7. CVIČENÍ Z ADS2

Hradla a obvody

Booleovská funkce n proměnných: Jakákoli funkce $f : \{0,1\}^n \to \{0,1\}$.

Obvyklá reprezentace: Pokud to jde, tak předpisem. Často to ale nejde, pak je zadaná tabulkou výstupů pro všechny vstupy.

Booleovská formule: Formule s proměnnými, logickými spojkami (většinou $\vee, \wedge, \neg$) a závorkami. Její *velikost* je počet všech výskytů proměnných, všech závorek a všech spojek.

Obvyklá reprezentace: Klasickým logickým zápisem formule. Pravdivostní tabulka sice počítá ekvivalentní hodnoty, ale není to zápis formule samotné.

Hradlová síť/obvod: Acyklický orientovaný graf sestávající ze *vstupů* odpovídajícím binárním proměnným na vstupu, *hradel* s několika vstupními a výstupními hranami a *výstupními terminály.*

Obvykle bývají hradla binární nebo unární (ale nemusí), a obvykle bývá jeden výstup pro všechny vstupy (ale nemusí).

Obvyklá reprezentace: Diagramem.

V dnešním cvičení budeme řešit pouze booleovské hradlové síťě, tedy ty, co podporují unární nebo binární operace.

Příklad první

Rozvička: Hypoteticky existuje 16 binárních hradel. Ukažte, že je všechny umíme implementovat pomocí `AND`, `OR` a `NOT` hradel.

Bonus: Všechny si je napište a pojmenujte co nejvíce z nich zažitými jmény.

Příklad druhý

Jde každá booleovská funkce n proměnných zapsat jako hradlová síť? Můžete použít libovolně hradel. Zkuste vyjádřit svůj počet hradel jako funkci n.

Příklad třetí

Na rozdíl od obecných algoritmů umíme o hradlových sítích ihned říci nějaké zajímavé dolní odhady. Třeba tento:

„Pro každé k platí, že existuje Booleovská funkce na n proměnných, která nejde spočítat hradlovou sítí s $O(n^k)$ hradly.“

Zkuste to dokázat! Může se hodit nějaký počítací argument.

Příklad čtvrtý

1. Obvyklá reprezentace hradlové sítě je graf. Řekněme, že je vaším úkolem hradlovou síť s A hradly co nejkompaktněji popsat binárním řetězcem. Vymyslete nějakou reprezentaci (můžete být kreativní). Spočitejte si, jakou délku bude mít váš binární řetězec v nejhorším případě.
2. Odvoďte z předchozího tvrzení fakt, že *existuje booleovská funkce n proměnných, která potřebuje na svou reprezentaci alespoň* $2^n/(100 \cdot n)$ *hradel.* To je o chlup silnější tvrzení, než jsme nahlédli v minulém příkladu.

Příklad pátý

Jsou hradla aspoň tak silná, jako polynomiální programy? Ano. Zkuste dokázat, že pokud existuje pro problém s n-bitovým vstupem polynomiální algoritmus, který ho vyřeší (a řekněme odpoví 0/1), tak existuje obvod s polynomiálním počtem hradel, který problém také vyřeší.

Váš důkaz nemusí být zcela formální, zkuste použít vlastní slova.

Příklad šestý

Jsou hradla aspoň tak silná, jako booleovské formule? Ukažte, že máme-li booleovskou formuli délky l, tak umíme postavit obvod délky $O(l)$, který ji počítá.

Poznámka: A co naopak? Spočítají polynomiálně velké formule totéž, co polynomiálně velké hradlové sítě? Ano (to kdyžtak uvidíme jindy).

PŘÍKLAD SEDMÝ Pojďme si hrát s paritou! `PARITY` je booleovská funkce na n proměnných, která počítá paritu (sudost počtu jedniček na vstupu.

1. Ukažte triviální booleovskou hradlovou síť, která spočíta `PARITY` v hloubce $O(\log n)$ a s $O(n)$ hradly.
2. Dokažte, že `PARITY` nelze spočítat jen pomocí hradel typu `AND`.
3. Podívejme se teď na formule, a to konkrétně formule v DNF tvaru. (Ty odpovídají speciálním „třívrstvým“ hradlovým sítím, kde výstupní stupeň je vždy jedna, v první vrstvě jsou jen hradla `NOT`, v druhé `AND` a nakonec `OR`). Ukažte, že DNF formule potřebují velikost $\Omega(2^n)$ na spočítání `PARITY`.
   Jak na to? Funkce `PARITY` je vysoce symetrická; ukažte ted nejprve, že každá klauzule v DNF zápisu vypadá skoro stejně, a pak spočítejte, kolik jich musí být, aby klauzule popsaly všechny možné vstupy.

Poznámka: Platí i silnější tvrzení: booleovské hradlové sítě konstantní hloubky nemohou počítat `PARITY`. To si ale necháme na jiný předmět ...