



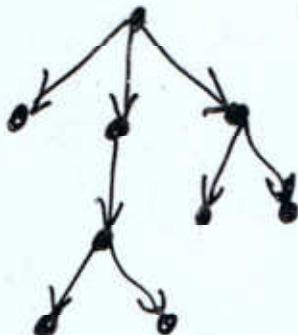
Starke Zusammenhangskomponente
von V : $\{v\}$

Schwache Zusammenhangskomp.:
Alle drei Knoten.

Baum:

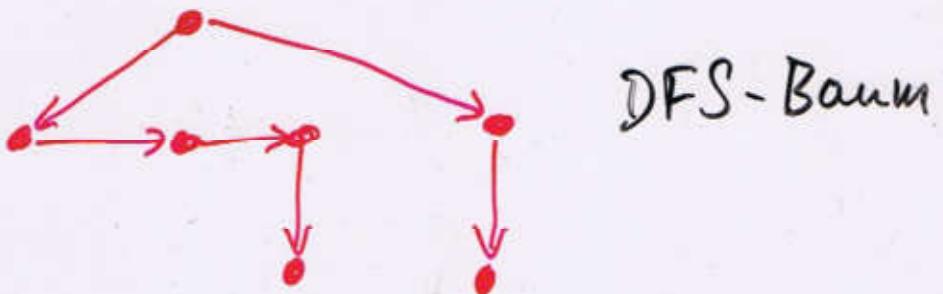
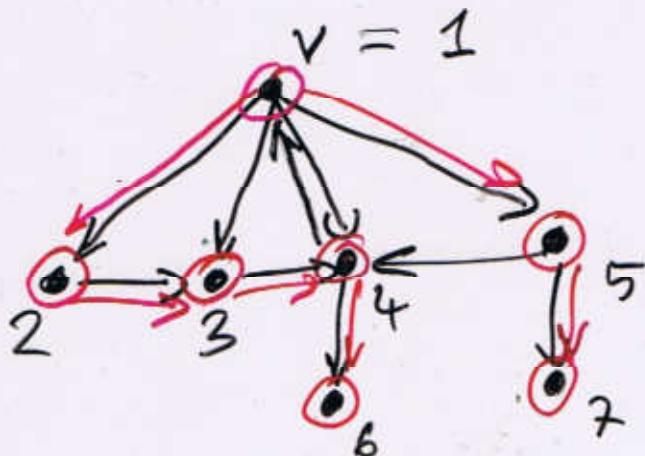


Geordneter Baum:



Beispiel Tiefensuche:

①



Stack: Eine Datenstruktur, bei der Daten oben hinzufüge und von oben wieder lese und entferne.

13
5
7

(lifo, last in, first out).

Stack bei dieser Tiefensuche:

1
1 2
1 2 3
1 2 3 4
1 2 3 4 6
1 2 3 4
1 2 3

1 2
1
1 5
1 5 7
1 5
1 ← Algorithma
Terminiert

(3)

Beweis von Satz 5.45:

Einfache Richtung: Sei B ein DFS-Baum mit Wurzel v .

Da B ein Teilgraph von G ist, ist jedes gerichtete Weg in B auch ein ger. Weg in G . In B gibt es für jedes $w \in V(B)$ einen ger. Weg von v nach w .

\Rightarrow auch in G ex. diese Weg.

Andere Richtung: Jeder von v aus in G erreichbare Knoten liegt in B .

Beweis durch Induktion über die Länge eines Weges von v zu diesem Knoten.

Ind.-Auf.: Sei $w \in V(G)$, der von v aus in 0 Schritten erreichbar ist.

$\rightarrow v = w \Rightarrow w \in V(B)$.

Ind. Schritt: Sei w in $n+1$ Schritten von v aus erreichbar, alle Knoten, die in n oder weniger Schritte erreichbar sind liegen in B .

