Karlsruher Institut für Technologie

Algorithmen II
Übung am 05.12.2013

Randomisierte Algorithmen

INSTITUT FÜR THEORETISCHE INFORMATIK · PROF. DR. DOROTHEA WAGNER

Organisatorisches

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Klausur

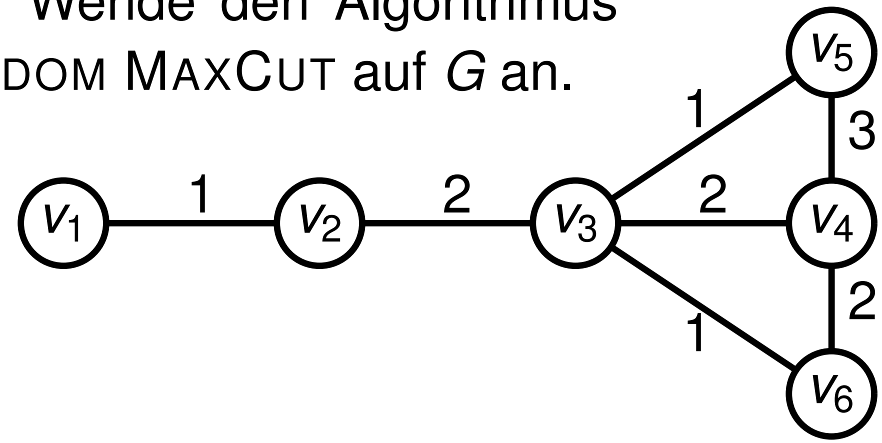
- Anmeldung für die Hauptklausur am 24.02.2014 (14:00 Uhr) ist ab jetzt möglich.
- An- und Abmeldung ist bis zum 17.02.2014 online möglich.
- **Danach ist keine Anmeldung mehr möglich.**
- Nachklausur findet erst im Sommer statt.

Random MaxCut

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1

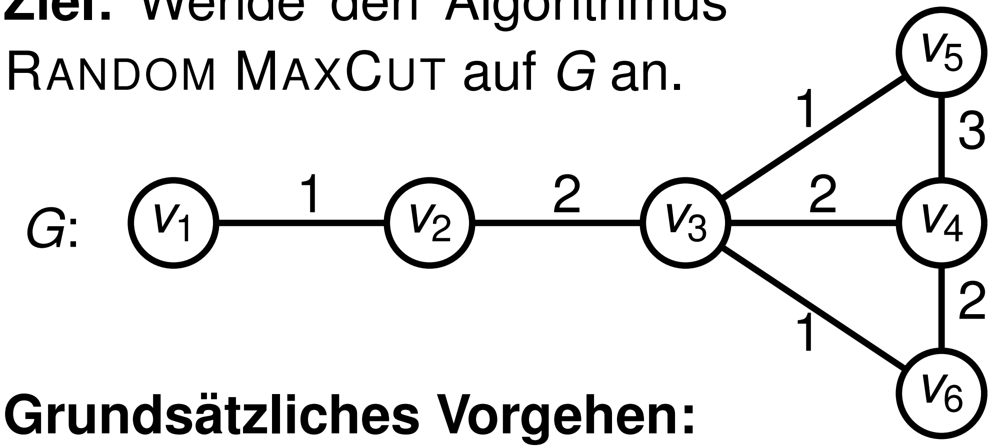
Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.

G: 

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



Grundsätzliches Vorgehen:

$G = (V, E)$ —Transformation→ 1-dimensionales quadratisches Programm

1-dimensionales quadratisches Programm —Relaxierung auf k Dimensionen für $k \leq n$→ quadratisches Programm QP^k

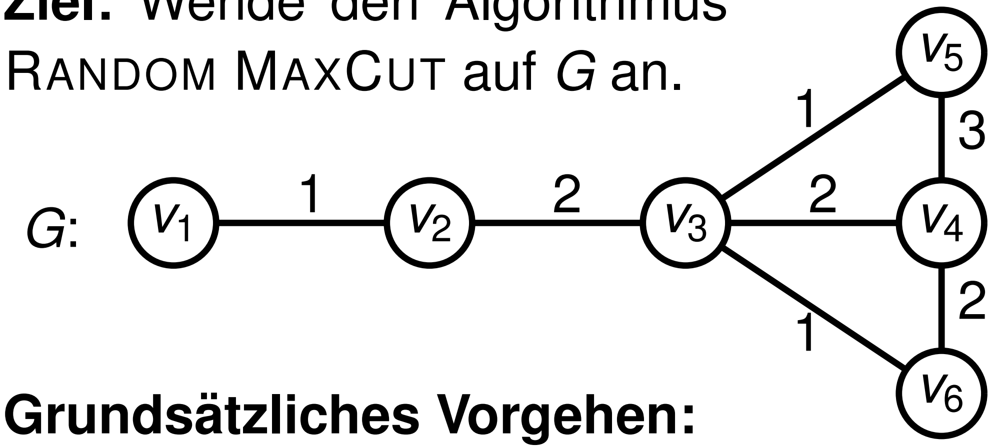
quadratisches Programm QP^k —Lösen von QP^k→ Reellwertige Lösung von QP^k

Reellwertige Lösung von QP^k —Runden der Lösung randomisierter Algo.→ Ganzzahlige 1-dim. Lösung

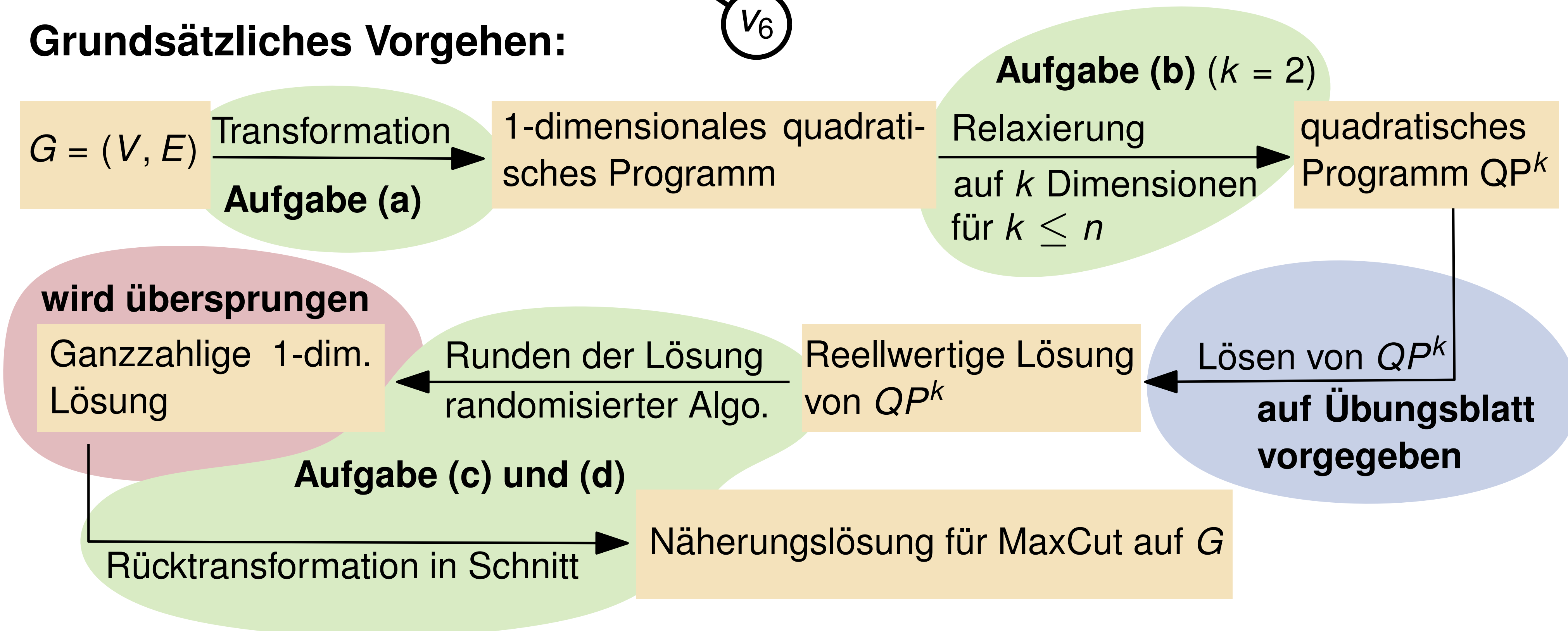
Ganzzahlige 1-dim. Lösung —Rücktransformation in Schnitt→ Näherungslösung für MaxCut auf G

Problem 1

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.

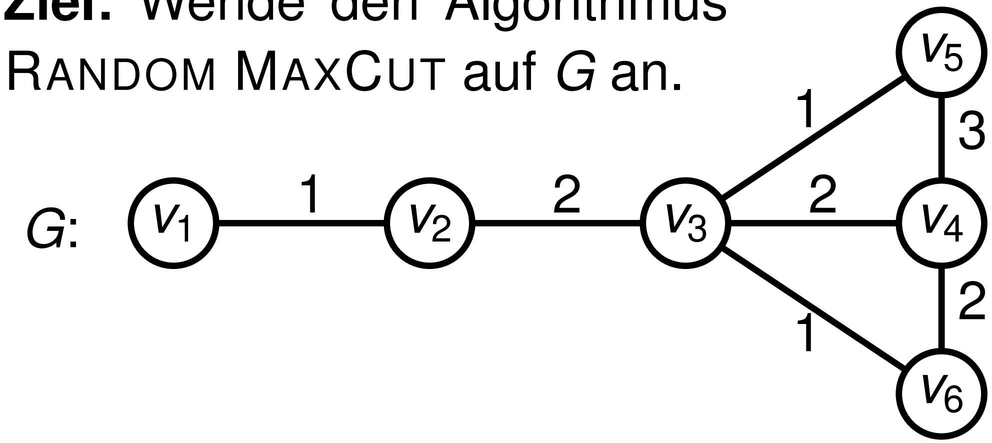


Grundsätzliches Vorgehen:



Problem 1 (a)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



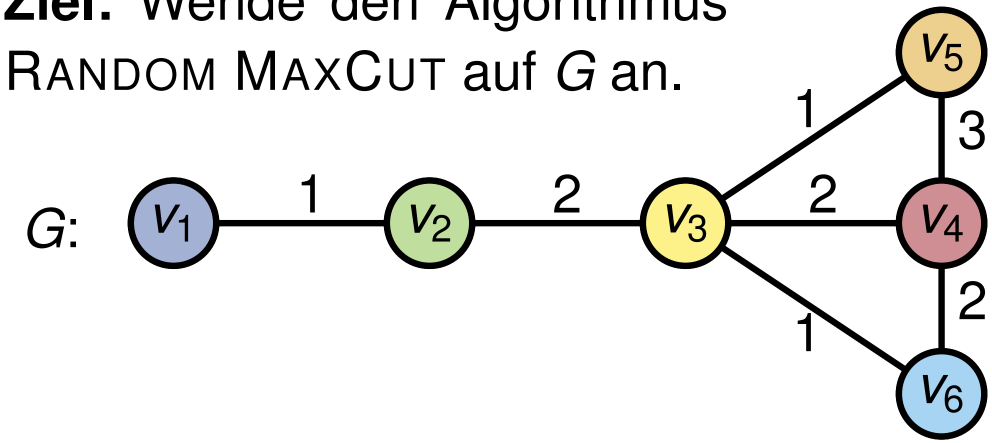
$G = (V, E)$

↓ Transformation **Aufgabe (a)**

1-dimensionales quadratisches Programm

Problem 1 (a)

Ziel: Wende den Algorithmus Random MaxCut auf G an.



