1.13 Testování prvočíselnosti

1.13.1 Jazyky L_p a L_s. Jazyk L_p obsahuje všechna prvočísla, jazyk L_s obsahuje všechna složená čísla; přesněji:

$$L_p = \{w \mid w \text{ je binární zápis prvočísla}\}$$

$$L_s = \{w \mid w \text{ je binární zápis složeného čísla}\}.$$

Jazyk L_s je (až na číslo 1) doplňkem jazyka L_p; přidáme-li 1 do jazyka L_s, pak dostáváme

$$L_s = \overline{L_p}, \quad L_p = \overline{L_s}.$$

1.13.2 Tvrzení. Jazyk L_s leží ve třídě $\mathcal{NP}$.

Zdůvodněni: Jestliže číslo n je složené, znamená to, že má dělitele r, pro nějž platí $1 < r < n$. Známe-li některého (tzv. vlastního) dělitele r, jsme schopni dělením čísla n číslem r zjistit, že n je opravdu složené číslo. Pro prvočíslo žádný takový vlastní dělitel neexistuje.

Nyní si stačí uvědomit, že vlastní dělitel je hledaný certifikát s polynomiální velkostí. Ano, délka binárního slova odpovídajícího n, je $k = \lg n$, délka dělitele r je $\mathcal{O}(k)$ a celočíselné dělení dvou binárních čísel délky k lze provést v polynomiáním čase vzhledem k délce binárního zápisu čísel.

1.13.3 Důsledek. Jazyk L_p je ve třídě co-$\mathcal{NP}$.

1.13.4 Tvrzení. Jazyk L_p je ve třídě $\mathcal{NP}$.

Najít polynomiální certifikát pro jazyk obsahující prvočísla je podstatně těžší než pro jazyk obsahující složená čísla. V tomto případě se jedná o generátor grupy $(\mathbb{Z}_p \setminus \{0\}, \odot, 1)$ (p prvočíslo); tj primitivní prvek konečného tělesa $(\mathbb{Z}_p, \oplus, \odot, 0, 1)$.

1.13.5 Důsledek. Jazyky L_p a L_s patří do průniku tříd $\mathcal{NP}$ a co-$\mathcal{NP}$.

1.13.6 V dalším ukážeme, že existuje pravděpodobnostní algoritmus — Millerův test prvočíselnosti, který pro dané velké liché číslo n s pravděpodobností aspoň $\frac{1}{2}$ rozhodne, zda n je prvočíslo. Dříve než algoritmus uvedeme, připomeneme několi faktů z algebry, které budeme potřebovat.

- Množina $\mathbb{Z}_n$ tzv. zbytkových tříd modulo n je
$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$
- Na množině $\mathbb{Z}_n$ jsou definovány operace $\oplus$ a $\odot$ takto
$$a \oplus b = c, \text{ kde } c \text{ je zbytek při dělení čísla } a+b \text{ číslem } n,$$
$$a \odot b = c, \text{ kde } c \text{ je zbytek při dělení čísla } a.b \text{ číslem } n.$$
- $(\mathbb{Z}_n, \oplus, 0)$ je komutativní grupa, $(\mathbb{Z}_n, \odot, 1)$ je komutativní monoid a platí distributivní zákony

  Navíc, prvek $a \in \mathbb{Z}_n$ má inverzní prvek (vzhledem k operaci $\odot$) právě tehdy, když a a n jsou nesoudělná čísla.

  Proto $(\mathbb{Z}_n, \oplus, \odot, 0, 1)$ pro n prvočíslo je těleso; pro složená n, tělesem není.

- Podle malé Fermatovy věty pro a nesoudělné s prvočíslem p platí

$$a^{p-1} \equiv 1 \pmod{n}.$$

- Je-li H podgrupa konečné grupy G, pak počet prvků podgrupy H dělí počet prvků grupy G.
- Operace sčítání, násobení, umocňování a dělení v $\mathbb{Z}_n$ je možné provést v polynomiálním čase vzhledem k velikosti čísel, se kterými se operace provádějí.

1.13.7 Millerův test prvočíselnosti.

Vstup: velké liché přirozené číslo n.

Výstup: „prvočíslo" nebo „složené".

