Kante: 3

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1



Peterson-Graph

Gewicht pro Kante: 3

1. Schritt: Initialisierung mit Nichtbaumkanten $S_1 = \{e_4\}$, $S_2 = \{e_6\}$, $S_3 = \{e_{11}\}$, $S_4 = \{e_{13}\}$, $S_5 = \{e_{14}\}$, $S_6 = \{e_{15}\}$

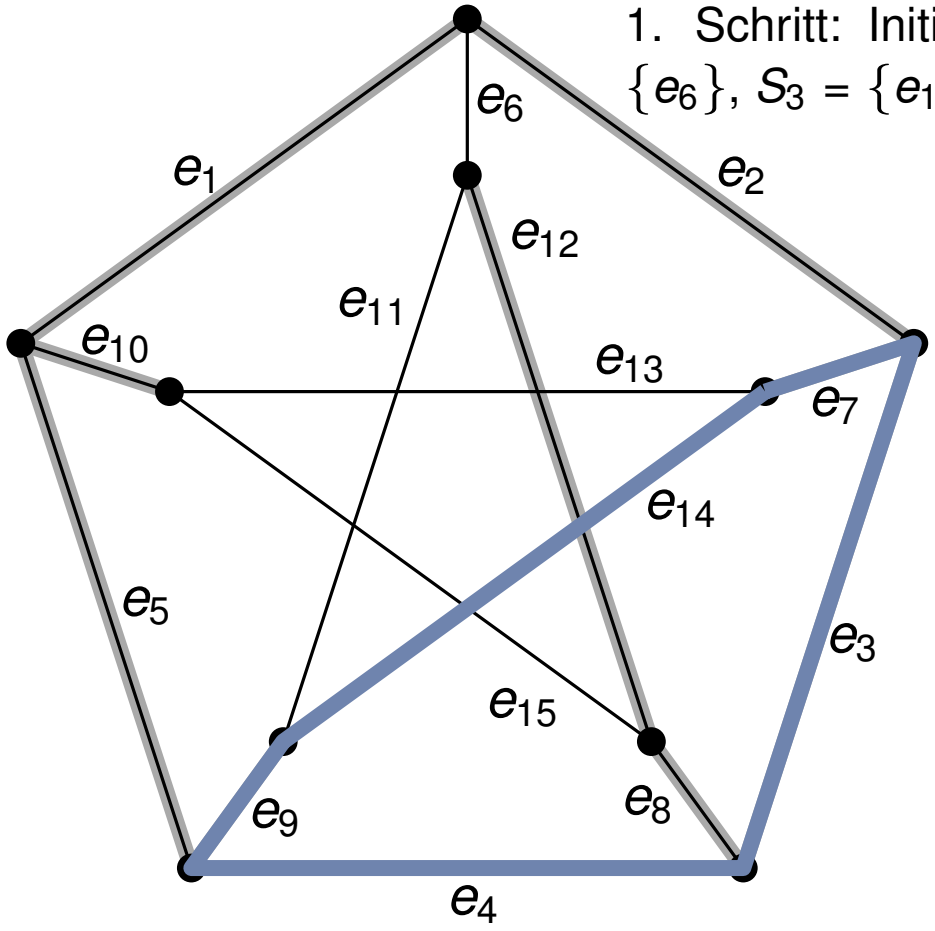
k = 1: Wähle $C_1 = \{e_1, e_2, e_3, e_4, e_5\}$, $w(C_1)$=15
Für i=2...6 gibt es kein S_i mit $\langle C_1, S_i \rangle = 1$

k = 2: Wähle $C_2 = \{e_6, e_2, e_3, e_8, e_{12}\}$, $w(C_2)$=15
Für i=3...6 gibt es kein S_i mit $\langle C_2, S_i \rangle = 1$

k = 3: Wähle $C_3 = \{e_{11}, e_6, e_1, e_5, e_9\}$, $w(C_3)$=15
Für i=4...6 gibt es kein S_i mit $\langle C_3, S_i \rangle = 1$

k = 4: Wähle $C_4 = \{e_{13}, e_{14}, e_9, e_5, e_{10}\}$, $w(C_4)$=15
$\langle C_4, S_5 \rangle = 1$, $S_5 := S_5 \oplus S_4 = \{e_{13}, e_{14}\}$

Problem 1



Peterson-Graph

1. Schritt: Initialisierung mit Nichtbaumkanten $S_1 = \{e_4\}$, $S_2 = \{e_6\}$, $S_3 = \{e_{11}\}$, $S_4 = \{e_{13}\}$, $S_5 = \{e_{14}\}$, $S_6 = \{e_{15}\}$

k = 1: Wähle $C_1 = \{e_1, e_2, e_3, e_4, e_5\}$, $w(C_1)$=15
Für i=2...6 gibt es kein S_i mit $\langle C_1, S_i \rangle = 1$

k = 2: Wähle $C_2 = \{e_6, e_2, e_3, e_8, e_{12}\}$, $w(C_2)$=15
Für i=3...6 gibt es kein S_i mit $\langle C_2, S_i \rangle = 1$

k = 3: Wähle $C_3 = \{e_{11}, e_6, e_1, e_5, e_9\}$, $w(C_3)$=15
Für i=4...6 gibt es kein S_i mit $\langle C_3, S_i \rangle = 1$

