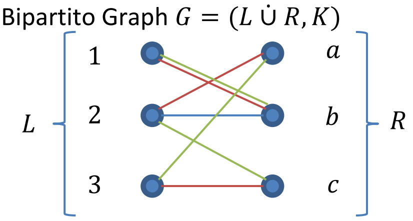
THEORETISCHE INFORMATIK - PROBLEME

P-Probleme

Matrizen-addition & -multiplikation	Gegeben: $A, B \in M(n\ x\ n)$ $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ Gesucht: $\#Mult\ von\ A\ und\ B = m(A * B)$	$n = 2$ Matrizen-Addition $A + B$: $= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$ $\#Add = n^2 = 4$ Matrizen-Multiplikation Gauss-Lösung $A * B$: $= \begin{pmatrix} a_{11} * b_{11} + a_{12} * b_{21} & \dots \\ \dots & \dots \end{pmatrix}$ $\#Mult \leq n^3 = 8$ V.Strassen / Winograd: $\#Mult \leq n^{\log_2 7} \approx n^{2.807}$
AK: Additionsketten	Gegeben: Steigende Folge von Zahlen $a_0, \dots, a_r \in \mathbb{N}^*$ 1. $a_0 = 1$ 2. $a_k = a_i + a_j, mit\ i > 0, j < k$ 3. $a_r = n$ Gesucht: Minimaler Berechnungsaufwand $l(n)$ Bsp: $n = 4$ $a_0 = 1$, $a_1 = 2$, $a_2 = 3$: $a_3 = 4, 5, 6$; $a_2 = 4$: $a_3 = 5, 6, 8$ $l(4)$ $\rightarrow l(n) \leq n - 1$ $\rightarrow l(2n) \leq l(n) + 1$	$n = 9$ Binärer: $\frac{9+1}{2} = \mathbf{5} = \mathbf{4} + 1;\ \frac{4}{2} = \mathbf{2};\ \frac{2}{2} = \mathbf{1}$ Brauer: $n = a_p t^p + a_{p-1} t^{p-1} + \dots + a_1 t + a_0$ mit $0 \leq a_i < t$ (t-adische Darstellung) 1. $t = 2^\lambda \rightarrow p * \lambda \leq \log_2 n$ 2. $a_0, \dots, a_p \in \Sigma(0 \dots t-1)$ 3. Horner-Schema: $n = \left(\left(\underbrace{a_p t}_{\lambda} + \underbrace{a_{p-1}}_{1} \right) \underbrace{t}_{\lambda} + \dots + a_1 \right) t + a_0$ $l(n) \leq \log_2 n + \frac{\log_2 n}{\log_2 \log_2 n} + o \frac{\log_2 n}{(\log_2 \log_2 n)^2}$ o geht gegen 0 wenn n gross dann ist er besser als der binäre Alg
Determinante	Gegeben: $A \in M(n\ x\ n)$ $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ Gesucht: $\#Summanden\ für\ V = \lvert\det A\rvert$	3x3: $V = \lvert aei + bfg + cdh - ceg - afh - bdi \rvert$ $\#Summanden = 6$ nxn: $\det A = \sum_{\sigma \in S_n} \left(sign(\sigma) \prod_{i=1}^{n} a_{1,\sigma(i)} \right)$ $\#Summanden = \lvert S_n \rvert = n!\ (Fakultät)$ Gauss: $A = \begin{pmatrix} a_{11} & * \\ 0 & a_{nn} \end{pmatrix} \rightarrow \det(A) = \prod_{i=1}^{n} a_{ii}$
Permanente / Bipartito Graph	Gegeben: Bipartito Graph $G = (L \dot\cup R, K)$  $L \cap R = \emptyset, \quad \lvert L \rvert = \lvert R \rvert$ Gesucht: Maximum Matching enthält die max. mögliche Anzahl von Kanten. Keine adjazente Kanten in M. adjazent = 2 Kanten vom gleichen Knoten	nxn: $perm(A) := \sum_{\sigma \in S_n} \left(\prod_{i=1}^{n} a_{i,\sigma(i)} \right)$ Ryter #perfekt Matching: $A_G = \begin{array}{c c} & \begin{array}{ccc} a & b & c \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{pmatrix} 0 & 1/1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \end{array} => perm(A_G) = 2$ $\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rightarrow$ perfektes Matching $\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \rightarrow$ kein perfektes Matching
2SAT-Problem		$2SAT \in P$
Euler Pfad	Weg durch jede Kante	

NP-Probleme

SAT-Problem	$\phi \in KNF\ (konjunktiver\ Normalform)$ $k_1 \wedge k_2 \wedge k_3$	$SAT \in NPC$ $kSAT \in NP$
3SAT-Problem	Jede Klausel hat 3 Literale z.B: Datenbankquery, Digitaltechnik	$3SAT \in NPC$ $3SAT \subset kSAT$

Subset-Sum (SSS)

Gegeben:

$a_1, \dots, a_n, t \in \mathbb{N}^*$

Gesucht:

$(x_1, \dots, x_n) \in \{0,1\}^n : \sum_{i=1}^{n} x_i a_i = t$

$a_1 = 1, a_2 = 4, a_3 = 10, a_4 = 13, a_5 = 28, a_6 = 29, a_7 = 53, t = 99$

Lösung: $\bar{x} = (0,1,0,1,0,1,1)$

Codierung: als EP über $\Sigma = \{0,1,\#\}, x =$

$\underbrace{1}_{1}\#\underbrace{100}_{4}\#\underbrace{1010}_{10}\#\dots\#\underbrace{110011}_{t}$