1. Spočítáme $n-1 = 2^l\, m$, kde m je liché číslo.
2. Náhodně vybereme $a \in \{1, 2, \ldots, n-1\}$.
3. Spočítáme $a^m \pmod{n}$,
   jestliže $a^m \equiv 1 \pmod{n}$, stop, výstup „prvočíslo".
4. Opakovaným umocňováním počítáme
   $a^{2\, m} \pmod{n}, a^{2^2\, m} \pmod{n}, \ldots, a^{2^l\, m} \pmod{n}$.
5. Jestliže $a^{2^l\, m} \not\equiv 1 \pmod{n}$, stop, výstup „složené".
6. Vezmeme k takové, že $a^{2^k\, m} \not\equiv 1 \pmod{n}$ a $a^{2^{k+1}\, m} \equiv 1 \pmod{n}$.
   Jestliže $a^{2^k\, m} \equiv -1 \pmod{n}$, stop, výstup „prvočíslo".
   Jestliže $a^{2^k\, m} \not\equiv -1 \pmod{n}$, stop, výstup „složené".

1.13.8 Věta.

1. Jestliže pro vstup n dá Millerův test prvočíselnosti odpověď „složené", pak je číslo n složené.
2. Jestliže pro vstup n dá Millerův test prvočíselnosti odpověď „prvočíslo", pak n je prvočíslo s pravděpodobností větší než $\frac{1}{2}$.

Idea důkazu. Add 1. Jestliže je číslo n prvočíslo, tak nemůžeme dostat výstup „složené". Malá Fermatova věta totiž zaručuje, že nemůžeme skončit v kroku 5 s výstupem „složené". Dále pro n prvočíslo je $(\mathbb{Z}_n, \oplus, \odot)$ konečné těleso. V tělese existují pouze dva prvky, které umocněné na druhou dávají 1 (tzv. odmocniny z 1) — totiž číslo 1 a -1. Proto nemůžeme skončit ani v kroku 6 výstupem „složené".

Add 2. Ukázat druhou vlastnost je obtížnější. Důkaz není těžký pro taková složená n, pro která existuje $a \in \mathbb{Z}_n$, a nesoudělné s n, a $a^{n-1} \not\equiv 1 \pmod{n}$.

Pro ostatní složená čísla, tzv. „pseudoprvočísla“, (též „Carmichaelova čísla“), je důkaz dost obtížný.

Ukážeme základní myšlenku důkazu pro složená n: Spočítáme počet takových a vybraných v kroku 2, pro která dostaneme jistě správnou odpověď (tj. nedostaneme odpověď prvočíslo). Protože každé a má stejnou pravděpodobnost být vybráno, stačí, abychom ukázali, že jich je aspoň tolik, kolik jich může dát odpověď špatnou (prvočíslo).

Vybereme-li v kroku 2 neinvertibilní číslo a, určitě dostaneme odpověď složené, protože žádná mocnina neivertibilního čísla nemůže být rovna 1.

Předokládejme, že složené číslo n není pseudoprvočíslo, tj. existuje $a \in \mathbb{Z}_n$, a nesoudělné s n, a $a^{n-1} \not\equiv 1 \pmod{n}$. Označme

$$\mathbb{Z}_n^\star = \{a \in \mathbb{Z}_n \mid a \text{ je invertibilní}\}$$

$$K = \{a \in \mathbb{Z}_n \mid a^{n-1} = 1\}.$$

Víme, že $K \neq \mathbb{Z}_n^\star$, přitom $(K, \odot)$ je podgrupa grupy $(\mathbb{Z}_n^\star, \odot)$. Proto počet prvků K dělí počet prvků $\mathbb{Z}_n^\star$. Odtud počet prvků v množině K je nejvýše dvakrát méně než prvků v množině $\mathbb{Z}_n^\star$; jinými slovy

$$|\mathbb{Z}_n^\star \setminus K| \geq |K|.$$

Vybereme-li $a \in \mathbb{Z}_n^\star \setminus K$, dostaneme správnou odpověď „složené“, protože $a^{n-1} \neq 1$.

Špatnou odpověď můžeme dostat pouze pro $a \in K$ a těch je méně než nebo stejně jako $a \in \mathbb{Z}_n^\star \setminus K$.

Pro pseudoprvočísla platí $|K| = |\mathbb{Z}_n^\star|$ a musíme argumentovat krokem 6, kde se dá ukázat, že počet a, která vedou v kroku 6 na odmocninu z 1 různou od -1 je aspoň tak velký jako počet těch a, která vedou na -1.

1.14 Třídy založené na pravděpodobnostních algoritmech

1.14.1 Randomizovaný Turingův stroj. RTM je, zhruba řečeno, Turingův stroj M se dvěma nebo více páskami, kde první páska má stejnou roli jako u deterministického Turingova stroje, ale druhá páska obsahuje náhodnou posloupnost 0 a 1, tj. na každém políčku se 0 objeví s pravděpodobností $\frac{1}{2}$ a 1 také s pravděpodobností $\frac{1}{2}$.