$G = (V, E)$

↓ Transformation **Aufgabe (a)**

1-dimensionales quadratisches Programm

Variablen:

$\underbrace{x_1, x_2, x_3, x_4, x_5, x_6}_{\text{eine Variable für jeden Knoten}}$

Nebenbedingungen:

$$x_i \cdot x_i = 1$$

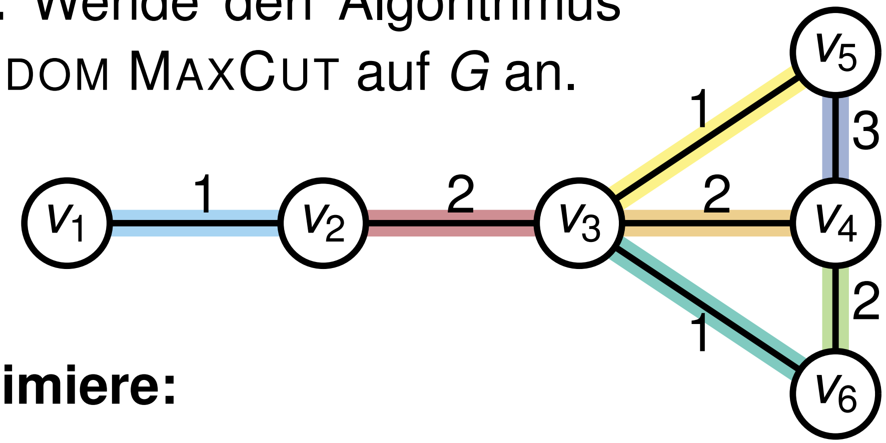
Variablen sind entweder 1 oder -1
(also auf der einen oder anderen Seite des Schnitts)

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1 (a)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.

G:



$G = (V, E)$

Transformation
Aufgabe (a)

1-dimensionales quadratisches Programm

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

Variablen:

$$\underbrace{x_1, x_2, x_3, x_4, x_5, x_6}_{\text{eine Variable für jeden Knoten}}$$

Nebenbedingungen:

$$x_i \cdot x_i = 1$$

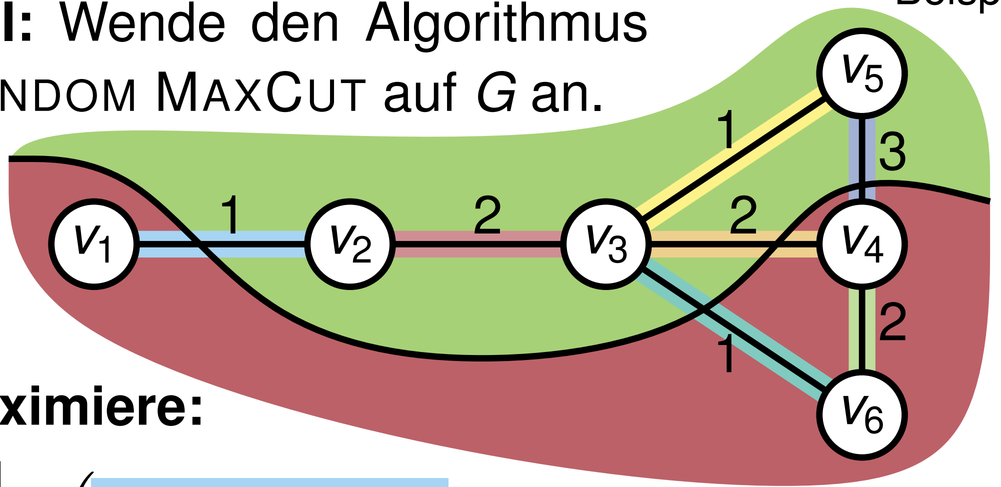
Variablen sind entweder 1 oder -1
(also auf der einen oder anderen Seite des Schnitts)

Problem 1 (a)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.

Beispielschnitt

G:



$G = (V, E)$

Transformation
Aufgabe (a)

1-dimensionales quadratisches Programm

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

ergibt genau das Gewicht des Schnitts

Variablen:

$\underbrace{x_1, x_2, x_3, x_4, x_5, x_6}$ eine Variable für jeden Knoten

Nebenbedingungen:

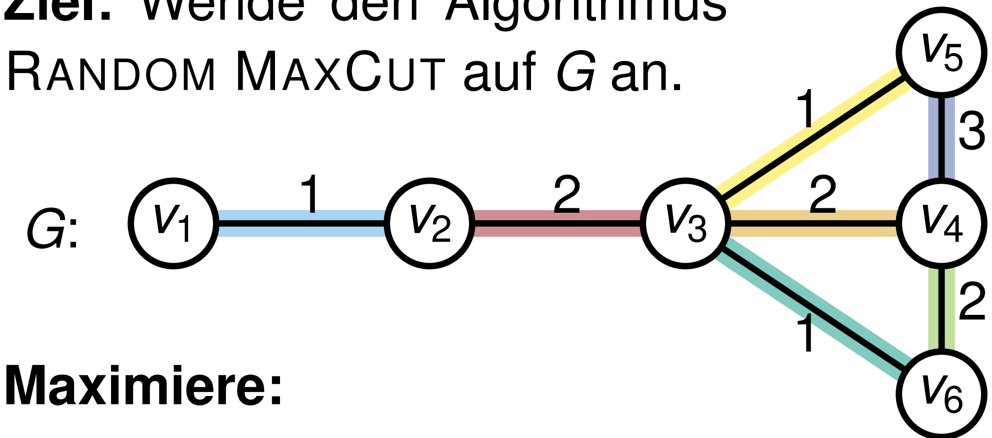
$$x_i \cdot x_i = 1$$

Variablen sind entweder 1 oder -1
(also auf der einen oder anderen Seite des Schnitts)

Problem 1 (b)

Karlsruher Institut für Technologie

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



1-dimensionales quadratisches Programm

Relaxierung auf k Dimensionen

Aufgabe (b) ($k = 2$)

quadratisches Programm QP^k

Was ändert sich?

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

ergibt genau das Gewicht des Schnitts

Variablen:

$$\underbrace{x_1, x_2, x_3, x_4, x_5, x_6}_{\text{eine Variable für jeden Knoten}}$$

Nebenbedingungen:

$$x_i \cdot x_i = 1$$

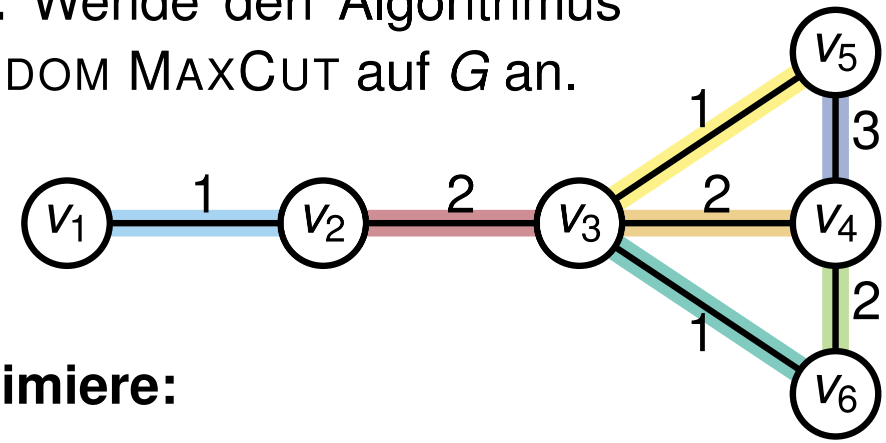
Variablen sind entweder 1 oder -1
(also auf der einen oder anderen Seite des Schnitts)

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1 (b)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.

G:



1-dimensionales quadratisches Programm

$\downarrow$ Relaxierung auf k Dimensionen
Aufgabe (b) ($k = 2$)

quadratisches Programm QP^k

Was ändert sich?

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

ergibt genau das Gewicht des Schnitts

Variablen:

$\underbrace{x_1, x_2, x_3, x_4, x_5, x_6}$

ein 2-Dim Vektor als
~~eine~~ Variable für jeden Knoten

Nebenbedingungen:

$$x_i \cdot x_i = 1$$

Variablen sind entweder 1 oder -1
(also auf der einen oder anderen Seite des Schnitts)

Problem 1 (b)

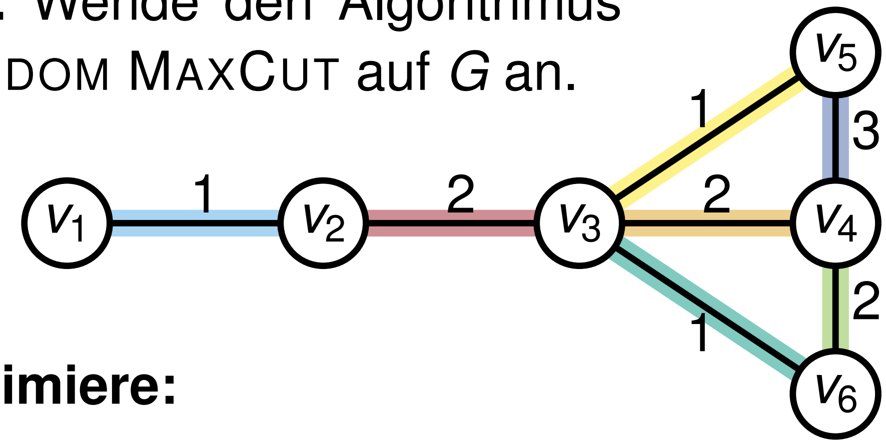
Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.

1-dimensionales quadratisches Programm

Relaxierung auf k Dimensionen
Aufgabe (b) ($k = 2$)

quadratisches Programm QP^k

G:



Was ändert sich?

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

ergibt genau das Gewicht des Schnitts

Variablen:

$x_1, x_2, x_3, x_4, x_5, x_6$

ein 2-Dim Vektor als

~~eine~~ Variable für jeden Knoten

Nebenbedingungen:

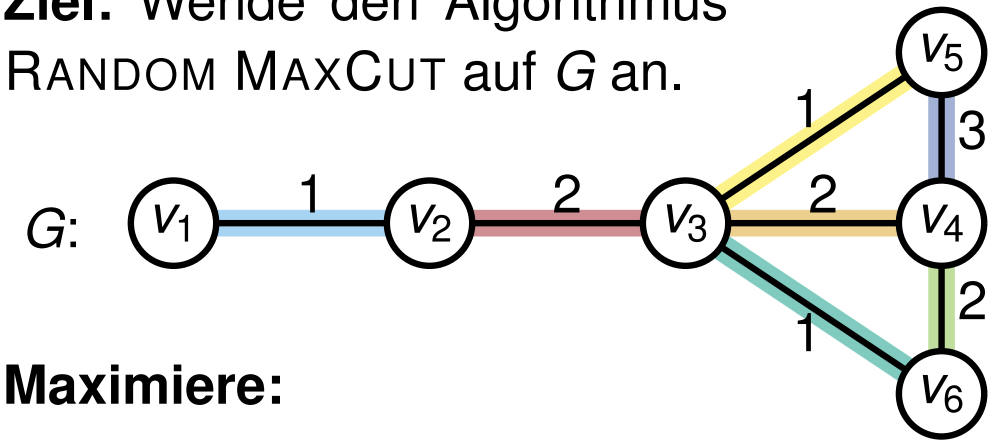
$x_i \cdot x_i = 1$

jeder Vektor x_i hat Länge 1

~~Variablen sind entweder 1 oder −1~~
~~(also auf der einen oder anderen Seite des Schnitts)~~

Problem 1 (b)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



1-dimensionales quadratisches Programm

Relaxierung auf k Dimensionen
Aufgabe (b) ($k = 2$)

quadratisches Programm QP^k

Was ändert sich?

