∃∀

Ukažte, že jazyk L je rozhodnutelný, právě když existují rozhodnutelné jazyky A a B, pro které platí, že $L = \{x|(\exists y)[\langle x, y\rangle \in A]\} = \{x|(\forall y)[\langle x, y\rangle \in B]\}$.

→:
Máme rozhodnutelný jazyk L a chceme ukázat, že existují rozhodnutelné jazyky A a B.

To ukážeme tak, že dané jazyky zkonstruujeme:

1) $A = \{\langle x, y\rangle | x \in L \wedge y = \epsilon\}$, kde ϵ značí prázdné slovo nad abecedou Σ.
2) $B = \{\langle x, y\rangle | x \in L \wedge y \in \Sigma^*\}$

Tyto dva zkonstruované jazyky jsou rozhodnutelné, protože dokážeme pro každý z nich vytvořit algoritmicky vyčíslitelnou funkci f pro m-převoditelnost:

1) $A \leq_m L$: slovo $\langle x, y\rangle$ z A uznáme, pokud $x \in L$ a $y = \epsilon$.
2) $B \leq_m L$: slovo $\langle x, y\rangle$ z B uznáme, pokud $x \in L$.

←:
Máme rozhodnutelné jazyky A, B a chceme ukázat, že jazyk L je rozhodnutelný.

To ukážeme tak, že najdeme vyčíslitelnou funkci f pro m-převoditelnost $L \leq_m B$:

$f(x) = \langle x, \epsilon\rangle \in B$.

Prime

Popište algoritmus (pro Turingův stroj), který ignoruje svůj vstup a na výstup vypisuje postupně všechna prvočísla v rostoucím pořadí.

Budeme potřebovat systém, ve kterém bychom byli schopni reprezentovat čísla. Zavedeme tedy abecedu $\Sigma = \{0,1,S,D,d,E\}$, kde 0 a 1 označují bity. S bude označovat startovní pozici na pásce. Znak D a d použijeme jako oddělovače čísel. E pak označuje konec pásky.

Dále budeme potřebovat základní bitové operace jako je sčítání a odčítání 1. Přičítání je jednoduché, začneme zprava čísla a měníme jedničky na nuly. Jakmile narazíme na první nulu, změníme ji na jedničku. Odečítání bude obdobné, načneme zprava, měníme nuly na jedničky a první jedničku změníme na 0. Záporná čísla uvažovat nemusíme – nebudeme je potřebovat. Je potřeba rozmyslet alokaci nového prostoru při překročení maximálního počtu bitů, které máme pro číslo alokované (pomocí oddělovačů). Při překročení alokované kapacity, využijeme další bit vlevo a posuneme zbytek pásky.

Mějme tedy turingův stroj se dvěmi páskami. Procesní a výstupní. Začneme vstupním stavem, který zapíše na procesní pásku řetězec $E0D0SD11DE$. Tento řetězec značí, že zpracováváme číslo 2 ($D11D$), pak je zde označený začátek pásky, dvě pomocná pole pro čísla a konec pásky směrem vlevo. Na výstupní pásku zapíšeme $ESDE$. Na výstupní pásce budou čísla v reverzním bitovém zápisu.

Nyní můžeme začít kontrolu prvočíselnosti pro aktuálně zpracovávané číslo. To uděláme tak, že na výstupní pásce dojedeme hlavou až na konec pásky. Přejdeme do stavu Q_1, najdeme číslo o jedno vlevo a přepíšeme jej reverzně do pole o jedno vlevo od počáteční pozice na procesní pásce. Toto číslo pak postupně snižujeme, pomocí bitové operace odečtení 1, dokud se nerovná 0. Při každém snížení ***připíšeme*** do druhého pomocného pole jednu jedničku. V poli úplně vlevo by tedy mělo být tolik jedniček, jako byla hodnota čísla pomocného pole, kde bylo původně zkopírované číslo a v poli o jedna vpravo by měly být samé 0.