$u = 010101100$

Merkle-Hellmann-Kryptosystem based on SSS

	Secret-Key	Public-Key	Encrypt
	$a_1, \dots, a_n \in \mathbb{N}^* (super\ increasing)$ $m \in \mathbb{N}^*\ mit \sum_{i=1}^{n} a_i < m$ $w \in \mathbb{Z}_m^*\ (any\ smaller\ m)$	$b_1, \dots, b_n \in \mathbb{N}^*$ $b_i \equiv wa_i\ mod\ m$	$P := \{0,1\}^n \to C := \mathbb{N}^*$ $(x_1, \dots x_n) \to c := \sum_{i=1}^{n} x_i b_i$ Decrypt (with modular inverse) $T \equiv w^{-1} c\ mod\ m$
e.g.	$3, 7, 11, 23, 45, 90, 200, 423, 901$ $m = 2011$ $w = 99$	$297, 693, 1089, 266, 433, 866, 1701, 1657, 715$	$x = (0,0,1,0,0,1,0,0,1)$ $send\ c = 2670$ $\to w^{-1} = 1686$ $T = 1002 \to SSS \to x$

CYK-Algorithm Cocke-Younger-Kasami

$is\ \omega(e.g.\ aab)\ in\ CFG?$

needs to be in Chomsky Normalform

$S \to AB|BC$

$A \to BA|a$

$B \to CC|b$

$C \to AB|a$

bottom-up

3	$aab =$ $a \cup ab = AS, AC, CS, CC = \boldsymbol{B}$ $\mid aa \cup b) = BB = \emptyset$		
2	$aa = AA, AC, CA, CC = B$	$ab = AB, CB$ $= S, C$	
1	$a = A, C$	$a = A, C$	$b = B$
	a	a	b

Graph Colouring k-GC

Bsp: Ampelproblem

Gegeben: $G = (V, E)$

Gesucht: Färbung mit F als Farben (GC=Graph Colouring)

Def: Färbung von G mit den Farben F

$\Leftrightarrow f: V \to F$

$v \to f(v)$

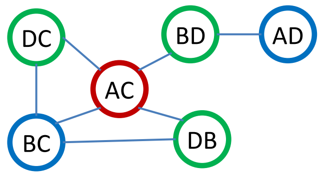
mit $\forall k\{v, u\} \in E: f(v) \neq f(u)$ (keine gleichen Nachbarn)

Praktisch: Stundenplan erstellen

Lektionen = k, Fächer = Kreise, Linien sind Doppelte Belgungen der Stundenten.

EP (k-GC), Gegeben: $G = (V, E), k \in \mathbb{N}^*$

Frage: Können wir G mit k Farben färben.



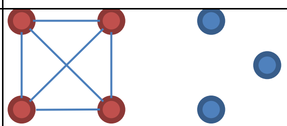
$Ampel \le_T (GC)\ mit\ p(n) = O(n^2)$

$q(n) = 1, \quad r(n) = O(n^2)$

Clique

Gesucht:

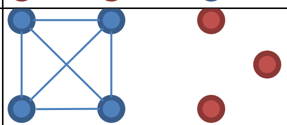
Maximale Clique: Eine Teilmenge C, bei dem jeder Knoten von C mit jedem anderen Knoten von C verbunden ist.



IS: Independent Set

Gesucht:

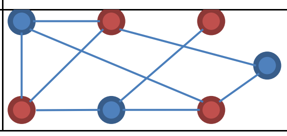
Maximale Anticlique: Eine Teilmenge AC, bei dem kein Knoten von AC mit einem anderen Knoten von AC verbunden ist.



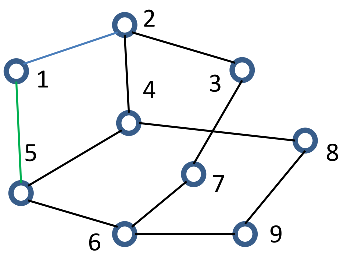
VC: Vertex Cover

Gesucht: Minimale Knotenüberdeckung:

Jede Kante hat ein Ende, welches in VC liegt.



e.g. Überwachung der Verkehrsaches einer Stadt



Gegeben: $G = (V, E)\ Graph, Vertex, Edges$

Gesucht $VC \subset V\ minimal$

$\forall e = \{x, y\} \in E: \exists v \in VC: v = x\ oder\ v = y$

Codierung von VC: Adjazendzmatrix von G

$$A_G = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Graphen als ein Wort über $\Sigma = \{0,1\},\ G \to \omega(G) \subset \Sigma^*$

$\omega(G): \quad \underbrace{C(1)}_{10110101011} \quad 00 \quad \underbrace{C(2)}_{110101101101} \quad 00 \dots$

$\underbrace{|\omega(G)|}_{Inputlänge} \le (3|V| + 1)|V| = O(|V|^2)$

Trivialer Alg. Ausprobieren aller $A \subset V, |P(V)| = 2^{|V|}$

Hamilton Pfad

Weg durch jeden Knoten

Rucksackproblem Knapsack

Gegeben:

$a_1, \dots, a_n, t$

$\boldsymbol{g_1, \dots, g_n}$

Gesucht:

$x_1, \dots, x_n \in \{0,1\}\ mit \sum_{i=1}^{n} x_i a_i \le t$	$c = \sum_{i=1}^{n} x_i g_i\ maximal$	$c = f_\pi(x, s), s \in S(x)$