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

~~ergibt genau das Gewicht des Schnitts~~
maximiert Winkel zwischen verbundenen Knoten
(gewichtet mit Kantengewicht)

Variablen:

$$\underbrace{x_1, x_2, x_3, x_4, x_5, x_6}$$

~~eine~~ ein 2-Dim Vektor als Variable für jeden Knoten

Nebenbedingungen:

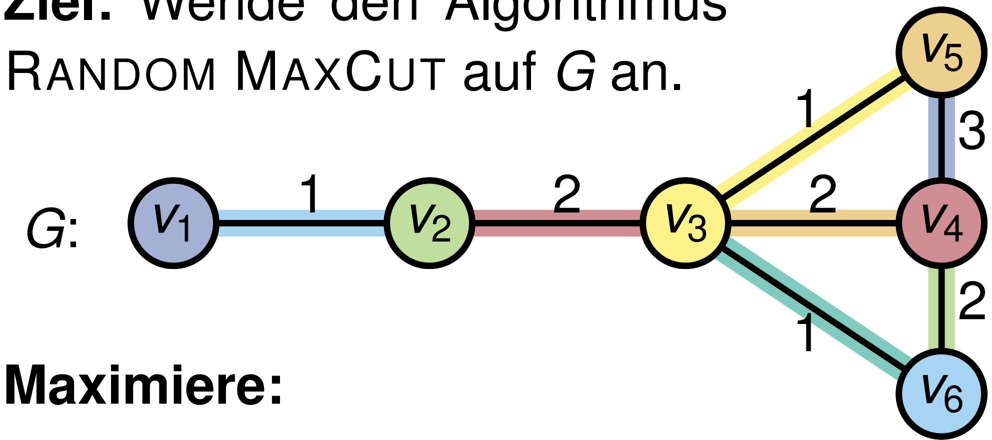
$$x_i \cdot x_i = 1$$

jeder Vektor x_i hat Länge 1
~~Variablen sind entweder 1 oder −1~~
~~(also auf der einen oder anderen Seite des Schnitts)~~

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



quadratisches Programm QP^k

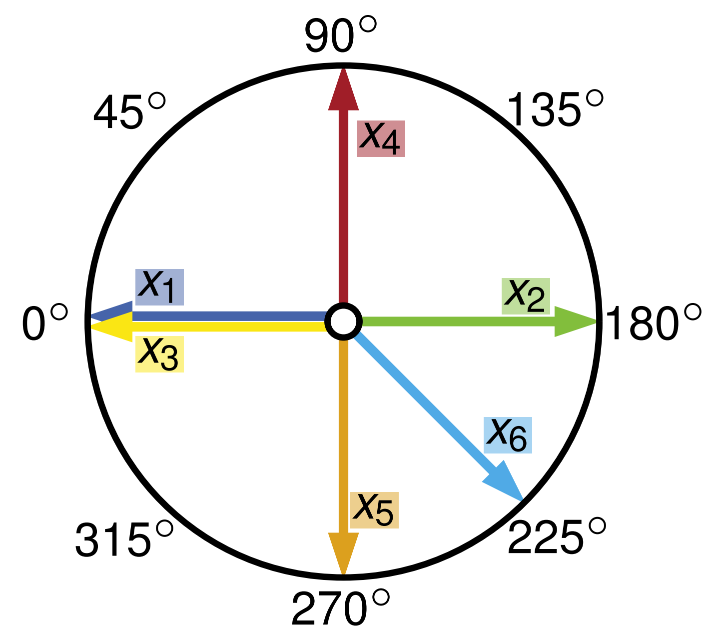
↓ Lösen von QP^k

Reellwertige Lösung von QP^k

auf Übungsblatt vorgegeben

Maximiere:

$$\frac{1}{2} \cdot \Big(1 \cdot (1 - x_1 \cdot x_2) + 2 \cdot (1 - x_2 \cdot x_3) + 2 \cdot (1 - x_3 \cdot x_4) + 1 \cdot (1 - x_3 \cdot x_5) + 1 \cdot (1 - x_3 \cdot x_6) + 3 \cdot (1 - x_4 \cdot x_5) + 2 \cdot (1 - x_4 \cdot x_6) \Big)$$

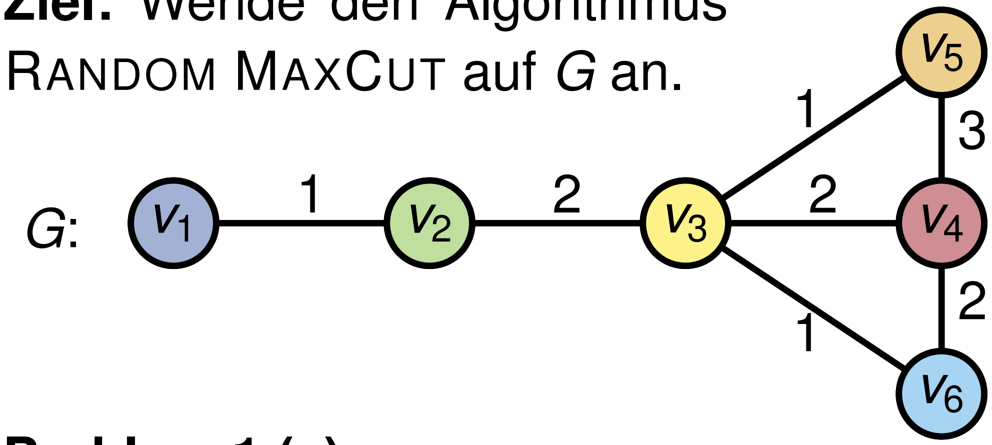


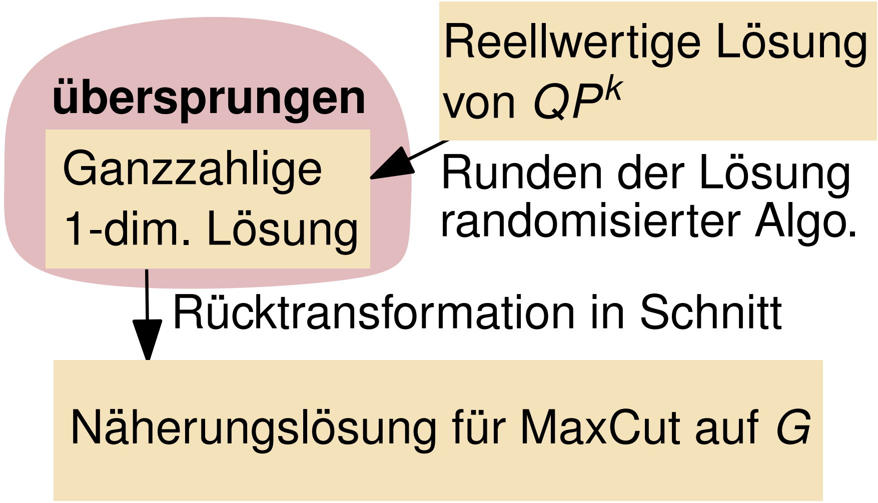
maximiert Winkel zwischen verbundenen Knoten (gewichtet mit Kantengewicht)

~~ergibt genau das Gewicht des Schnitts~~

Problem 1 (c)

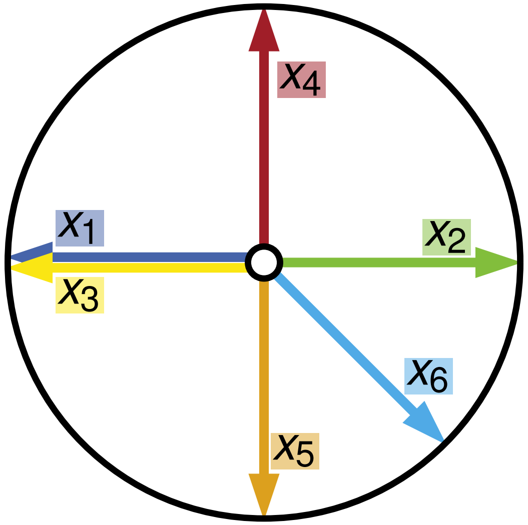
Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.





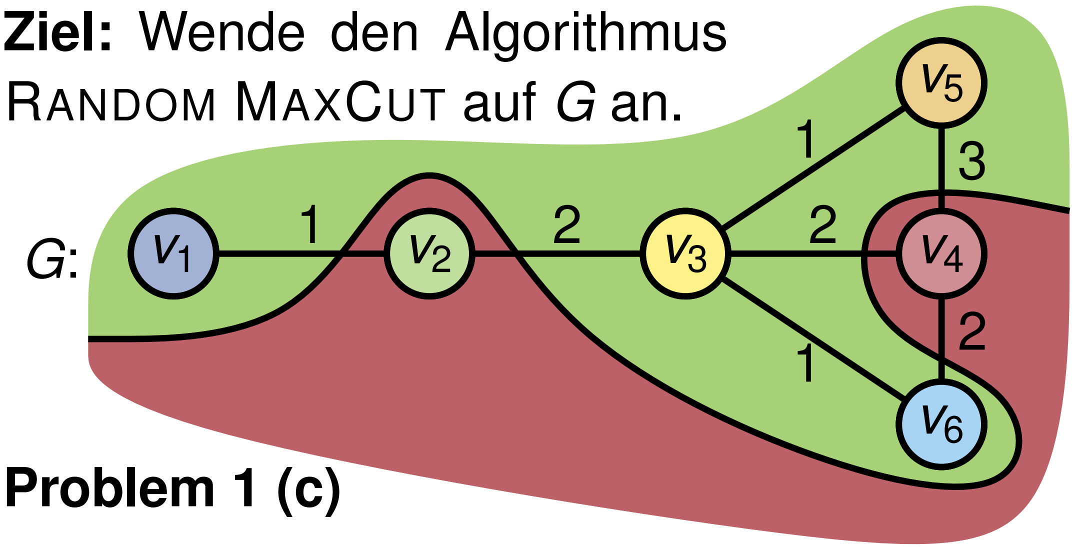
Problem 1 (c)

- *Zähle alle Schnitte auf, die man erhalten kann.*
- *Wie groß ist der Erwartungswert beim zufälligen Runden?*



Problem 1 (c)

Ziel: Wende den Algorithmus Random MaxCut auf G an.



übersprungen

Ganzzahlige 1-dim. Lösung

Reellwertige Lösung von QP^k

Runden der Lösung randomisierter Algo.