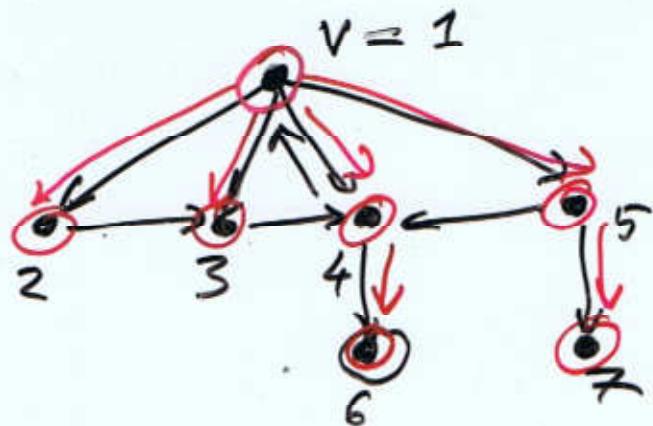
Sei v_0, \dots, v_{n+1} gerichteter Weg von ④
v nach w.
Dann ist v_n in n Schritten erreichbar.
 $\Rightarrow v_n \in B$.

Betrachte den Moment in dem als,
in dem v_n vom Stapel entfernt wurde.

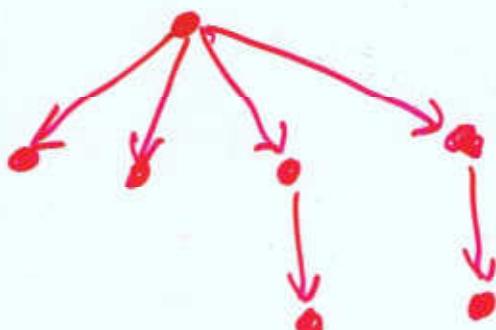
In diesem Schritt hatte v_n keinen
unmarkierten Nachbarn!

$\rightarrow v_{n+1}$ war markiert $\Rightarrow v_{n+1} \in V(B)$.

D



5



BFS-Baum.

Warteschlange: Datenstruktur, bei der man Daten hinten anfügt und vorne liest/entfernt.

(lifo: last in, last out).

Warteschlange im Beispiel oben:

1
1 2
1 2 3
1 2 3 4
1 2 3 4 5
2 3 4 5
3 4 5
4 5

4 5 6
5 6
5 6 7
6 7
7
—

Tue die markierten Knoten in die Warteschlange!

Entscheidender Schritt im Beweis ⑥
von Satz 5.46:

Induktions schritt: Sei $w \in V(G)$,
 v_0, \dots, v_{n+1} Weg von v nach w in G ,
alle in n Schritten erreichbaren
Knoten in B .

Nach I.A. ist $v_n \in V(B)$.

v_n wurde irgendwann aus der
Warteschlange entfernt.

In diesem Moment hatte v_n keinen
unmarkierten Nachbarn mehr.

$\Rightarrow v_{n+1}$ ist markiert $\Rightarrow v_{n+1} \in V(B) \quad \square$

Beispiel:

$$[2]_5 = \{\dots, -3, 2, 7, 12, \dots\}$$

$$[0]_5 = \{\dots, -5, 0, 5, 10, \dots\}.$$

$$[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$$

Beispiel: $[1]_5 \oplus [2]_5 = [1+2]_5$
 $= [3]_5.$

$$\rightarrow [3]_5 \oplus [4]_5 = [7]_5 = [2]_5$$

$$[3]_5 \odot [4]_5 = [3 \cdot 4]_5 = [12]_5$$

$$\rightarrow [8]_5 \oplus [-6]_5 = [8 + (-6)]_5 = [2]_5.$$

$$= [8 - 6]_5 = [2]_5$$

2. Bonushlausur findet am
16.1.2015 hier statt.

[5] 27

5 ist der Vertreter/
Repräsentant.

Das Produkt $[a]_m \odot [b]_m$ ist auch wohldefiniert.

Seien $a \equiv c \pmod{m}$ und $b \equiv d \pmod{m}$
(d.h. $[a]_m = [c]_m$ und $[b]_m = [d]_m$).

Dann gilt $a \cdot b \equiv c \cdot d \pmod{m}$
(also $[a \cdot b]_m = [c \cdot d]_m$.)

