

Zum Konsistenzproblem (3):

- ▶ Die gesuchte Transformation $KS \mapsto KS'$ ist einfach, wenn man die Primfaktorisierung der Moduln kennt.
- ▶ Man kann immer eine "Quasi-Faktorisierung" der Moduln $\{m_1, m_2, \dots, m_k\}$ *effizient konstruieren*:
 - ▶ Zu $\mathcal{M} = \{m_1, m_2, \dots, m_k\} \subset \mathbb{N}_{\geq 2}$ kann man $\mathcal{P} = \{\pi_1, \pi_2, \dots, \pi_\ell\} \subset \mathbb{N}_{\geq 2}$ konstruieren mit:
 - die $\pi_j \in \mathcal{P}$ sind paarweise teilerfremd;
 - jedes $m_i \in \mathcal{M}$ hat eine eindeutige Darstellung

$$(*) \quad m_i = \pi_1^{\alpha_1} \pi_2^{\alpha_2} \dots \pi_\ell^{\alpha_\ell}$$

mit $\alpha_j \in \mathbb{N}$.

- ▶ Die Elemente von \mathcal{P} müssen keine Primzahlen sein!
- ▶ Sowohl die Konstruktion von \mathcal{P} aus auch die Konstruktion der Darstellungen (*) ist effizient!

Zum Konsistenzproblem (4):

- ▶ Zwei nützliche Funktionen:
 - ▶ Für $(m, n) \in \mathbb{N} \times \mathbb{N}$ sei

$$\text{split1}(m, n) = (u, v) \text{ mit } \begin{cases} m = u \cdot v \\ \text{ggT}(u, n) = 1 \\ p \mid v \Rightarrow p \mid n \quad (\forall p \text{ Primzahl}) \end{cases}$$

split1 ist durch diese Forderungen eindeutig definiert!

- ▶ Für $(m, n) \in \mathbb{N} \times \mathbb{N}$ sei

$$\text{split2}(m, n) = (u, v) \text{ mit } \begin{cases} u \mid m \\ v \mid n \\ \text{ggT}(u, v) = 1 \\ u \cdot v = \text{kgV}(m, n) \end{cases}$$

split2 ist durch diese Forderungen noch nicht eindeutig definiert! Es wird eindeutig, wenn man noch verlangt, dass u maximal und v minimal mit diesen Eigenschaften sind.

Zum Konsistenzproblem (5):

- ▶ split1 und split2 lassen sich in Bezug auf die Primfaktorierungen

$$m = \prod_{p \text{ prim}} p^{\alpha_p}, \quad n = \prod_{p \text{ prim}} p^{\beta_p}$$

einfach beschreiben:

- ▶ Ist $\text{split1}(m, n) = (u, v)$, so gilt

$$u = \prod_{\substack{p \text{ prim} \\ p \nmid n}} p^{\alpha_p}, \quad v = \prod_{\substack{p \text{ prim} \\ p \mid n}} p^{\alpha_p}.$$

- ▶ Ist $\text{split2}(m, n) = (u, v)$, so gilt

$$u = \prod_{\substack{p \text{ prim} \\ \beta_p \leq \alpha_p}} p^{\alpha_p}, \quad v = \prod_{\substack{p \text{ prim} \\ \beta_p > \alpha_p}} p^{\beta_p}.$$

Zum Konsistenzproblem (6):

- ▶ Beispiele:

$$\begin{array}{ll} \text{split1}(15, 28) = (15, 1) & \text{split2}(15, 28) = (15, 28) \\ \text{split1}(45, 75) = (1, 45) & \text{split2}(45, 75) = (9, 25) \\ \text{split1}(36, 14) = (9, 4) & \text{split2}(36, 14) = (36, 7) \end{array}$$

- ▶ Wichtig: $\text{split1}(m, n)$ und $\text{split2}(m, n)$ lassen sich effizient berechnen, also ohne Rückgriff auf die Primfaktorierungen der Argumente, nur mit ggT und Division!
- ▶ Ein konsistentes Kongruenzsystem

$$x \equiv a \pmod{m}, x \equiv b \pmod{n}$$

mit $\text{split2}(m, n) = (u, v)$ ist äquivalent zu

$$x \equiv a \pmod{u}, x \equiv b \pmod{v}.$$

- ▶ Die allgemeine Aussage von (2) lässt sich mit Hilfe von (3) analog zum Fall $k = 2$ behandeln.

Zum Überdeckungsproblem (1):

- ▶ Aus dem Chinesischen Restesatz ergibt sich

$$KS \text{ überdeckt } \mathbb{Z} \iff \bigcup_{1 \leq i \leq k} \langle c_i, m_i \rangle = \mathbb{Z}$$

$$\iff \bigcap_{1 \leq i \leq k} \langle c_i, m_i \rangle \supseteq [0, M)$$

- ▶ Dieses Problem ist co-NP-vollständig!
Es ist unter dem Namen SIMULTANEUOS INCONGRUENCES (SI) bekannt (STOCKMEYER, MEYER 1973; GAREY, JOHNSON 1979).