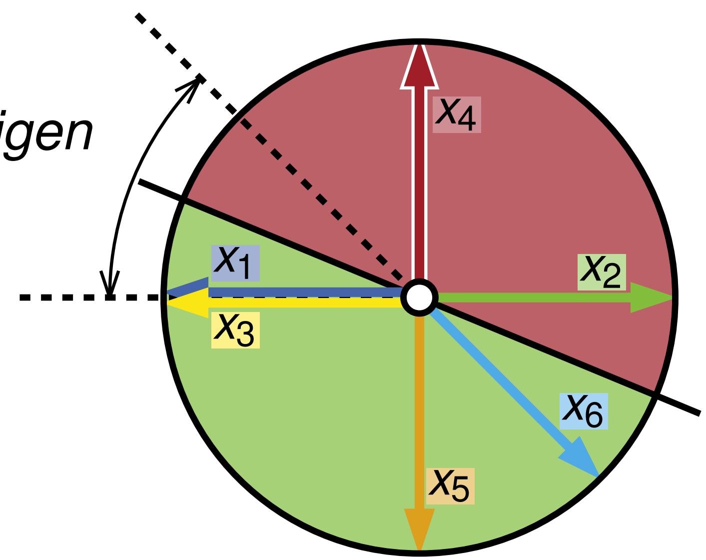
Rücktransformation in Schnitt

Näherungslösung für MaxCut auf G

Problem 1 (c)

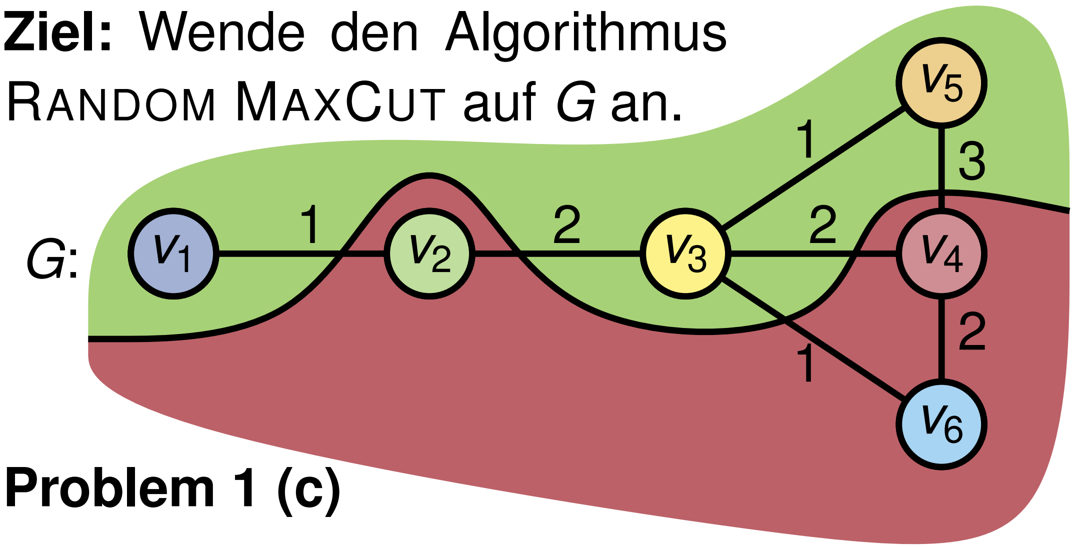
- *Zähle alle Schnitte auf, die man erhalten kann.*
- *Wie groß ist der Erwartungswert beim zufälligen Runden?*

Schnitt	Gewicht	Bereich
$(\{v_1, v_3, v_5, v_6\}, \{v_2, v_4\})$	10	45°



Problem 1 (c)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



übersprungen

Ganzzahlige 1-dim. Lösung

Reellwertige Lösung von QP^k

Runden der Lösung randomisierter Algo.

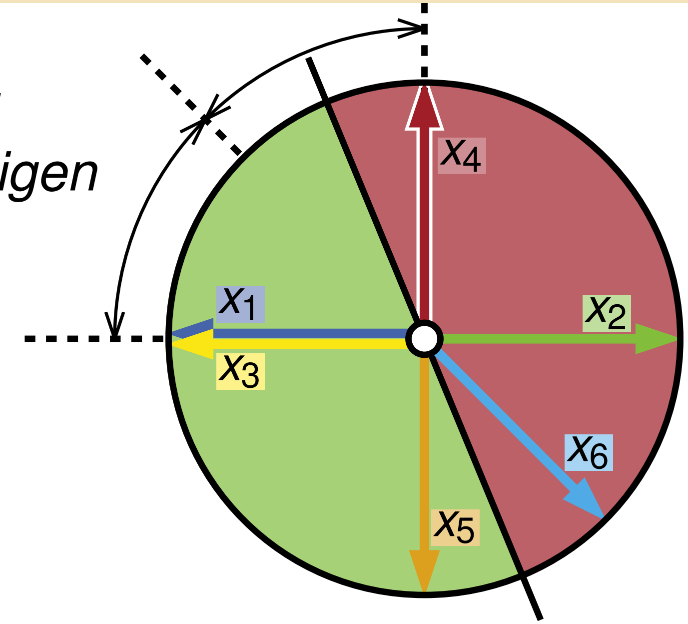
Rücktransformation in Schnitt

Näherungslösung für MaxCut auf G

Problem 1 (c)

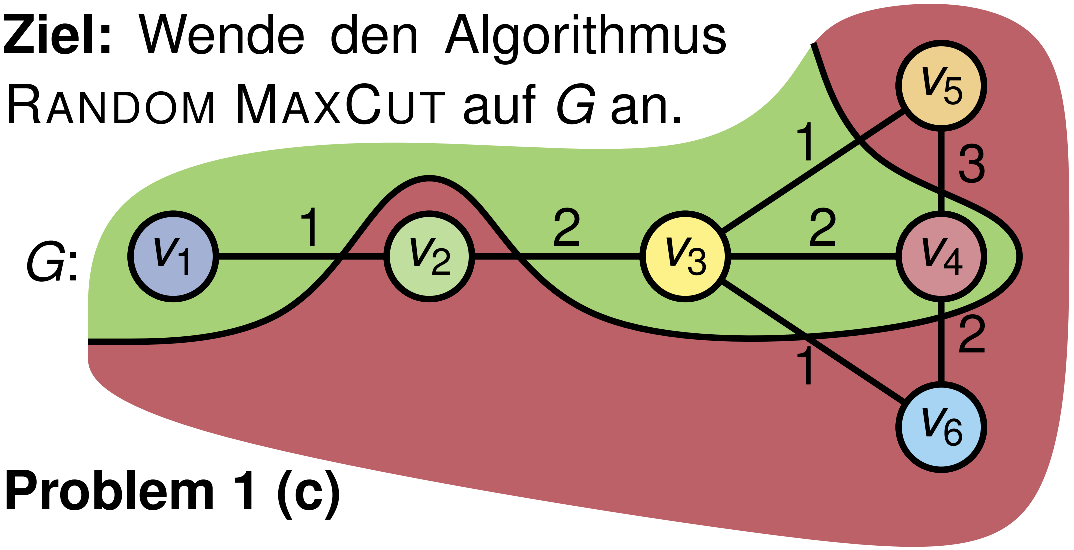
- *Zähle alle Schnitte auf, die man erhalten kann.*
- *Wie groß ist der Erwartungswert beim zufälligen Runden?*

Schnitt	Gewicht	Bereich
$(\{v_1, v_3, v_5, v_6\}, \{v_2, v_4\})$	10	45°
$(\{v_1, v_3, v_5\}, \{v_2, v_4, v_6\})$	9	45°



Problem 1 (c)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



übersprungen

Reellwertige Lösung von QP^k

Ganzzahlige 1-dim. Lösung

Runden der Lösung randomisierter Algo.

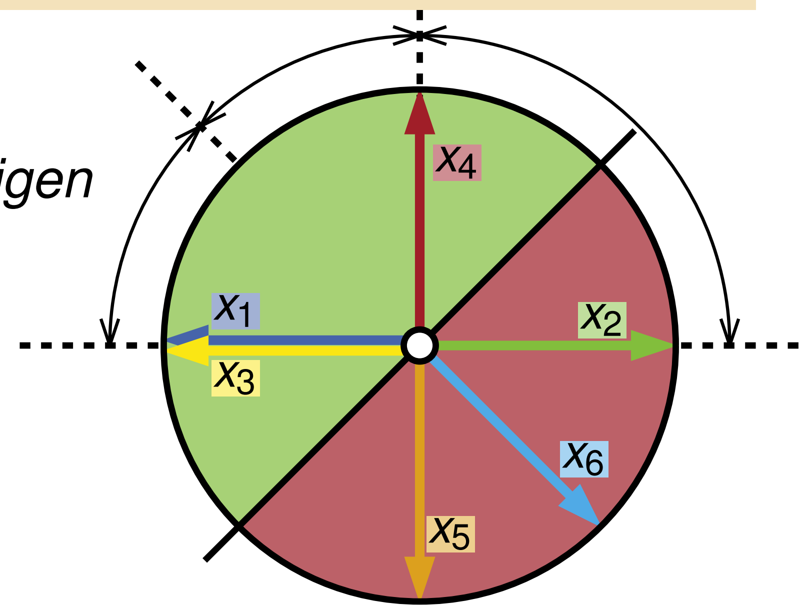
Rücktransformation in Schnitt

Näherungslösung für MaxCut auf G

Problem 1 (c)

- *Zähle alle Schnitte auf, die man erhalten kann.*
- *Wie groß ist der Erwartungswert beim zufälligen Runden?*

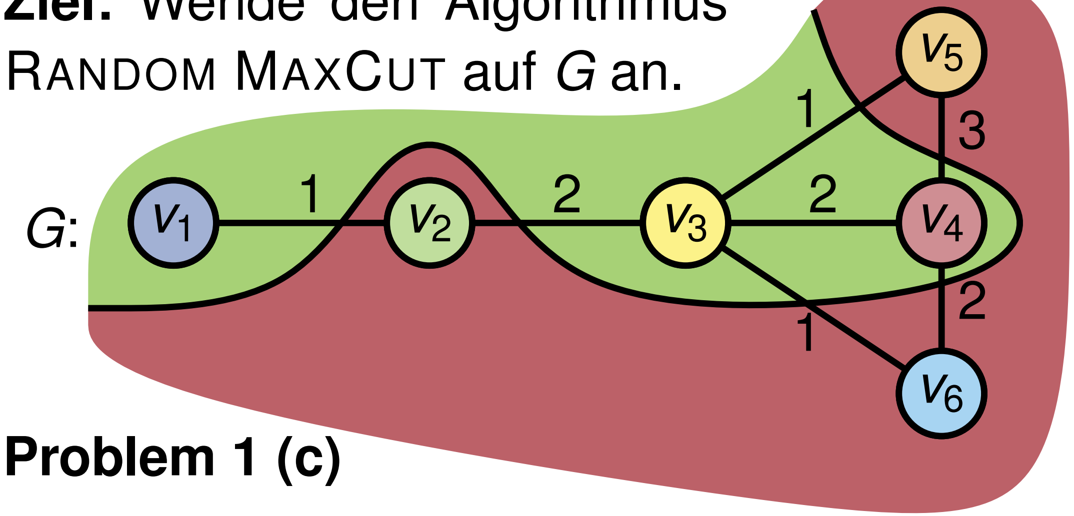
Schnitt	Gewicht	Bereich
$(\{v_1, v_3, v_5, v_6\}, \{v_2, v_4\})$	10	45°
$(\{v_1, v_3, v_5\}, \{v_2, v_4, v_6\})$	9	45°
$(\{v_1, v_3, v_4\}, \{v_2, v_5, v_6\})$	10	90°



Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1 (c)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



übersprungen

Ganzzahlige 1-dim. Lösung

Reellwertige Lösung von QP^k

Runden der Lösung randomisierter Algo.