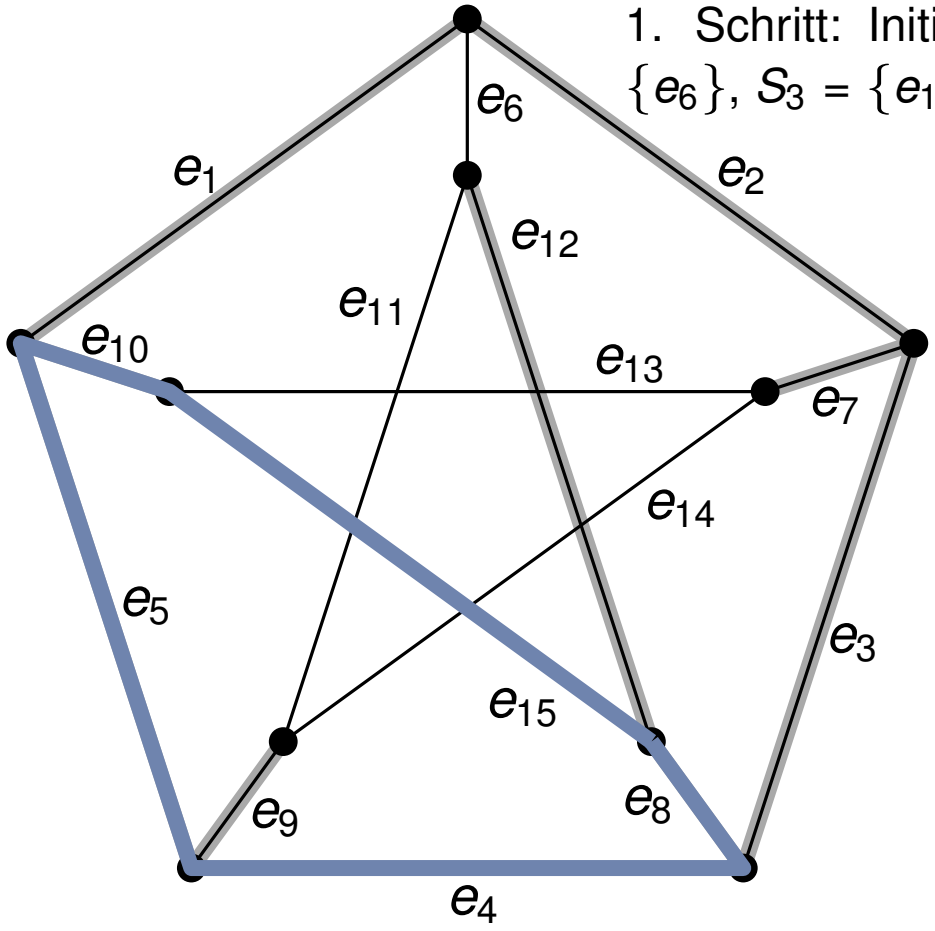
k = 4: Wähle $C_4 = \{e_{13}, e_{14}, e_9, e_5, e_{10}\}$, $w(C_4)$=15
$\langle C_4, S_5 \rangle = 1$, $S_5 := S_5 \oplus S_4 = \{e_{13}, e_{14}\}$

k = 5: Wähle $C_5 = \{e_{14}, e_9, e_4, e_3, e_7\}$, $w(C_5)$=15
$\langle C_5, S_6 \rangle = 0$

Gewicht pro Kante: 3

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1



Peterson-Graph

Gewicht pro Kante: 3

1. Schritt: Initialisierung mit Nichtbaumkanten $S_1 = \{e_4\}$, $S_2 = \{e_6\}$, $S_3 = \{e_{11}\}$, $S_4 = \{e_{13}\}$, $S_5 = \{e_{14}\}$, $S_6 = \{e_{15}\}$

k = 1: Wähle $C_1 = \{e_1, e_2, e_3, e_4, e_5\}$, $w(C_1)$=15
Für i=2...6 gibt es kein S_i mit $\langle C_1, S_i \rangle = 1$

k = 2: Wähle $C_2 = \{e_6, e_2, e_3, e_8, e_{12}\}$, $w(C_2)$=15
Für i=3...6 gibt es kein S_i mit $\langle C_2, S_i \rangle = 1$

k = 3: Wähle $C_3 = \{e_{11}, e_6, e_1, e_5, e_9\}$, $w(C_3)$=15
Für i=4...6 gibt es kein S_i mit $\langle C_3, S_i \rangle = 1$