Zum Überdeckungsproblem (2):

- ▶ p_1, p_2, \dots, p_n : die ersten n Primzahlen
($p_1 = 2, p_2 = 3, p_3 = 5, \dots$),
 $P_n = p_1 p_2 \cdots p_n$.
- ▶ Zu $\mathbf{e} = (e_1, e_2, \dots, e_n) \in \mathbb{B}^n$ sei $x^{\mathbf{e}}$ die eindeutig bestimmte Lösung des Kongruenzsystems

$$\begin{cases} x \equiv e_1 \pmod{p_1} \\ x \equiv e_2 \pmod{p_2} \\ \vdots \\ x \equiv e_n \pmod{p_n} \end{cases}$$

mit $0 \leq x < P_n$.

Zum Überdeckungsproblem (2):

- ▶ Ziel: Reduktion 3-SAT \rightarrow SI
 - ▶ $Y_n = \{y_1, y_2, \dots, y_n\}$: boolesche Variable
 - ▶ $Y \cup \bar{Y} = \{y_1, y_2, \dots, y_n\} \cup \{\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n\}$: Literale
 - ▶ 3-Klauseln: Disjunktionen von 3 Literalen

$$C = \lambda_a \vee \lambda_b \vee \lambda_c,$$

wobei $1 \leq a < b < c \leq n$ mit $\lambda_i \in \{y_i, \bar{y}_i\}$ ($1 \leq i \leq n$).

- ▶ AL-Formeln in 3-CNF: Konjunktionen von 3-Klauseln:

$$F = C_1 \wedge C_2 \wedge \dots \wedge C_m$$

wobei $C_j = \lambda_a^j \vee \lambda_b^j \vee \lambda_c^j$, ($1 \leq j \leq m$).

- ▶ 3-SAT : Erfüllbarkeit von AL-Formeln F in CNF mit 3 Literalen pro Klausel
- ▶ Theorem von COOK: 3-SAT ist ein NP-vollständiges Problem.

Zum Überdeckungsproblem (3):

- ▶ Eine Zahl x mit $0 \leq x < P_n$ ist numerische Codierung einer Bewertung, d.h. $x = x^{\mathbf{e}}$ für ein $\mathbf{e} \in \mathbb{B}^n$, genau dann, wenn

$$(S_n) \begin{cases} x \not\equiv 2 \pmod{3} \\ x \not\equiv 2, 3, 4 \pmod{5} \\ \vdots \\ x \not\equiv 2, 3, \dots, p_n - 1 \pmod{p_n} \end{cases}$$

- ▶ Beispiel $n = 3$:

\mathbf{e}	000	100	010	001	110	101	011	111
$x^{\mathbf{e}}$	0	15	10	6	25	21	16	1

Zum Überdeckungsproblem (4):

- Für jedes $1 \leq i \leq n$ sei

$$[y_i] : x \equiv 0 \pmod{p_i}, \quad [\bar{y}_i] : x \equiv 1 \pmod{p_i}$$

- Zu jeder Klausel $C = \lambda_a \vee \lambda_b \vee \lambda_c$ sei $x^C \in [0 \dots p_a p_b p_c)$ die eindeutig bestimmte simultane Lösung von

$$[\lambda_a], [\lambda_b], [\lambda_c]$$

- Für alle $e \in \mathbb{B}^n$ und alle Klauseln C_j gilt:

$$e \models C_j = \lambda_a^j \vee \lambda_b^j \vee \lambda_c^j \iff x^e \not\equiv x^{C_j} \pmod{p_a^j p_b^j p_c^j}$$

- Beispiel:

$$C = y_1 \vee \bar{y}_2 \vee \bar{y}_3 \iff x^C \equiv \begin{cases} 0 \pmod{2} \\ 1 \pmod{3} \\ 1 \pmod{5} \end{cases} \iff x^C = 16$$

Zum Überdeckungsproblem (5):

- Für alle $e \in \mathbb{B}^n$ und alle Formeln $F = C_1 \wedge \dots \wedge C_m$ gilt:

$$e \models F \iff (T_F) \begin{cases} x^e \not\equiv x^{C_1} \pmod{p_a^1 p_b^1 p_c^1} \\ \vdots \\ x^e \not\equiv x^{C_m} \pmod{p_a^m p_b^m p_c^m} \end{cases}$$

- Für alle Formeln $F = C_1 \wedge \dots \wedge C_m$ gilt:

$$F \text{ ist erfüllbar} \iff \exists e \in \mathbb{B}^n : x^e \models (T_F)$$

$$\iff \exists_{0 \leq x < P_n} : x \models (S_n) \text{ und } (T_F)$$

- Bekannte Aussagen über die Grösse von p_n und Effizienz der Lösbarkeit von Kongruenzsystemen (Konstruktion der x^{C_i}) zeigen, dass dies eine polynomielle Reduktion ist.