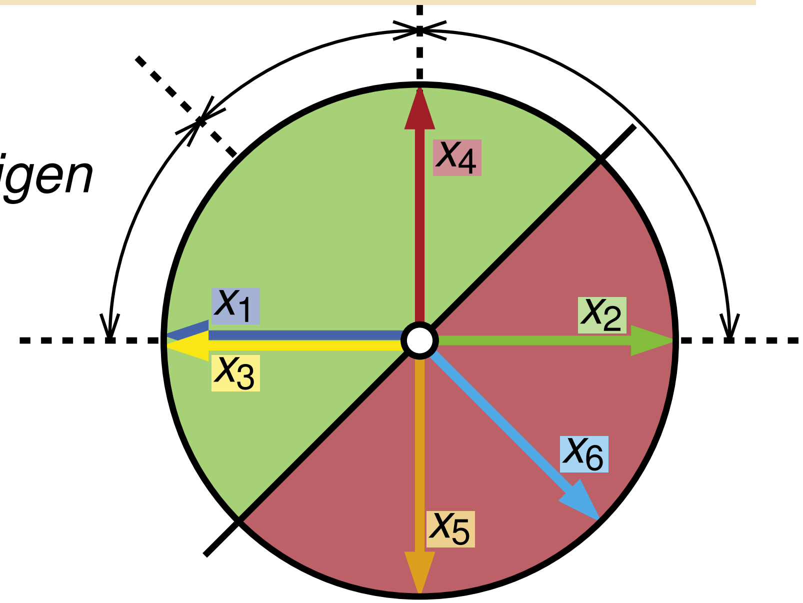
Rücktransformation in Schnitt

Näherungslösung für MaxCut auf G

Problem 1 (c)

- *Zähle alle Schnitte auf, die man erhalten kann.*
- *Wie groß ist der Erwartungswert beim zufälligen Runden?*

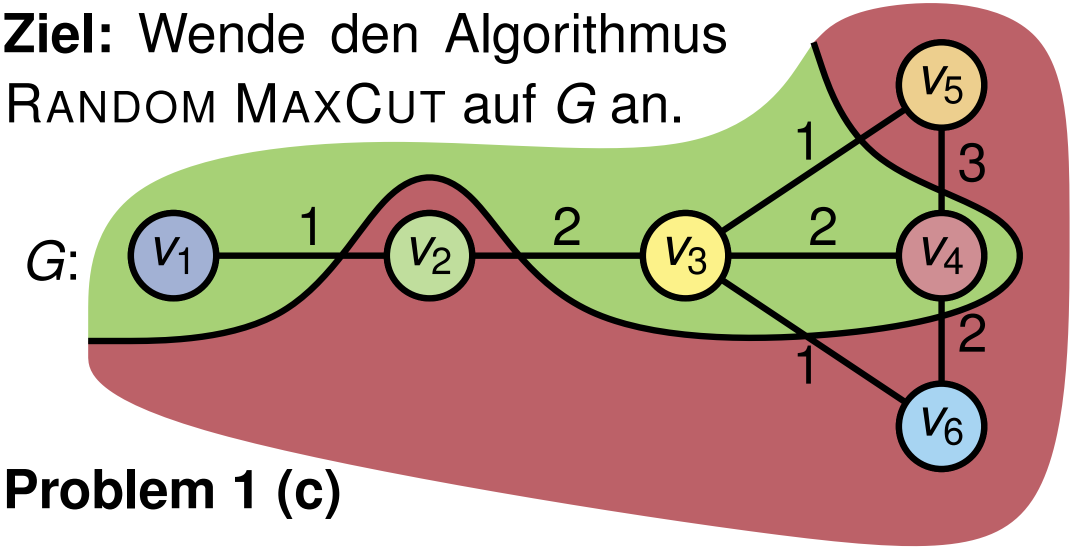
Schnitt	Gewicht	Bereich	Wahrsch.
$(\{v_1, v_3, v_5, v_6\}, \{v_2, v_4\})$	10	45°	$\frac{1}{4}$
$(\{v_1, v_3, v_5\}, \{v_2, v_4, v_6\})$	9	45°	$\frac{1}{4}$
$(\{v_1, v_3, v_4\}, \{v_2, v_5, v_6\})$	10	90°	$\frac{1}{2}$



Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1 (c)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



übersprungen

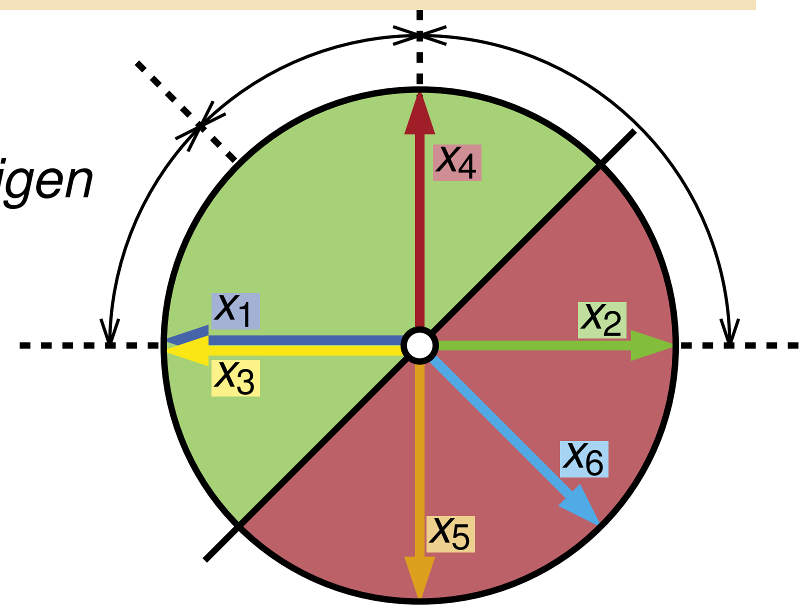
Ganzzahlige 1-dim. Lösung

Reellwertige Lösung von QP^k

Runden der Lösung randomisierter Algo.

Rücktransformation in Schnitt

Näherungslösung für MaxCut auf G



Problem 1 (c)

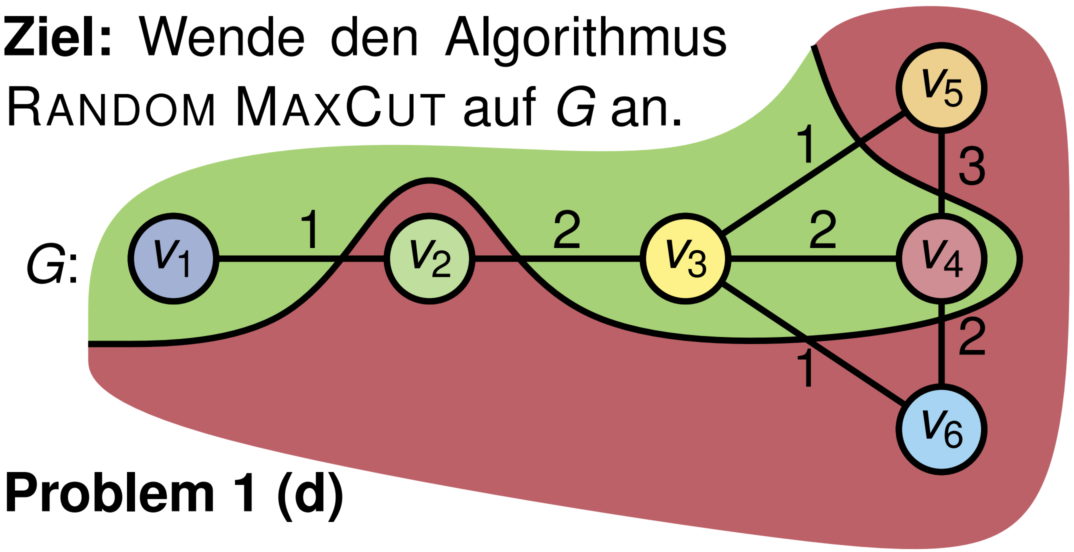
- *Zähle alle Schnitte auf, die man erhalten kann.*
- *Wie groß ist der Erwartungswert beim zufälligen Runden?*

Schnitt	Gewicht	Bereich	Wahrsch.
$(\{v_1, v_3, v_5, v_6\}, \{v_2, v_4\})$	10	45°	$\frac{1}{4}$
$(\{v_1, v_3, v_5\}, \{v_2, v_4, v_6\})$	9	45°	$\frac{1}{4}$
$(\{v_1, v_3, v_4\}, \{v_2, v_5, v_6\})$	10	90°	$\frac{1}{2}$

$\Rightarrow$ Erwartungswert: $\frac{10}{4} + \frac{9}{4} + \frac{10}{2} = \frac{39}{4} = 9.75$

Problem 1 (d)

Ziel: Wende den Algorithmus RANDOM MAXCUT auf G an.



übersprungen

Ganzzahlige 1-dim. Lösung

Reellwertige Lösung von QP^k

Runden der Lösung randomisierter Algo.

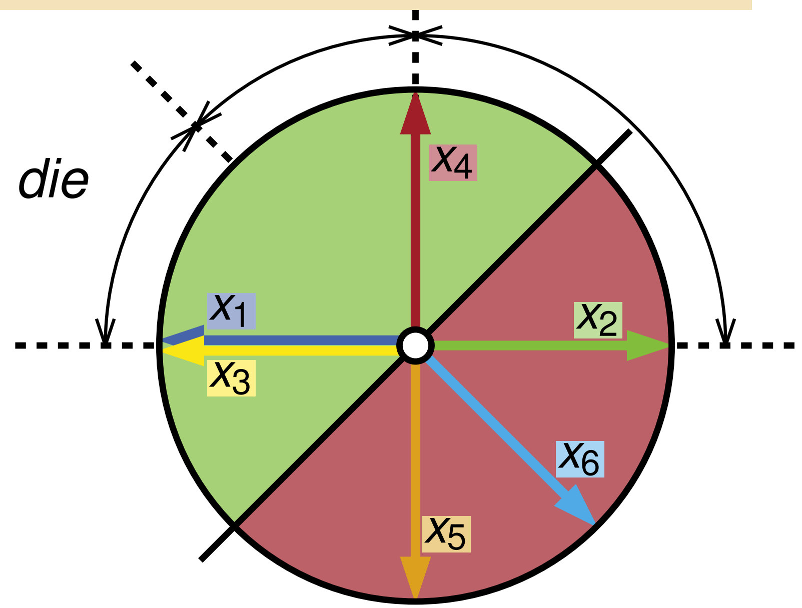
Rücktransformation in Schnitt

Näherungslösung für MaxCut auf G

Problem 1 (d)

- *Warum wählt man eine zufällige Gerade?*
- *Kann man nicht einfach die Gerade wählen, die den beste Schnitt liefert?*

Schnitt	Gewicht	Bereich	Wahrsch.
$(\{v_1, v_3, v_5, v_6\}, \{v_2, v_4\})$	10	45°	$\frac{1}{4}$
$(\{v_1, v_3, v_5\}, \{v_2, v_4, v_6\})$	9	45°	$\frac{1}{4}$
$(\{v_1, v_3, v_4\}, \{v_2, v_5, v_6\})$	10	90°	$\frac{1}{2}$

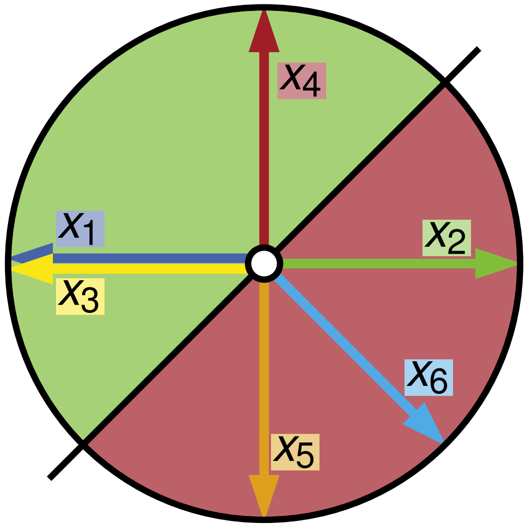


$\Rightarrow$ Erwartungswert: $\frac{10}{4} + \frac{9}{4} + \frac{10}{2} = \frac{39}{4} = 9.75$

Problem 1(d)

Problem 1 (d)

- *Warum wählt man eine zufällige Gerade?*
- *Kann man nicht einfach die Gerade wählen, die den beste Schnitt liefert?*