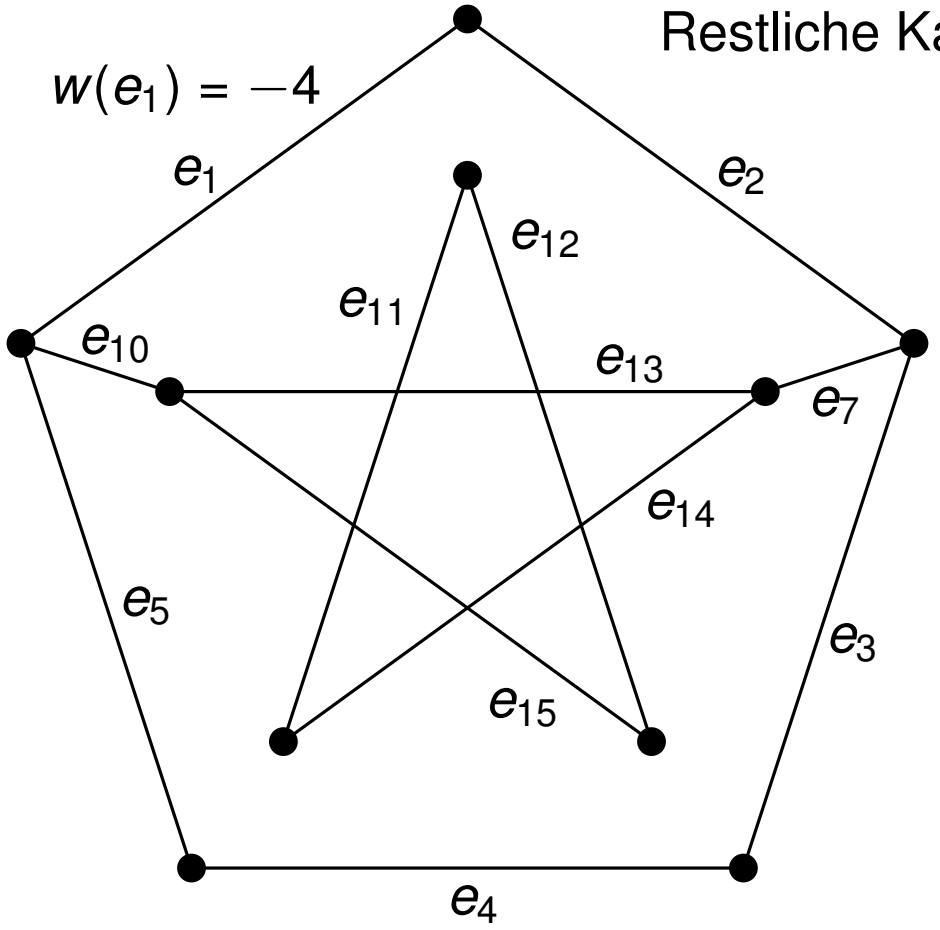
k = 4: Wähle $C_4 = \{e_{13}, e_{14}, e_9, e_5, e_{10}\}$, $w(C_4)$=15
$\langle C_4, S_5 \rangle = 1$, $S_5 := S_5 \oplus S_4 = \{e_{13}, e_{14}\}$

k = 5: Wähle $C_5 = \{e_{14}, e_9, e_4, e_3, e_7\}$, $w(C_5)$=15
$\langle C_5, S_6 \rangle = 0$