Zum Überdeckungsproblem (6):

Beispiel einer erfüllbaren Formel $F = C_1 \wedge C_2 \wedge \dots \wedge C_8$:

- $C_1 : \bar{y}_1 \vee \bar{y}_2 \vee \bar{y}_3 \iff x^{C_1} \equiv 1 \pmod{30}$
- $C_2 : \bar{y}_1 \vee \bar{y}_2 \vee y_3 \iff x^{C_2} \equiv 25 \pmod{30}$
- $C_3 : y_1 \vee \bar{y}_2 \vee y_4 \iff x^{C_3} \equiv 28 \pmod{42}$
- $C_4 : \bar{y}_1 \vee y_2 \vee \bar{y}_4 \iff x^{C_4} \equiv 15 \pmod{42}$
- $C_5 : \bar{y}_1 \vee \bar{y}_2 \vee \bar{y}_4 \iff x^{C_5} \equiv 1 \pmod{42}$
- $C_6 : y_1 \vee y_3 \vee \bar{y}_4 \iff x^{C_6} \equiv 50 \pmod{70}$
- $C_7 : y_1 \vee \bar{y}_3 \vee \bar{y}_4 \iff x^{C_7} \equiv 36 \pmod{70}$
- $C_8 : y_2 \vee y_3 \vee y_4 \iff x^{C_8} \equiv 0 \pmod{105}$

Bewertungen als Zahlen mod 210:

e	0000	1000	0100	1100	0010	1010	0110	1110
x^e	0	105	70	175	126	21	196	91
e	0001	1001	0101	1101	0011	1011	0111	1111
x^e	120	15	190	85	36	141	106	1

$(y_1, y_2, y_3, y_4) = 1010$ erfüllt F : 21 ist $\neq 1, 25 \pmod{30}, \neq 1, 15, 28 \pmod{42}, \neq 50, 36 \pmod{70}, \neq 0 \pmod{105}$

Zum Überdeckungsproblem (7):

Beispiel einer unerfüllbaren Formel $F = C_1 \wedge C_2 \wedge \dots \wedge C_8$:

- $C_1 : \bar{y}_1 \vee \bar{y}_2 \vee \bar{y}_3 \iff x^{C_1} \equiv 1 \pmod{30}$
- $C_2 : \bar{y}_1 \vee \bar{y}_2 \vee y_3 \iff x^{C_2} \equiv 25 \pmod{30}$
- $C_3 : y_1 \vee \bar{y}_2 \vee y_4 \iff x^{C_3} \equiv 28 \pmod{42}$
- $C_4 : \bar{y}_1 \vee y_2 \vee \bar{y}_4 \iff x^{C_4} \equiv 15 \pmod{42}$
- $C_5 : y_1 \vee y_3 \vee \bar{y}_4 \iff x^{C_5} \equiv 50 \pmod{70}$
- $C_6 : y_1 \vee \bar{y}_3 \vee \bar{y}_4 \iff x^{C_6} \equiv 36 \pmod{70}$
- $C_7 : y_2 \vee y_3 \vee y_4 \iff x^{C_7} \equiv 0 \pmod{105}$
- $C_8 : y_2 \vee \bar{y}_3 \vee y_4 \iff x^{C_8} \equiv 21 \pmod{105}$

- $0000 \not\models C_7 \iff 0 \equiv 0 \pmod{105}$
- $1000 \not\models C_7 \iff 105 \equiv 0 \pmod{105}$
- $0100 \not\models C_3 \iff 70 \equiv 28 \pmod{42}$
- $1100 \not\models C_2 \iff 175 \equiv 25 \pmod{30}$
- $0010 \not\models C_8 \iff 126 \equiv 21 \pmod{105}$
- $1010 \not\models C_8 \iff 21 \equiv 21 \pmod{105}$
- $0110 \not\models C_3 \iff 196 \equiv 28 \pmod{42}$
- $1110 \not\models C_1 \iff 91 \equiv 1 \pmod{30}$
- $0001 \not\models C_5 \iff 120 \equiv 50 \pmod{70}$
- $1001 \not\models C_4 \iff 15 \equiv 15 \pmod{42}$
- $0101 \not\models C_5 \iff 190 \equiv 50 \pmod{70}$
- $1101 \not\models C_2 \iff 85 \equiv 25 \pmod{30}$
- $0011 \not\models C_6 \iff 36 \equiv 36 \pmod{70}$
- $1011 \not\models C_4 \iff 141 \equiv 15 \pmod{42}$
- $0111 \not\models C_6 \iff 106 \equiv 36 \pmod{70}$
- $1111 \not\models C_1 \iff 1 \equiv 1 \pmod{30}$