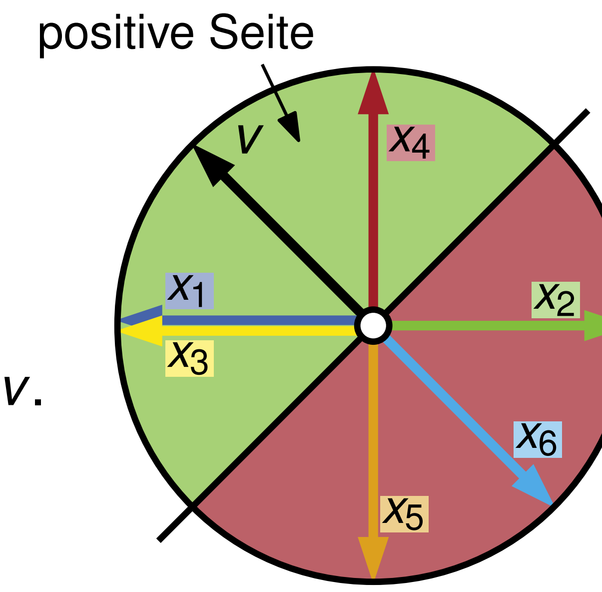
Problem 1(d)

Problem 1 (d)

- *Warum wählt man eine zufällige Gerade?*
- *Kann man nicht einfach die Gerade wählen, die den beste Schnitt liefert?*

Beachte:

- Die Wahl der Gerade entspr. der Wahl eines Vektors v.
- x_i ist auf der *positiven* Seite, wenn $v \cdot x_i \geq 0$



Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 1(d)

Problem 1 (d)

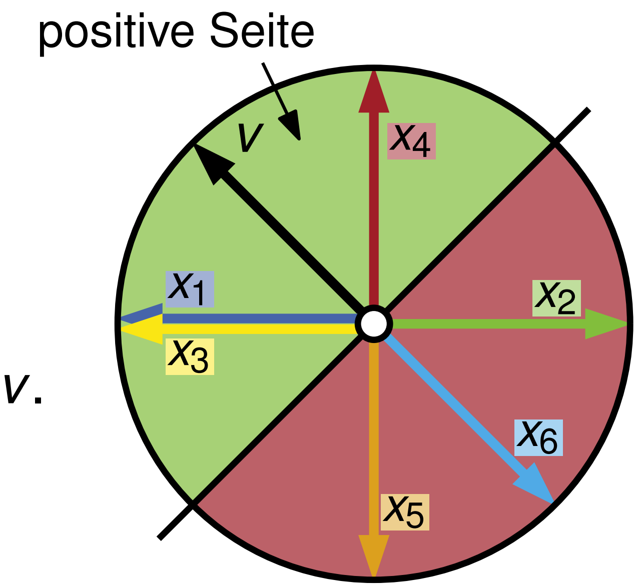
- *Warum wählt man eine zufällige Gerade?*
- *Kann man nicht einfach die Gerade wählen, die den beste Schnitt liefert?*

Beachte:

- Die Wahl der Gerade entspr. der Wahl eines Vektors v.
- x_i ist auf der *positiven* Seite, wenn $v \cdot x_i \geq 0$

Problem:

- Eigentlich hat man keine Lösung von QP^2 sondern von $QP^n \Rightarrow x_i$ hat Dim. n.

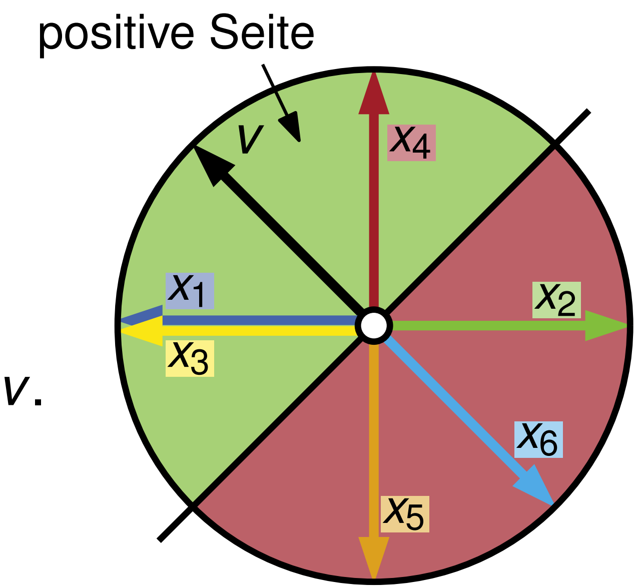


Wie viele verschiedene Schnitte können wir erhalten?

Problem 1(d)

Problem 1 (d)

- *Warum wählt man eine zufällige Gerade?*
- *Kann man nicht einfach die Gerade wählen, die den beste Schnitt liefert?*



Beachte:

- Die Wahl der Gerade entspr. der Wahl eines Vektors v.
- x_i ist auf der *positiven* Seite, wenn $v \cdot x_i \geq 0$

Problem:

- Eigentlich hat man keine Lösung von QP^2 sondern von $QP^n \Rightarrow x_i$ hat Dim. n.

Wie viele verschiedene Schnitte können wir erhalten?

Ungünstiger Fall:

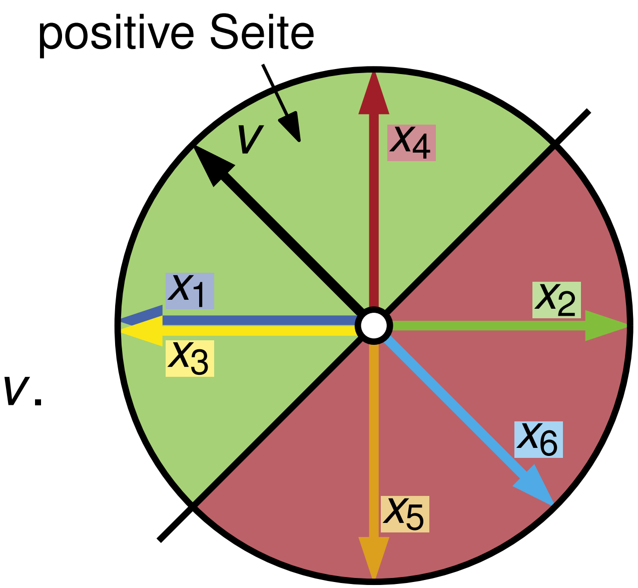
- $\{x_1, \ldots, x_n\}$ bilden Standardbasis im $\mathbb{R}^n$
- $\Rightarrow v \cdot x_i \geq 0$ genau dann, wenn $v_i \geq 0$ (v_i ist i-ter Eintrag von v)

$$x_1, \ldots, x_n = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Problem 1(d)

Problem 1 (d)

- *Warum wählt man eine zufällige Gerade?*
- *Kann man nicht einfach die Gerade wählen, die den beste Schnitt liefert?*



Beachte:

- Die Wahl der Gerade entspr. der Wahl eines Vektors v.
- x_i ist auf der *positiven* Seite, wenn $v \cdot x_i \geq 0$

Problem:

- Eigentlich hat man keine Lösung von QP^2 sondern von $\mathrm{QP}^n \Rightarrow x_i$ hat Dim. n.

Wie viele verschiedene Schnitte können wir erhalten?

Ungünstiger Fall:

- $\{x_1, \ldots, x_n\}$ bilden Standardbasis im $\mathbb{R}^n$
- $\Rightarrow v \cdot x_i \geq 0$ genau dann, wenn $v_i \geq 0$ (v_i ist i-ter Eintrag von v)

$$x_1, \ldots, x_n = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

$\Rightarrow$ Alle 2^n möglichen Schnitte können gefunden werden.

Gleichverteiltes JA/NEIN

Problem 2

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* $\frac{1}{2}$*.*

Problem 2

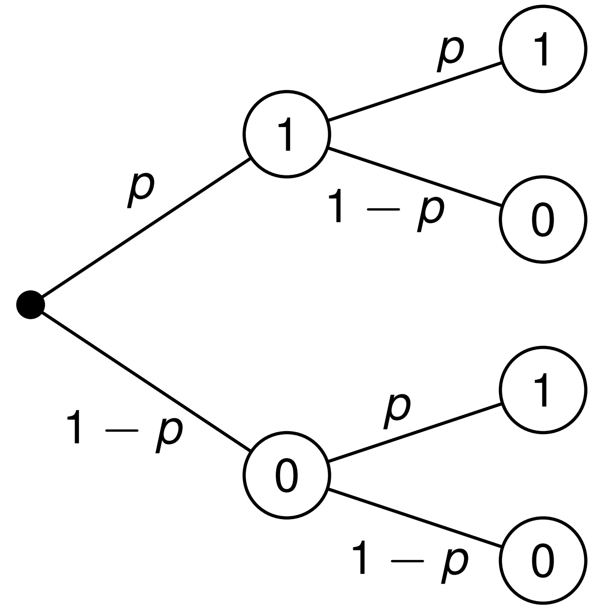
Gegeben: *Zufallsgenerator* $\mathcal{A}_1$*:*

- *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* $\frac{1}{2}$.

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



Problem 2

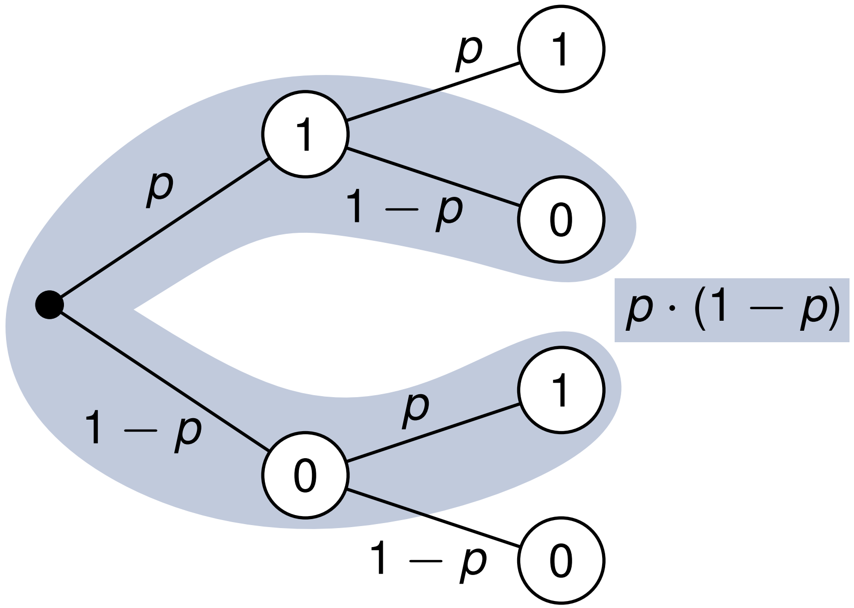
Gegeben: *Zufallsgenerator* $\mathcal{A}_1$*:*

- *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* $\frac{1}{2}$*.*

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



Problem 2

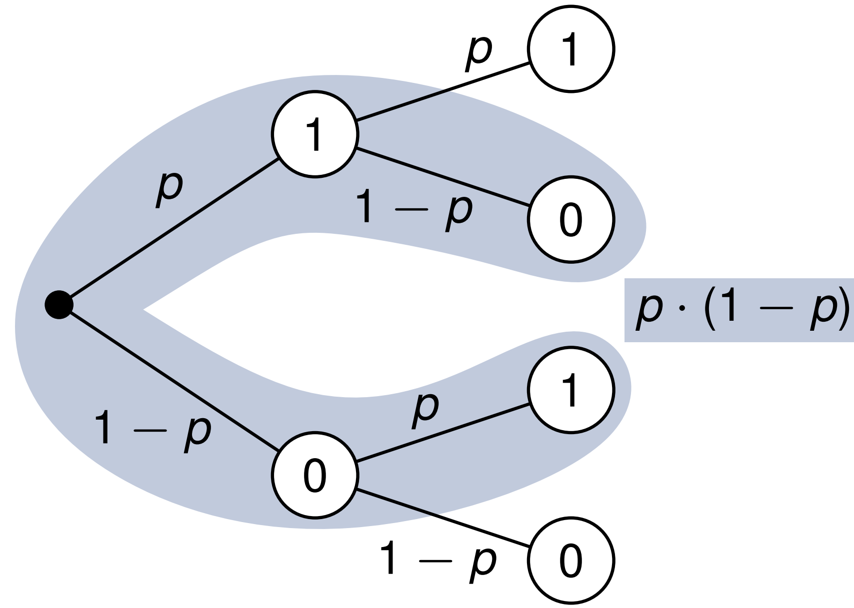
Gegeben: *Zufallsgenerator* $\mathcal{A}_1$:

- *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* $\frac{1}{2}$.