k = 6: Wähle $C_6 = \{e_{15}, e_{10}, e_5, e_4, e_8\}$, $w(C_5)$=15

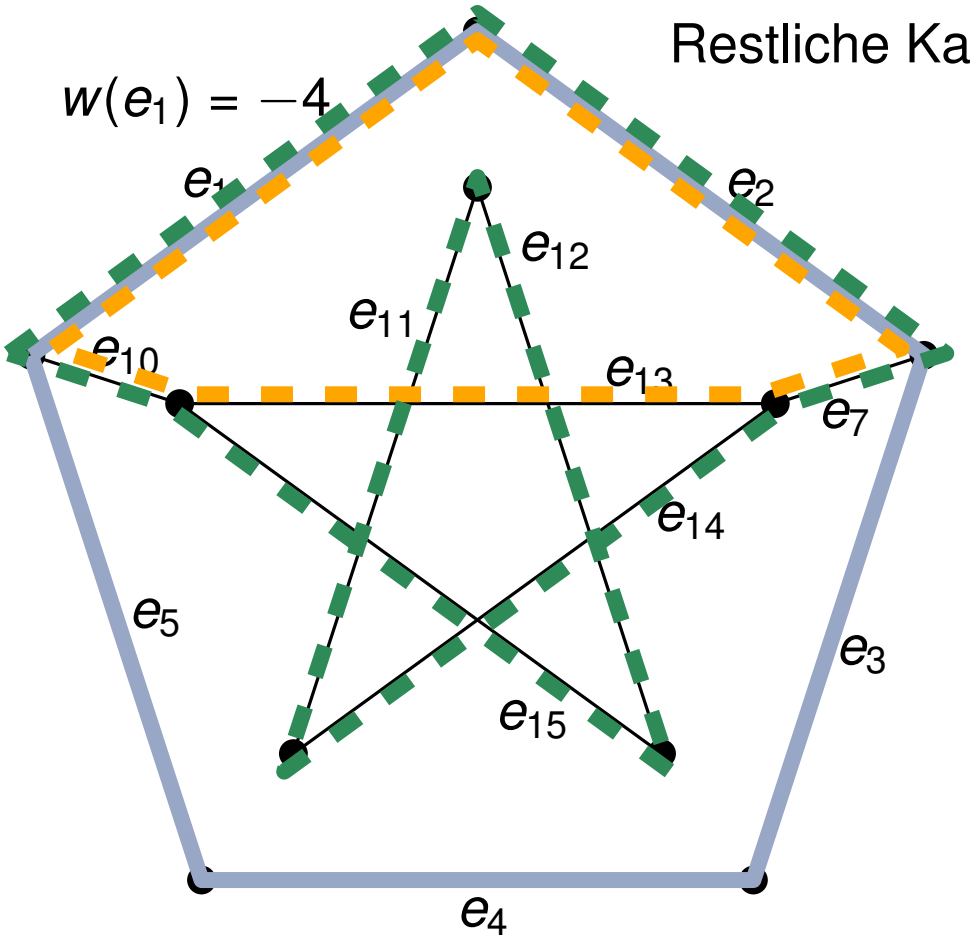
Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1



Restliche Kanten haben Gewicht 1.

Problem 1



Restliche Kanten haben Gewicht 1.

$MCB = \{C_1, C_2, C_3\}$ mit

$C_1 = \{e_1, e_2, e_3, e_4, e_5\}$

$C_2 = \{e_1, e_2, e_7, e_{13}, e_{10}\}$

$C_3 = \{e_1, e_2, e_7, e_{14}, e_{11}, e_{12}, e_{15}, e_{10}\}$

$w(MCB) = 3$

Karlsruher Institut für Technologie

Randomisierte Algorithmen

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

4. Problem

Gegeben: Zufallsgenerator $\mathcal{A}_1$:

- Liefert Wert 1 mit Wahrscheinlichkeit p.
- Liefert Wert 0 mit Wahrscheinlichkeit $1 - p$.

Gesucht: Zufallsgenerator $\mathcal{A}_2$:

- Liefert Wert 1 mit Wahrscheinlichkeit $\frac{1}{2}$.
- Liefert Wert 0 mit Wahrscheinlichkeit $\frac{1}{2}$.

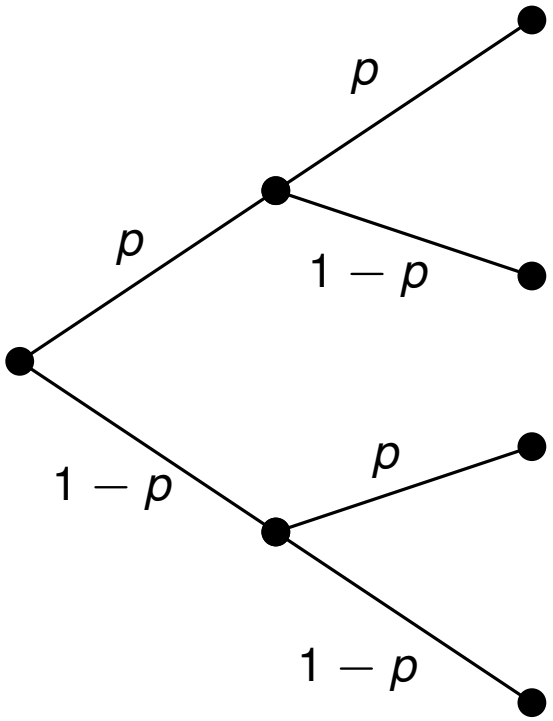
4. Problem

Gegeben: Zufallsgenerator $\mathcal{A}_1$:

- Liefert Wert 1 mit Wahrscheinlichkeit p.
- Liefert Wert 0 mit Wahrscheinlichkeit $1 - p$.

Gesucht: Zufallsgenerator $\mathcal{A}_2$:

- Liefert Wert 1 mit Wahrscheinlichkeit $\frac{1}{2}$.
- Liefert Wert 0 mit Wahrscheinlichkeit $\frac{1}{2}$.