Es gibt $q_a, q_c, q_b, q_d \in \mathbb{Z}$ und

$r_1, r_2 \in \mathbb{Z}$ mit $0 \leq r_1, r_2 < m$

und $a = q_a \cdot m + r_1, b = q_b \cdot m + r_2$
 $c = q_c \cdot m + r_1, d = q_d \cdot m + r_2$

$$a \cdot b = (q_a \cdot m + r_1) \cdot (q_b \cdot m + r_2)$$

$$= q_a \cdot q_b \cdot m^2 + r_1 \cdot q_b \cdot m + r_2 \cdot q_a \cdot m + r_1 \cdot r_2$$

$$\text{D.h. } a \cdot b \equiv r_1 \cdot r_2 \pmod{m}$$

$$\text{Analog: } c \cdot d \equiv r_1 \cdot r_2 \pmod{m}$$

$$\Rightarrow a \cdot b \equiv c \cdot d \pmod{m}$$

②

Beweis Satz 6.4:

$$1. [a]_m \oplus [b]_m = [a+b]_m$$

$$= [b+a]_m = [b]_m \oplus [a]_m.$$

$$2. ([a]_m \odot [b]_m) \odot [c]_m = [a \cdot b]_m \odot [c]_m$$

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

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

$$3. [a]_m \oplus [0]_m = [a+0]_m = [a]_m.$$

$$4. [a]_m \odot ([b]_m \oplus [c]_m) = [a \cdot (b+c)]_m$$

$$= [a \cdot b + a \cdot c]_m = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m).$$

\mathbb{Z}_m ist ein kommutativer Ring mit 1.

\mathbb{Z}_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Additionstabelle

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Multiplikationstabelle.

(3)

Beweis von Satz 6.7

Angenommen, $[b]_m, [c]_m$ sind
beide invers zu $[a]_m$.

$$\begin{aligned}[b]_m &= [b]_m \cdot [1]_m = [b]_m \cdot ([a]_m \cdot [c]_m) \\ &= ([b]_m \cdot [a]_m) \cdot [c]_m = [1]_m \cdot [c]_m \\ &= [c]_m \quad \square\end{aligned}$$

Beispiel: \mathbb{Z}_2 ist ein Körper

+	0	1
0	0	1
1	1	0

(xor)

·	0	1
0	0	0
1	0	1

(und)

Beweis von S. 6.8

(4)

Sei $[a]_m$ invertierbar. Dann ex $[b]_m \in \mathbb{Z}_m$ mit $[a]_m \cdot [b]_m = [1]_m$.

$$a \cdot b \equiv 1 \pmod{m}$$

Dann ex. $q \in \mathbb{Z}$ mit $a \cdot b = q \cdot m + 1$.

Angenommen, $c \mid a \cdot b, m$.

Dann gilt $c \mid 1$, da $1 = a \cdot b - q \cdot m$

$$\Rightarrow c = \pm 1. \Rightarrow \text{ggT}(a, m) = 1.$$

$\Rightarrow a$ und m sind teilerfremd.

Seien a und m teilerfremd.

Betrachte die Restklassen

$$[0 \cdot a]_m, [1 \cdot a]_m, \dots, [(m-1) \cdot a]_m.$$

Beh: Diese Restklassen sind pw. versch.

Angenommen $0 \leq r, s < m$ und

$$[r \cdot a]_m = [s \cdot a]_m.$$

$$\Rightarrow r \cdot a \equiv s \cdot a \pmod{m}.$$

$$\Rightarrow m \mid ra - sa = (r-s) \cdot a.$$

$\Rightarrow m \mid r-s$, da a, m teilerfremd.

$$\Rightarrow r \equiv s \pmod{m} \Rightarrow [r]_m = [s]_m.$$

$$\Rightarrow r = s.$$

Haben eigentlich gezeigt: Sind
a und m teilerfremd,

(5)

so kann man $[a]_m \cdot [r]_m = [a]_m \cdot [s]_m$
durch $[a]_m$ kürzen und erhält

$$\underline{[r]_m = [s]_m}$$

$$\Rightarrow \{[0]_m, \dots, [m-1]_m\} = \{[0 \cdot a]_m, \dots, [(m-1) \cdot a]_m\}$$

$$\Rightarrow \{[1]_m, \dots, [m-1]_m\} = \{[1 \cdot a]_m, \dots, [(m-1) \cdot a]_m\}$$