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$

$y \leftarrow 0$

while $x = y$ **do**

  $x \leftarrow \mathcal{A}_1()$

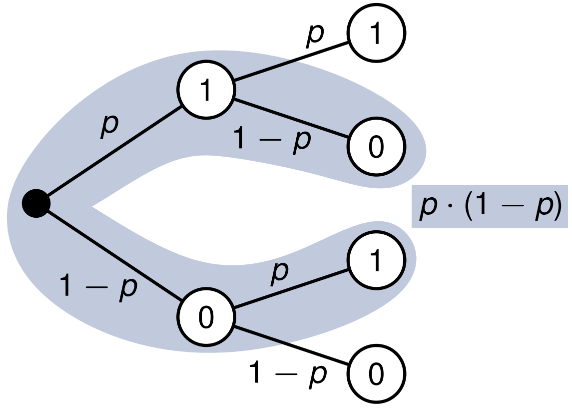
  $y \leftarrow \mathcal{A}_1()$

return x

Problem 2

Was ist die erwartete Laufzeit?

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$

$y \leftarrow 0$

while $x = y$ **do**

  $x \leftarrow \mathcal{A}_1()$

  $y \leftarrow \mathcal{A}_1()$

return x

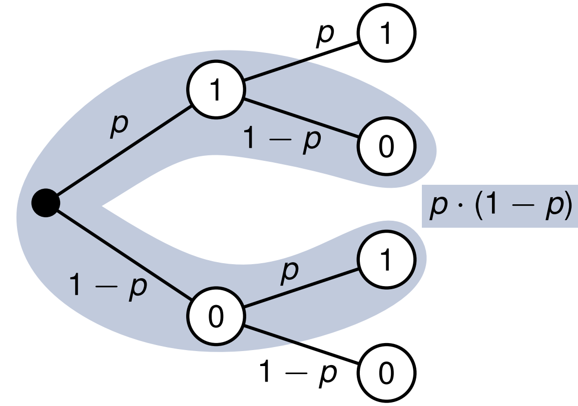
Problem 2

Was ist die erwartete Laufzeit?

- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit

$$q = \Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$$

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$
$y \leftarrow 0$
while $x = y$ **do**
  $x \leftarrow \mathcal{A}_1()$
  $y \leftarrow \mathcal{A}_1()$
return x

Problem 2

Karlsruher Institut für Technologie

Was ist die erwartete Laufzeit?

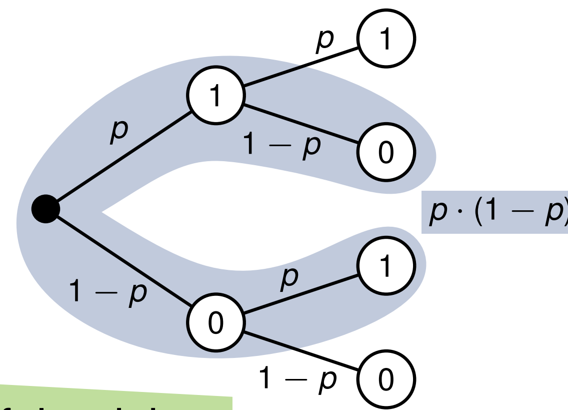
- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit

$$q = \Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$$

- Wahrscheinlichkeit für n Durchläufe:

$$\Pr[X = n] = \underbrace{(1-q)^{n-1}}_{n-1 \text{ erfolglose,}} \cdot \underbrace{q}_{\text{gefolgt von einem erfolgreichen}}$$

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$

$y \leftarrow 0$

while $x = y$ **do**

  $x \leftarrow \mathcal{A}_1()$

  $y \leftarrow \mathcal{A}_1()$

return x

Problem 2

Was ist die erwartete Laufzeit?

- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit

$$q = \Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$$

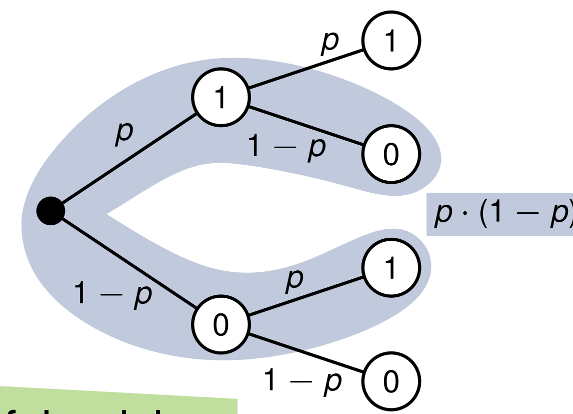
- Wahrscheinlichkeit für n Durchläufe:

$$\Pr[X = n] = \underbrace{(1-q)^{n-1}}_{n-1 \text{ erfolglose,}} \cdot \underbrace{q}_{\text{gefolgt von einem erfolgreichen}}$$

- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X = n]} \cdot n$$

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$
$y \leftarrow 0$
while $x = y$ **do**
  $x \leftarrow \mathcal{A}_1()$
  $y \leftarrow \mathcal{A}_1()$
return x

Problem 2

Was ist die erwartete Laufzeit?

- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit

$$q = \Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$$

- Wahrscheinlichkeit für n Durchläufe:

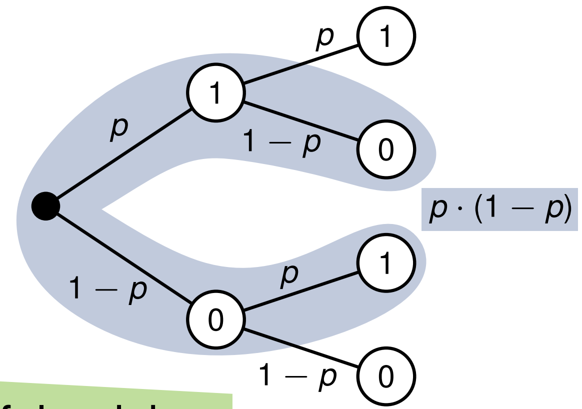
$$\Pr[X = n] = \underbrace{(1-q)^{n-1}}_{n-1 \text{ erfolglose,}} \cdot \underbrace{q}_{\text{gefolgt von einem erfolgreichen}}$$

- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X = n]} \cdot n = \frac{1}{q}$$

geometrische Verteilung
(Beweis: folgt gleich)

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$
$y \leftarrow 0$
while $x = y$ **do**
  $x \leftarrow \mathcal{A}_1()$
  $y \leftarrow \mathcal{A}_1()$
return x

Problem 2

Was ist die erwartete Laufzeit?

- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit

$$q = \Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$$

- Wahrscheinlichkeit für n Durchläufe:

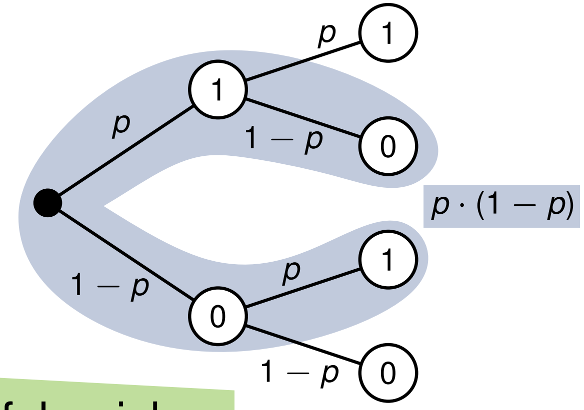
$$\Pr[X = n] = \underbrace{(1-q)^{n-1}}_{n-1 \text{ erfolglose,}} \cdot \underbrace{q}_{\text{gefolgt von einem erfolgreichen}}$$

- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X = n]} \cdot n = \frac{1}{q} = \frac{1}{2 \cdot p \cdot (1-p)}$$

geometrische Verteilung
(Beweis: folgt gleich)

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$
$y \leftarrow 0$
while $x = y$ **do**
  $x \leftarrow \mathcal{A}_1()$
  $y \leftarrow \mathcal{A}_1()$
return x

Problem 2

Was ist die erwartete Laufzeit?

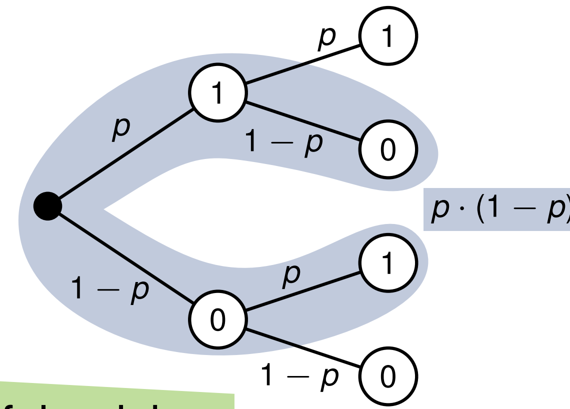
- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit

  $$q = \Pr[x \neq y] = 2 \cdot p \cdot (1 - p)$$

- Wahrscheinlichkeit für n Durchläufe:

  $$\Pr[X = n] = \underbrace{(1 - q)^{n-1}}_{n-1 \text{ erfolglose,}} \cdot \underbrace{q}_{\text{gefolgt von einem erfolgreichen}}$$

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



- Erwartungswert:

  $$E(X) = \sum_{n=1}^{\infty} \underbrace{(1 - q)^{n-1} \cdot q}_{\Pr[X = n]} \cdot n = \frac{1}{q} = \frac{1}{2 \cdot p \cdot (1 - p)}$$

  geometrische Verteilung
  (Beweis: folgt gleich)

$\Rightarrow$ Erwartete Laufzeit: $\Theta\left(\dfrac{1}{p \cdot (1 - p)}\right)$

$x \leftarrow 0$
$y \leftarrow 0$
while $x = y$ **do**
    $x \leftarrow \mathcal{A}_1()$
    $y \leftarrow \mathcal{A}_1()$
return x