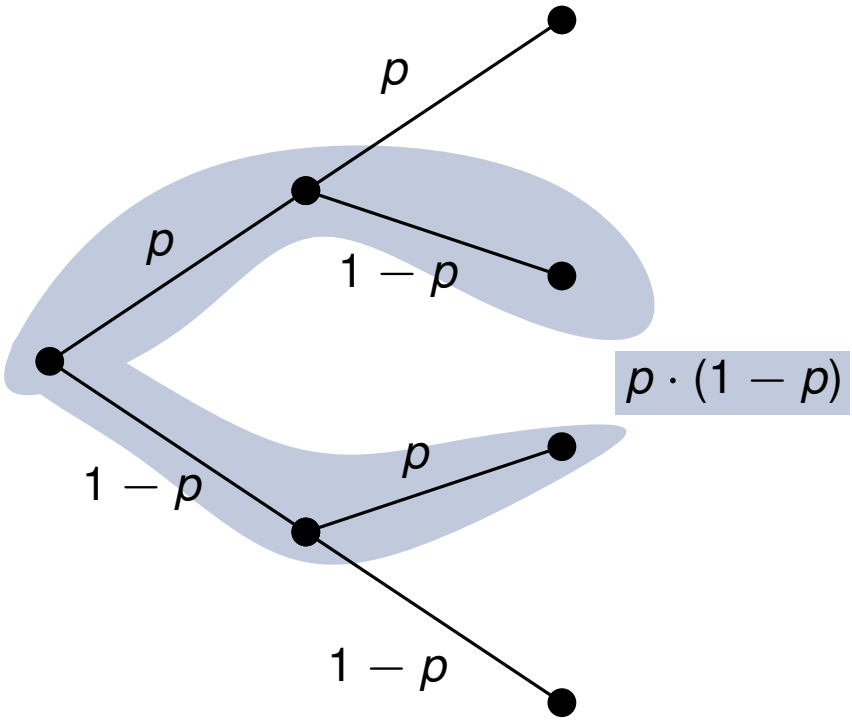
4. Problem

Gegeben: Zufallsgenerator $\mathcal{A}_1$:

- Liefert Wert 1 mit Wahrscheinlichkeit p.
- Liefert Wert 0 mit Wahrscheinlichkeit $1 - p$.

Gesucht: Zufallsgenerator $\mathcal{A}_2$:

- Liefert Wert 1 mit Wahrscheinlichkeit $\frac{1}{2}$.
- Liefert Wert 0 mit Wahrscheinlichkeit $\frac{1}{2}$.



Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

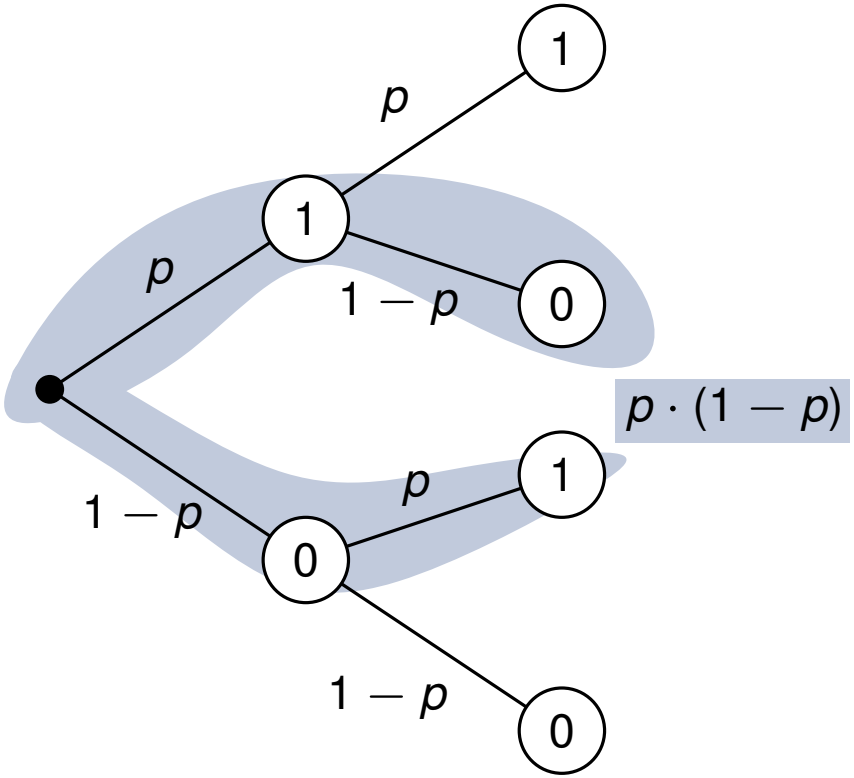
4. Problem

Gegeben: Zufallsgenerator $\mathcal{A}_1$:

- Liefert Wert 1 mit Wahrscheinlichkeit p.
- Liefert Wert 0 mit Wahrscheinlichkeit $1 - p$.

Gesucht: Zufallsgenerator $\mathcal{A}_2$:

- Liefert Wert 1 mit Wahrscheinlichkeit $\frac{1}{2}$.
- Liefert Wert 0 mit Wahrscheinlichkeit $\frac{1}{2}$.

