

Limity datových struktur, komunikace a karet – abstrakt

V této práci studujeme několik aspektů výpočetní složitosti. Jedno z hlavních témat je složitost datových struktur, což jsou algoritmy pro efektivní ukládání dat podporující efektivní dotazy na daná data. Dynamické datové struktury také umožňují měnit data před dotazem. Dlouho otevřený problém v této oblasti je dokázat nepodmíněný polynomiální dolní odhad na porovnání času na editaci a času na dotaz adaptivní dynamické struktury počítající nějakou explicitní funkci.

Ukazujeme nepodmíněný polynomiální dolní odhad pro omezenou třídu semi-adaptivních dynamických datových struktur počítající funkce s velkou korupční mezí, což zobecňuje výsledek od Ko a Weinsteina [FOCS '20], kteří ukázali takový dolní odhad pro datové struktury počítající funkci disjunkce. Dále ukazujeme podmíněný dolní odhad pro určité statické datové struktury počítající inverzi permutací, a vyhodnocení a interpolaci polynomů. Tyto dolní odhady jsou lepší než nejlepší známé nepodmíněné dolní odhady pro dané problémy.

Dále studujeme komunikační složitost eliminačního problému, který je velmi blízký problému přímého součtu. U eliminačního problému, Alenka a Bob dostanou k n -bitových řetízků, x_1, \dots, x_k , respektive y_1, \dots, y_k . Jejich cílem je komunikovat co nejméně bitu a vystoupit řetízek $o \in \{0, 1\}^k$ který se liší od řetízku z , kde $z_i = f(x_i, y_i)$ pro nějakou zafixovanou booleovskou funkci $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ – tedy vyeliminují jednu nesprávnou odpověď. Uvažujeme eliminační problém pro funkci Větší-Než (GT), t.j., $GT(x, y) = 1$ právě tehdy, když $x \geq y$, kdy x a y chápeme jako n -bitová čísla. Dokážeme, že triviální protokol pro tuto funkci (kdy Alenka a Bob spočítají, zda $x_i \geq y_i$ pro nějaké i) je optimální.

Poslední téma této práce jsou takzvané karetní protokoly. V tomto modelu Alenka a Bob reprezentují své vstupy kartami a chtějí spočítat výsledek dané funkce bez odhalení jejich vstupů. Identifikujeme třídu karetních protokolů, která odpovídá třídě obvodů NC^1 . Dále pak studujeme souvislost mezi karetními protokoly a Turingovými stroji a navrhuje nové kódování vstupu pomocí karet.