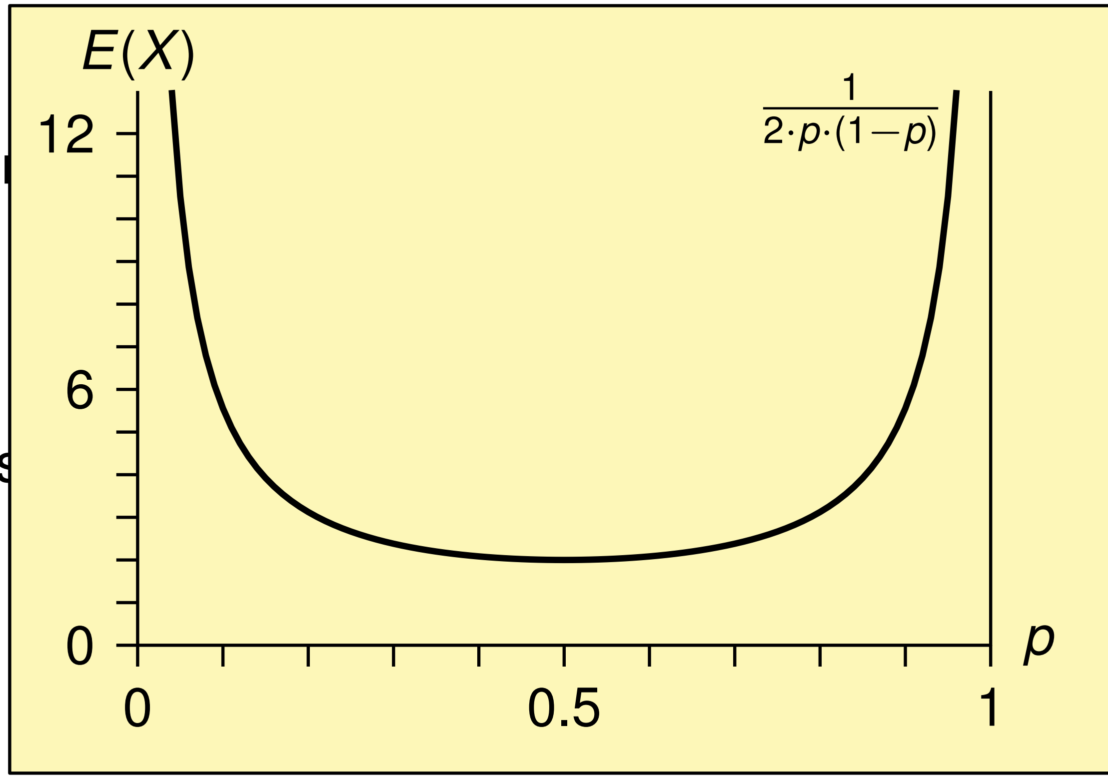
Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 2

Was ist die erwartete Laufzeit?

- Zufallsvariable X = Laufzeit = Anz. Schleifendurchläufe
- Ein Durchlauf: Bernoulli-Experiment mit Wahrscheinlichkeit
- Wahrschei
- Erwartungs

$E(X) =$

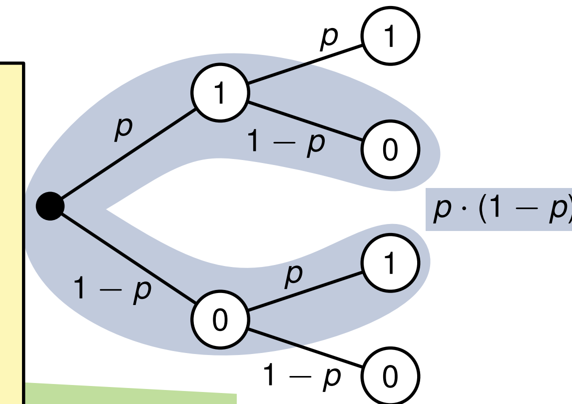


(Beweis: folgt gleich)

olgreichen

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

Entscheidungsbaum:
zweimaliges Anwenden von $\mathcal{A}_1$



$x \leftarrow 0$
$y \leftarrow 0$
while $x = y$ **do**
  $x \leftarrow \mathcal{A}_1()$
  $y \leftarrow \mathcal{A}_1()$
return x

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X=n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X=n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X=n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$ Wahrscheinlichkeit: q
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$ $(1-q)$

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X=n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$ Wahrscheinlichkeit: q
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$ $(1-q)$

$$\Rightarrow E(X) = q \cdot 1 + (1-q) \cdot (1 + E(X))$$

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X = n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$ Wahrscheinlichkeit: q
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$ $(1-q)$

$$\Rightarrow E(X) = q \cdot 1 + (1-q) \cdot (1 + E(X)) = q + (1-q) + (1-q) \cdot E(X)$$

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X=n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$ — Wahrscheinlichkeit: q
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$ — $(1-q)$

$$\Rightarrow E(X) = q \cdot 1 + (1-q) \cdot (1 + E(X)) = q + (1-q) + (1-q) \cdot E(X) = 1 + (1-q) \cdot E(X)$$

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X = n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$ Wahrscheinlichkeit: q
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$ $(1-q)$

$$\Rightarrow E(X) = q \cdot 1 + (1-q) \cdot (1 + E(X)) = q + (1-q) + (1-q) \cdot E(X) = 1 + (1-q) \cdot E(X)$$

$$E(X) = 1 + (1-q) \cdot E(X)$$

Problem 2

- Bernoulli-Experiment mit Erfolgswahrscheinlichkeit q
- Zufallsvariable X = Anz. Experimente bis zum ersten Erfolg.
- Erwartungswert:

$$E(X) = \sum_{n=1}^{\infty} \underbrace{(1-q)^{n-1} \cdot q}_{\Pr[X=n]} \cdot n = \frac{1}{q} \quad \textbf{zu zeigen}$$

Zwei Fälle:

- Das erste Experiment ist erfolgreich. $\Rightarrow X = 1$ Wahrscheinlichkeit: q
- Das erste Experiment ist nicht erfolgreich. $\Rightarrow X$ ist erwartet $1 + E(X)$ $(1-q)$

$$\Rightarrow E(X) = q \cdot 1 + (1-q) \cdot (1 + E(X)) = q + (1-q) + (1-q) \cdot E(X) = 1 + (1-q) \cdot E(X)$$

$$\begin{aligned} E(X) &= 1 + (1-q) \cdot E(X) \\ \Leftrightarrow E(X) &= 1 + E(X) - q \cdot E(X) \\ \Leftrightarrow q \cdot E(X) &= 1 \\ \Leftrightarrow E(X) &= \frac{1}{q} \end{aligned}$$

Fingerabdrücke

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 3 (a)

Ziel: Teste für Matritzen A, B und C ob $AB = C$ gilt.

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

(a) Zeige, dass die Rückgabe JA ist, wenn $AB = C$ gilt.

Problem 3 (a)

Ziel: Teste für Matritzen A, B und C ob $AB = C$ gilt.

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

(a) Zeige, dass die Rückgabe JA ist, wenn $AB = C$ gilt.

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

Matrixmultiplikation ist assoziativ

Problem 3 (b)

(b) Zeige, 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

Problem 3 (b)

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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$
Aber: $ABr = Cr$, also $Dr = 0$

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

Problem 3 (b)

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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$
Aber: $ABr = Cr$, also $Dr = 0$

- Sei d eine Zeile von D mit $d \neq 0$.
- Sei d_i in d ein Eintrag mit $d_i \neq 0$

$$\underset{d}{\begin{pmatrix} \dots & d_i & \dots \end{pmatrix}} \cdot \underset{r}{\begin{pmatrix} \vdots \\ r_i \\ \vdots \end{pmatrix}} = 0$$

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

Problem 3 (b)

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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$
Aber: $ABr = Cr$, also $Dr = 0$

- Sei d eine Zeile von D mit $d \neq 0$.
- Sei d_i in d ein Eintrag mit $d_i \neq 0$

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

$$\underbrace{(\ldots \quad d_i \quad \ldots)}_{d} \cdot \underbrace{\begin{pmatrix} \vdots \\ r_i \\ \vdots \end{pmatrix}}_{r} = 0$$

- Ändert man r_i von 0 auf 1 oder von 1 auf 0, dann ändert sich $d \cdot r$ um $|d_i|$.

Problem 3 (b)

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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$
Aber: $ABr = Cr$, also $Dr = 0$

- Sei d eine Zeile von D mit $d \neq 0$.
- Sei d_i in d ein Eintrag mit $d_i \neq 0$

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

$$\underbrace{(\dots \quad d_i \quad \dots)}_{d} \cdot \underbrace{\begin{pmatrix} \vdots \\ r_i \\ \vdots \end{pmatrix}}_{r} = 0$$

- Ändert man r_i von 0 auf 1 oder von 1 auf 0, dann ändert sich $d \cdot r$ um $|d_i|$.
- Einträge in r unabhängig gewählt $\Rightarrow$ man kann annehmen, dass r_i als letztes gewählt wurde.

Problem 3 (b)

(b) Zeige, 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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$
Aber: $ABr = Cr$, also $Dr = 0$

- Sei d eine Zeile von D mit $d \neq 0$.
- Sei d_i in d ein Eintrag mit $d_i \neq 0$

$$\underbrace{(\dots \quad d_i \quad \dots)}_{d} \cdot \underbrace{\begin{pmatrix} \vdots \\ r_i \\ \vdots \end{pmatrix}}_{r} = 0$$

- Ändert man r_i von 0 auf 1 oder von 1 auf 0, dann ändert sich $d \cdot r$ um $|d_i|$.
- Einträge in r unabhängig gewählt $\Rightarrow$ man kann annehmen, dass r_i als letztes gewählt wurde.

- r_i wird mit Wahrscheinlichkeit $\frac{1}{2}$ so gewählt, dass $d \cdot r \neq 0$

Problem 3 (b)

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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$
Aber: $ABr = Cr$, also $Dr = 0$

- Sei d eine Zeile von D mit $d \neq 0$.
- Sei d_i in d ein Eintrag mit $d_i \neq 0$

$$\underbrace{(\dots \quad d_i \quad \dots)}_{d} \cdot \underbrace{\begin{pmatrix} \vdots \\ r_i \\ \vdots \end{pmatrix}}_{r} = 0$$

- Ändert man r_i von 0 auf 1 oder von 1 auf 0, dann ändert sich $d \cdot r$ um $|d_i|$.
- Einträge in r unabhängig gewählt $\Rightarrow$ man kann annehmen, dass r_i als letztes gewählt wurde.

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

- r_i wird mit Wahrscheinlichkeit $\frac{1}{2}$ so gewählt, dass $d \cdot r \neq 0$
- $\Rightarrow$ Die Wahrscheinlichkeit dass $D \cdot r \neq 0$ ist mindestens $\frac{1}{2}$.

Institut für Theoretische Informatik
Prof. Dr. Dorothea Wagner

Problem 3 (b)

Karlsruher Institut für Technologie

(b) Zeige, 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

Annahme: $AB \neq C$, also $D := AB - C \neq 0$

Aber: $ABr = Cr$, also $Dr = 0$

- Sei d eine Zeile von D mit $d \neq 0$.
- Sei d_i in d ein Eintrag mit $d_i \neq 0$

$$\underbrace{(\dots \quad d_i \quad \dots)}_{d} \cdot \underbrace{\begin{pmatrix} \vdots \\ r_i \\ \vdots \end{pmatrix}}_{r} = 0$$

- Ändert man r_i von 0 auf 1 oder von 1 auf 0, dann ändert sich $d \cdot r$ um $|d_i|$.
- Einträge in r unabhängig gewählt $\Rightarrow$ man kann annehmen, dass r_i als letztes gewählt wurde.
- r_i wird mit Wahrscheinlichkeit $\frac{1}{2}$ so gewählt, dass $d \cdot r \neq 0$
- $\Rightarrow$ Die Wahrscheinlichkeit dass $D \cdot r \neq 0$ ist mindestens $\frac{1}{2}$.
- $\Rightarrow$ Die Wahrscheinlichkeit dass der Algorithmus JA liefter ist maximal $\frac{1}{2}$.

Problem 3 (c)

(c) Wie kann diese Wahrscheinlichkeit einer fälschlichen Ausgabe JA einfach reduziert werden?

Problem 3 (c)

(c) 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.