Na začátku práce:

- stroj M se nachází v počátečním stavu q_0;
- první páska obsahuje vstupní slovo w, zbytek pásky pak blanky B;
- druhá páska obsahuje náhodnou posloupnost 0 a 1;
- případné další pásky obsahují B;
- všechny hlavy jsou nastaveny na prvním políčku dané pásky.

Na základě stavu q, ve kterém se stroj M nachází, a na základě obsahu políček, které jednotlivé hlavy čtou, přechodová funkce δ určuje, zda se M zastaví nebo přejde do nového stavu p, přepíše obsah první pásky (**nikoli ale obsah druhé pásky**) a hlavy posune doprava, doleva nebo zůstanou stát (posuny hlav jsou nezávislé).

Formálně, je-li M ve stavu q, hlava na první pásce čte symbol X, na druhé pásce je číslo a a

$$\delta(q, X, a) = (p, Y, D_1, D_2), \quad q, p \in Q, a \in \{0,1\}, X, Y \in \Gamma, D_1, D_2 \in \{L, R, S\},$$

pak M se přesune do stavu p, na první pásku napíše Y a i-tá hlava se posune doprava pro $D_i = R$, doleva pro $D_i = L$ nebo zůstane na místě pro $D_i = S$.

Jestliže $\delta(q, X, a)$ není definováno, M se zastaví.

M se úspěšně zastaví právě tehdy, když se přesune do koncového (přijímacího) stavu q_f.

1.14.2 Poznámka. Rozdíl mezi RTM a obyčejným TM je v roli druhé pásky. Dvoupáskový TM může přepisovat i obsah druhé pásky a to je v případě RTM zakázáno. Navíc při dvou bězích RTM může být průběh práce RTM různý (záleží na náhodně vygenerovaném obsahu druhé pásky). To se u vícepáskového deterministického TM stát nemůže.

Může se zdát, že tento model je nerealistický — nemůžeme před začátkem práce naplnit nekonečnou pásku. Toto je ale „realizováno“ tak, že v okamžiku, kdy druhá hlava čte dosud nenavštívené políčko druhé pásky, náhodně se vygeneruje 0 nebo 1 každé s pravděpodobností $\frac{1}{2}$ a tento symbol už se nikdy během jednoho průběhu práce TM nezmění.

1.14.3 Příklad. Je dán RTM M, kde $Q = \{q_0, q_1, q_2, q_3, q_f\}$, $\Gamma = \{0, 1, B\}$ a přechodová funkce δ je definována:

$$\begin{array}{rl} \delta(q_0, 0, 0) = (q_1, 0, R, S), & \delta(q_0, 1, 0) = (q_2, 1, R, S), \\ \delta(q_1, 0, 0) = (q_1, 0, R, S), & \delta(q_1, B, 0) = (q_f, B, S, S), \\ \delta(q_2, 1, 0) = (q_2, 1, R, S), & \delta(q_2, B, 0) = (q_f, B, S, S), \\ \delta(q_0, a, 1) = (q_3, a, S, R), & \delta(q_3, a, a) = (q_3, a, R, R), \\ \delta(q_3, B, a) = (q_f, B, S, S), & \text{pro } a \in \{0, 1\}. \end{array}$$

Předpokládejme, že na vstupu má RTM M slovo w, pak:

- Jestliže první symbol druhé pásky je 0 (tj. náhodně jsme vygenerovali 0), M zkontroluje, zda $w = 0^n$ nebo $w = 1^n$ pro nějaké $n > 0$.
- Jestliže první symbol druhé pásky je 1 (tj. náhodně jsme vygenerovali 1), hlava na druhé pásce se posune doprava a M zkontroluje, zda se obsah druhé pásky od druhého políčka shoduje se vstupem w.

Nenastane-li ani jeden z předchozích případů, M se neúspěšně zastaví.

V případě RTM je třeba spočítat pravděpodobnost s jakou se M pro dané vstupní slovo w úspěšně zastaví, tj. zastaví v „přijímacím“ stavu q_f. V našem příkladě je odpověď tato:

- Jestliže w je prázdné slovo, M se v q_f nikdy nezastaví (tj. pro žádný náhodný obsah druhé pásky).

- Jestliže $w = 0^n$ nebo $w = 1^n$ pro $n > 0$, M se zastaví v q_f s pravděpodobností
$$\frac{1}{2} + \frac{1}{2}\left(\frac{1}{2}\right)^n = \frac{1}{2} + 2^{-(n+1)}.$$
- Jestliže w je jiného tvaru, tj. obsahuje jak 0, tak 1, pak pravděpodbnost, že se M zastaví v q_f je
$$\frac{1}{2}\left(\frac{1}{2}\right)^{|w|} = 2^{-(|w|+1)}.$$