\rightarrow es gibt $r \in \{1, \dots, m-1\}$ mit

$$[1]_m = [r \cdot a]_m.$$

$$[r]_m \cdot [a]_m = [r \cdot a]_m = [1]_m$$

$\Rightarrow [a]_m$ ist invertierbar. \square

Beispiel: $a = 8, b = 12$ ⑥

$$d = \text{ggT}(8, 12) = 4$$

$$4 = (-1)a + 1 \cdot 12$$

$$\lambda = -1, \mu = 1.$$

$$a = 5, b = 7$$

$$d = \text{ggT}(5, 7) = 1$$

$$d = 3 \cdot 5 - 2 \cdot 7$$

$$\lambda = 3, \mu = -2.$$

$$\text{Sei } a = 5, m = 7.$$

Wollen $[5]_7$ invertieren.

$$1 = 3 \cdot 5 - 2 \cdot 7$$

$$\Rightarrow 1 \equiv 3 \cdot 5 \pmod{7}$$

$$\Rightarrow [3]_7 \cdot [5]_7 = [1]_7$$

Also: Sind a und m teilerfremd,
so ist $\text{ggT}(a, m) = 1$. Damit

ex. $\lambda, \mu \in \mathbb{Z}$ mit $\lambda a + \mu \cdot m = 1$.

Damit ist $\lambda a \equiv 1 \pmod{m}$

$\rightarrow [\lambda]_m$ ist das Inverse von $[a]_m$.

Beweis von Satz 6.10

(7)

Nehmen $a \leq b$.

Beweis durch Induktion über
die Laufzeit des euklidischen Alg.
zur Berechnung von $\text{ggT}(a, b)$.

Ind. Anf.: Terminiert nach einem Schritt,
d.h. $b \bmod a = 0$.

$\Rightarrow a | b$. Setze $\lambda = 1, \mu = 0$.

$$\text{ggT}(a, b) = a = \lambda \cdot a + \mu \cdot b.$$

Ind. schritt: Sei $n \in \mathbb{N}$.

Der euklidische Alg. mit den
Werten a und b terminiere nach
 $n+1$ Schritten.

Annahme: kann man $\text{ggT}(a', b')$
in höchstens n Schritten ber.,
so ex. λ', μ' mit $\text{ggT}(a', b') = \lambda' a' + \mu' b'$.

Wir führen den ersten Schritt
des eukl. Alg. für a und b durch. ⑧

$$b = q \cdot a + r.$$

$$d = \text{ggT}(a, b) = \text{ggT}(r, a)$$

Die Rechenzeit für $\text{ggT}(r, a)$
ist höchstens n .

D.h. ex. $\lambda', \mu' \in \mathbb{Z}$ mit

$$d = \text{ggT}(r, a) = \lambda' r + \mu' a$$

$$r = b - q \cdot a$$

$$d = \lambda'(b - q \cdot a) + \mu' a$$

$$= \lambda' \cdot b + (\mu' - \lambda' q) \cdot a$$

Setze also $\lambda := (\mu' - \lambda' q)$

und $\mu := \lambda' b$

Dann ist $d = \lambda a + \mu b$ \square

(9)

Beispiel 6.11:

$$a = 228 \text{ und } b = 294.$$

$$294 = 1 \cdot 228 + 66$$

$$228 = 3 \cdot 66 + 30$$

$$66 = 2 \cdot 30 + 6$$

$$30 = 5 \cdot 6 + 0$$

$$\Rightarrow d = \text{ggT}(228, 294) = 6$$

Vorletzte Gleichung:

$$6 = 66 - 2 \cdot 30$$

$$30 = 228 - 3 \cdot 66$$

$$\begin{aligned} \Rightarrow 6 &= 66 - 2 \cdot (228 - 3 \cdot 66) \\ &= 7 \cdot 66 - 2 \cdot 228. \end{aligned}$$

$$66 = 294 - 1 \cdot 228$$

$$6 = 7(294 - 1 \cdot 228) - 2 \cdot 228$$

$$6 = 7 \cdot 294 - 9 \cdot 228$$

$$\lambda = -9, \mu = 7.$$

$$6 = \lambda \cdot a + \mu \cdot b.$$