Nyní takto vytvořené jedničky použijeme jako pomocný oddělovač pro jedničky vpravo od S na procesní pásce. Postupným snižováním jedniček vlevo budeme posouvat oddělovač d mezi jedničkami vpravo, dokud vlevo nebudou samé 0. Pokud bychom zpracovávali například číslo 5 a dělali kontrolu pro číslo 2, vypadal by dosavadní postup takto:

Výstupní: $ESD01D11DE$
Procesní: $E10D00SD11111DE \rightarrow E00D11SD11111DE \rightarrow E00D00SD11d111DE$

Nyní se přepneme do dalšího stavu a budeme postupovat stejně jako v minulém kroku, pouze namísto toho, abychom použili pomocné pole, použijeme již jedničky, které máme před znakem d.

Procesní páska: $E00D00SD11d111DE \rightarrow E00D00SD00d11d1DE$

Takto pokračujeme, dokud nenarazíme na problém, kdy máme před posledním znakem d víc 1, než kolik nám zbývá. Pokud nám nezbyly vpravo za posledním d žádné 1, znamená to, že aktuální číslo je dělitelné. Smažeme tedy všechny d, od S vpravo přepíšeme 0 na 1 a připíšeme jednu 1, přesuneme hlavu na výstupní pásce úplně vpravo a pokračujeme stavem Q_1 pro další číslo.

Pokud dělení nevyšlo, nám došly jedničky vpravo od d, ale ne vlevo (viz $E00D00SD00d01d1dDE$), docházíme k závěru, že aktuálně zpracovávané číslo není dělitelné právě zkoušeným již nalezeným prvočíslem, opět smažeme všechny d, přepíšeme 0 na 1 a pokračujeme stavem Q_1. To nám zajistí, že zpracováváme stále stejné číslo, ale zkoušíme o jedno nižší dělitel.

Jakmile dojde stav Q_1 na výstupní pásce k symbolu S namísto očekávaného čísla, končí výpočet s tím, že aktuálně zpracovávané číslo je prvočíslem, jelikož ho nedělí žádné z nižších prvočísel a přepínáme se do fáze výpisu. Pásky vypadají tak, že na výstupní pásce je hlava na symbolu S a vpravo má nějaká prvočísla. Procesní páska má vlevo od S poze dvě 0 a vpravo záznam aktuálně zpracovávaného čísla v 1.

Přesuneme tedy hlavu na výstupní pásce až na poslední D a připíšeme za něj $0DE$. Postavíme hlavu na 0 na výstuupní pásce a na procesní pásce na první 1 vpravo od D. Začneme procházet jedničky na procesní pásce a zvyšovat číslo na výstupní pásce pomocí bitové operace přičítání jedničky, ovšem reverzně, aby nám přibývaly bity směrem ke konci pásky a dobře se nám alokoval prostor. Poté co na procesní pásce dojdeme ke znaku D, je náš přepis hotov. Připíšeme jednu jedničku na procesní pásku, posuneme konec pásky, posuneme hlavu na výstupní pásce až na konec a přepneme se do stavu Q_1. Začne zpracovávání dalšího čísla.

Paměťové nároky jsou $O(\log(N) * \#počet\ nalezených\ prvočísel)$, kde N značí počet velikost nejvyššího nalezeného prvočísla. Časové nároky jsou konstanta pro iniciaci, přepis prvočísla na jedničky lze v $O(P * \log(P)^2)$, kontrolu dělitelnosti poté zvládneme v $O(N * P)$. Úklid a posun hlav lze vždy schovat do $O(N)$. Celkovou složitost pro kontrolu jedním prvočíslem bych tedy odhanul pomocí $O\left(P * (\log(P)^2 + N)\right)$. $1 < P < N \to O(P * N)$. Prvočísel je až P a tedy hrubý horní odhad celkové složitosti pro kontrolu jednoho čísla na prvočíslo je $O(P^2 * N)$, kde P je velikost největšího prvočísla a N velikost aktuálně zpracovávaného čísla.