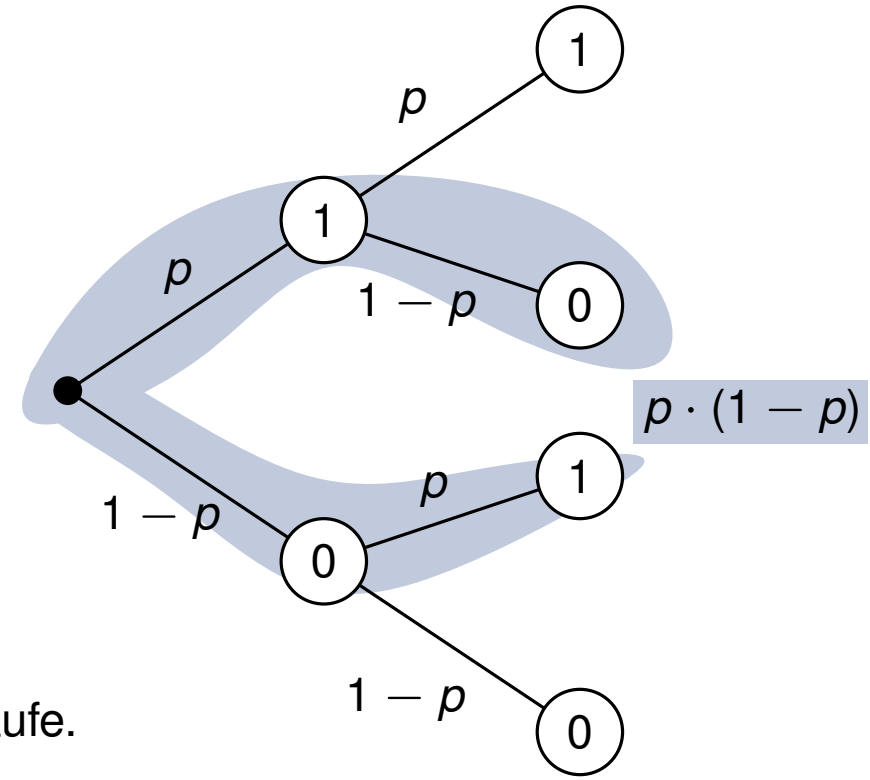



```
x ← 0
y ← 0
while x = y do
    x ← A1()
    y ← A1()
return x
```


Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

4. Problem

```
x ← 0
y ← 0
while x = y do
    x ← A_1()
    y ← A_1()
return x
```



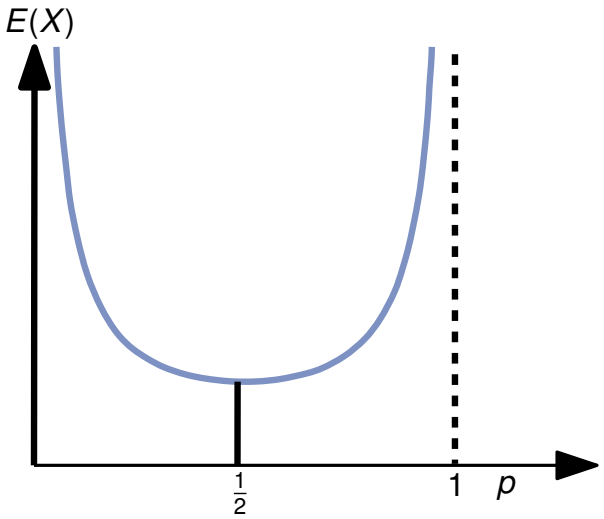
- Erwartete Laufzeit bestimmt durch Anzahl Durchläufe.
- Durchlauf = Bernoulli-Experiment mit $Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$.
- Schleife = unabhängige Bernoulli-Experimente mit geometrischer Verteilung:

