Algorithms and Complexity (AC)

Proof of the Cook-Levin Theorem (extra materials)

Paul Bouman & Tom van der Zanden (Based on slides by Gerhard Woeginger, Jesper Nederlof and Marie Schmidt)

September – November 2023

LNMB – Landelijk Netwerk Mathematische Besliskunde

Cook-Levin theorem

Cook-Levin theorem (1971)

SAT is NP-complete.

- Stephen Cook (born 1939):

American-Canadian computer scientist and mathematician

- Leonid Levin (born 1948):

Russian computer scientist, discovered the result somewhat earlier

Complexity classes P and NP

Definition: Complexity class NP

A decision problem *X* lies in the complexity class NP, if

- if it can be **solved** in polynomial time on a non-deterministic Turing machine (original, formal definition)
- (or, alternatively:) if it is solved by a *non-deterministic* algorithm with polynomial time complexity.
- (or, alternatively:) if the YES-instances of *X* possess certificates of polynomial length that can be verified in polynomial time.

Complexity classes P and NP

Definition: Complexity class NP

A decision problem X lies in the complexity class NP, if

- if it can be **solved** in polynomial time on a non-deterministic Turing machine (original, formal definition)
- (or, alternatively:) if it is solved by a *non-deterministic* algorithm with polynomial time complexity.
- (or, alternatively:) if the YES-instances of X possess certificates of polynomial length that can be verified in polynomial time.

Remark: **solved** means that YES-instances are 'checked' in polynomial time

Proof of Cook-Levin

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

Proof of Cook-Levin

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

clause group	restriction imposed
G_1	at each time i, M is in exactly one state
G_2	at each time i, the read-write head is scanning exactly one tape square
G_3	at each time i, each tape square contains exactly one symbol from Γ
G_4	at time 0, the computation is in the initial configuration of its checking stage for input x
G_5	By time $p(n)$, M has entered state q_y and hence has accepted x
G_6	For each time i the configuration of M at time $i+1$ follows by a single application of the transition function δ from the configuration at time i

G_1: at each time i, M is in exactly one state

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

G_1: at each time i, M is in exactly one state

$Q[i,0] \vee Q[i,1] \vee \ldots \vee Q[i,r]$	for all $0 \leq i \leq p(n)$
$\neg Q[i,j] \vee \neg Q[i,j']$	for all $0 \leq i \leq p(n), 0 \leq j \leq j' \leq r$

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q \rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert \Gamma \rvert$	at time i, the entry on tape square j is s_k

G_2: at each time i, the read-write head is scanning exactly one tape square

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

G_2: at each time i, the read-write head is scanning exactly one tape square

$H[i, -p(n)] \vee H[i, -p(n)+1] \vee \ldots \vee H[i, p(n)+1]$	for all $0 \leq i \leq p(n)$
$\neg H[i, j] \vee \neg H[i, j']$	for all $0 \leq i \leq p(n)$, $-p(n) \leq j \leq j' \leq p(n)+1$

Variable	Range	Intended meaning
$Q[i, k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q \rvert$	at time i, M is in state k
$H[i, j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i, j, k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert \Gamma \rvert$	at time i, the entry on tape square j is s_k

G_3: at each time i, each tape square contains at least one symbol from Γ

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

G_3: at each time i, each tape square contains at least one symbol from Γ

$S[i,j,0] \vee S[i,j,1] \vee \ldots \vee S[i,j,\lvert\Gamma\rvert]$	for all $0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$
$\neg S[i,j,k] \vee \neg S[i,j,k']$	for all $0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq k' \leq \lvert\Gamma\rvert$

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

G_4: at time 0, the computation is in the initial configuration of its checking stage for input x

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q \rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert \Gamma \rvert$	at time i, the entry on tape square j is s_k

G_4: at time 0, the computation is in the initial configuration of its checking stage for input x

$Q[0,0], H[0,1], S[0,0,0]$
$S[0,1,k_1], S[0,2,k_2], \ldots, S[0,n,k_n],$ with $x = (s_{k_1}, s_{k_2}, \ldots, s_{k_n})$
$S[0,n+1,0], S[0,n+2,0], \ldots, S[0,p(n)+1,0]$

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

Proof of Cook-Levin

G_5: by time $p(n)$, M has entered state q_y

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

Proof of Cook-Levin

G_5: by time $p(n)$, M has entered state q_y

$Q[p(n), 1]$

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

G_6: Changes according to transition function

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k

G_6: Changes according to transition function

$\neg H[i,j] \vee \neg Q[i,k] \vee \neg S[i,j,l] \vee H[i+1, j+\Delta]$
$\neg H[i,j] \vee \neg Q[i,k] \vee \neg S[i,j,l] \vee Q[i+1,k']$
$\neg H[i,j] \vee \neg Q[i,k] \vee \neg S[i,j,l] \vee S[i+1,j,l']$

with for $q_k \in Q \setminus \{q_Y, q_N\}$: $\delta(q_k, s_l) = (q_{k'}, s_{l'}, \Delta)$ and
for $q \in \{q_Y, q_N\}$: $\delta = 0$, $k' = k$, $l' = l$

Variable	Range	Intended meaning
$Q[i,k]$	$0 \leq i \leq p(n)$, $0 \leq k \leq \lvert Q\rvert$	at time i, M is in state k
$H[i,j]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$	at time i, the read-write head of M scans tape square j
$S[i,j,k]$	$0 \leq i \leq p(n)$, $-p(n) \leq j \leq p(n)+1$, $0 \leq k \leq \lvert\Gamma\rvert$	at time i, the entry on tape square j is s_k