$$E(X) = \frac{1}{Pr[x \neq y]} = \frac{1}{2 \cdot p \cdot (1 - p)}$$

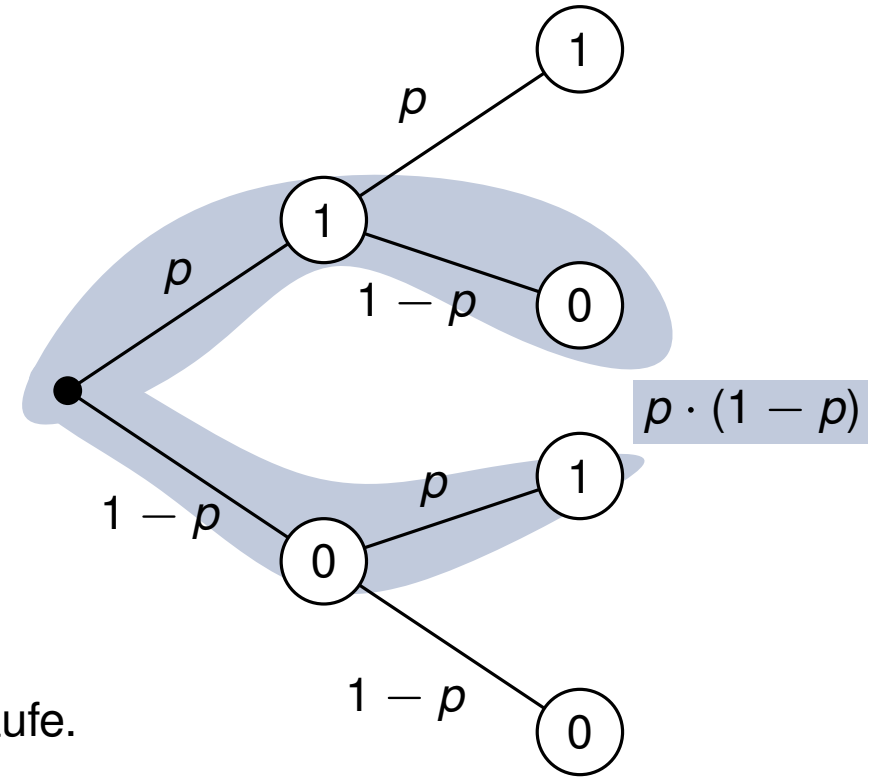
$\Rightarrow$ Erwartete Laufzeit $\Theta(\frac{1}{p \cdot (1-p)})$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

4. Problem




```
x ← 0
y ← 0
while x = y do
    x ← A_1()
    y ← A_1()
return x
```



- Erwartete Laufzeit bestimmt durch Anzahl Durchläufe.
- Durchlauf = Bernoulli-Experiment mit $Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$.
- Schleife = unabhängige Bernoulli-Experimente mit geometrischer Verteilung:

$$E(X) = \frac{1}{Pr[x \neq y]} = \frac{1}{2 \cdot p \cdot (1 - p)}$$

$\Rightarrow$ Erwartete Laufzeit $\Theta(\frac{1}{p \cdot (1-p)})$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

5. Problem

Eingabe: Matrix A, B und C

$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$

$x \leftarrow Br$

$y \leftarrow Ax$

$z \leftarrow Cr$

wenn $y \neq z$ **dann**
  return NEIN

sonst
  return JA

Algorithmus testet ob $AB = C$

1. Zeigen Sie, dass die Rückgabe JA ist, wenn gilt $AB = C$.

5. Problem

Eingabe: Matrix A, B und C

$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$

$x \leftarrow Br$

$y \leftarrow Ax$

$z \leftarrow Cr$

wenn $y \neq z$ **dann**
  return NEIN

sonst
  return JA

Algorithmus testet ob $AB = C$

1. Zeigen Sie, dass die Rückgabe JA ist, wenn gilt $AB = C$.

- Algorithmus überprüft ob $A(Br) = Cr$ gilt.
- Wenn $AB = C$ gilt, dann insbesondere auch $A(Br) = Cr$.

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

Eingabe: Matrix A, B und C

$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$

$x \leftarrow Br$

$y \leftarrow Ax$

$z \leftarrow Cr$

wenn $y \neq z$ **dann**
  return NEIN

sonst
  return JA

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.

Eingabe: Matrix A, B und C

$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$

$x \leftarrow Br$

$y \leftarrow Ax$

$z \leftarrow Cr$

wenn $y \neq z$ **dann**
  return NEIN

sonst
  return JA

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.

Eingabe: Matrix A, B und C

$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$

$x \leftarrow Br$

$y \leftarrow Ax$

$z \leftarrow Cr$

wenn $y \neq z$ **dann**
  return NEIN

sonst
  return JA

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.
- Seit d erste Zeile von D, o.B.d.A:
  - sei d nicht der Nullvektor und
  - die Nichtnulleinträge seien die ersten ℓ Einträge.

Eingabe: Matrix A, B und C
$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$
$x \leftarrow Br$
$y \leftarrow Ax$
$z \leftarrow Cr$
wenn $y \neq z$ **dann**
  return NEIN
sonst
  return JA

$$D = \begin{pmatrix} d_1 & \dots & d_\ell & 0 \dots 0 \\ & & \dots & \end{pmatrix}$$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.
- Seit d erste Zeile von D, o.B.d.A:
  - sei d nicht der Nullvektor und
  - die Nichtnulleinträge seien die ersten ℓ Einträge.

Suche obere Schranke dafür, dass $dr = 0$ ist:

Eingabe: Matrix A, B und C

$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$

$x \leftarrow Br$

$y \leftarrow Ax$

$z \leftarrow Cr$

wenn $y \neq z$ **dann**

| return NEIN

sonst

| return JA

$$D = \begin{pmatrix} d_1 & \dots & d_\ell & 0 \dots 0 \\ & & \dots & \end{pmatrix}$$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.
- Seit d erste Zeile von D, o.B.d.A:
  - sei d nicht der Nullvektor und
  - die Nichtnulleinträge seien die ersten ℓ Einträge.

Eingabe: Matrix A, B und C
$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$
$x \leftarrow Br$
$y \leftarrow Ax$
$z \leftarrow Cr$
wenn $y \neq z$ **dann**
  return NEIN
sonst
  return JA

$$D = \begin{pmatrix} d_1 & \dots & d_\ell & 0 \dots 0 \\ & & \dots & \end{pmatrix}$$

Suche obere Schranke dafür, dass $dr = 0$ ist:

Genau dann, wenn: $\sum_{i=1}^{\ell} d_i \cdot r_i = 0 \quad \Leftrightarrow \sum_{i=1}^{\ell-1} d_i \cdot r_i + d_\ell r_\ell = 0$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.
- Seit d erste Zeile von D, o.B.d.A:
  - sei d nicht der Nullvektor und
  - die Nichtnulleinträge seien die ersten ℓ Einträge.

Eingabe: Matrix A, B und C
$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$
$x \leftarrow Br$
$y \leftarrow Ax$
$z \leftarrow Cr$
wenn $y \neq z$ **dann**
  return NEIN
sonst
  return JA

$$D = \begin{pmatrix} d_1 & \dots & d_\ell & 0 \dots 0 \\ & & \dots & \end{pmatrix}$$

Suche obere Schranke dafür, dass $dr = 0$ ist:

Genau dann, wenn: $\sum_{i=1}^{\ell} d_i \cdot r_i = 0 \quad \Leftrightarrow \sum_{i=1}^{\ell-1} d_i \cdot r_i + d_\ell r_\ell = 0 \quad \Leftrightarrow r_\ell = -\frac{1}{d_\ell} \sum_{i=1}^{\ell-1} d_i \cdot r_i \qquad (1)$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

Eingabe: Matrix A, B und C
$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$
$x \leftarrow Br$
$y \leftarrow Ax$
$z \leftarrow Cr$
wenn $y \neq z$ **dann**
  return NEIN
sonst
  return JA

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.
- Seit d erste Zeile von D, o.B.d.A:
  - sei d nicht der Nullvektor und
  - die Nichtnulleinträge seien die ersten ℓ Einträge.

$$D = \begin{pmatrix} d_1 & \dots & d_\ell & 0 \dots 0 \\ & & \dots & \end{pmatrix}$$

Suche obere Schranke dafür, dass $dr = 0$ ist:

Genau dann, wenn: $\sum_{i=1}^{\ell} d_i \cdot r_i = 0 \quad \Leftrightarrow \sum_{i=1}^{\ell-1} d_i \cdot r_i + d_\ell r_\ell = 0 \quad \Leftrightarrow r_\ell = -\frac{1}{d_\ell} \sum_{i=1}^{\ell-1} d_i \cdot r_i \qquad (1)$

Nehme an $r_1, \dots, r_{\ell-1}$ wurden bereits gewählt:

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

5. Problem

2. Zeigen Sie, dass die Wahrscheinlichkeit dass der Algorithmus JA liefert, obwohl $AB \neq C$ gilt, kleiner gleich $\frac{1}{2}$ ist.

Eingabe: Matrix A, B und C
$r \leftarrow \langle$ Vektor von n unabhängigen Zufallsbits $\rangle$
$x \leftarrow Br$
$y \leftarrow Ax$
$z \leftarrow Cr$
wenn $y \neq z$ **dann**
  return NEIN
sonst
  return JA

- Nehme also an $AB \neq C$ und somit $D := AB - C \neq 0$.
- Alorithmus liefert JA genau dann wenn $Dr = 0$.
- Seit d erste Zeile von D, o.B.d.A:
  - sei d nicht der Nullvektor und
  - die Nichtnulleinträge seien die ersten ℓ Einträge.

$$D = \begin{pmatrix} d_1 & \dots & d_\ell & 0 \dots 0 \\ & & \dots & \end{pmatrix}$$

Suche obere Schranke dafür, dass $dr = 0$ ist:

$$\text{Genau dann, wenn: } \sum_{i=1}^{\ell} d_i \cdot r_i = 0 \quad \Leftrightarrow \sum_{i=1}^{\ell-1} d_i \cdot r_i + d_\ell r_\ell = 0 \quad \Leftrightarrow r_\ell = -\frac{1}{d_\ell} \sum_{i=1}^{\ell-1} d_i \cdot r_i \qquad (1)$$

Nehme an $r_1, \dots, r_{\ell-1}$ wurden bereits gewählt:

Gleichung (1) kann für höchstens einen Wert von r_i wahr sein.

Wahrscheinlichkeit ist $\frac{1}{2}$, dass gerade dieser Wert gewählt wurde.

5. Problem

3. Wie kann diese Wahrscheinlichkeit einer fälschlichen Ausgabe JA einfach reduziert werden?

Durch k-fache Wiederholung des Algorithmus kann die Fehlerwahrscheinlichkeit wie üblich auf 2^{-k} gedrückt werden.