Úkol 3

Příklad 1

Consider the following modification of the $(GEOGRAPHY)\,GAME$:

> A *parity game* is a quadruple (V, E, s, α) where (V, E) is a directed graph (with vertices V and edges $E \subseteq V \times V$), $s \in V$ is an initial vertex and $\alpha : V \to \mathbb{N}$ is the weight function. The game is played by two players (Player 1, who starts, and Player 2), who alternate in moving a token along the vertices of the graph according to the graph edges. Each vertex can be visited at most once. The game ends when it is not possible to make a move. The winner is Player 1 iff the smallest weight encountered along the game is odd and Player 2 if it is even (note that it does not matter whose turn it was when the game ended).

$PARITY\ \ GAME$ asks whether, given a parity game g, Player 1 has a winning strategy for g.
Prove that $PARITY\ \ GAME$ is $PSPACE$-complete.

Hint: modify the proof that $GEOGRAPHY\ \ GAME$ is $PSPACE$-complete from the book of Papadimitriou (an excerpt from the book with the proof can be found here: http://www.fit.vutbr.cz/~lengal/slo-2022/geography-pspace-complete.pdf).

Řešení 1

Důkaz. Důkaz $PSPACE$-úplnosti $PARITY\ \ GAME$ rozdělíme do dvou částí. Nejprve ukážeme, příslušnost do $PSPACE$ a poté, že existuje redukce ze známého $PSPACE$-úplného problému.

Důkaz náležitosti do $PSPACE$:

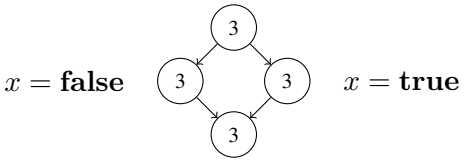
Uvažujme 3 páskový deterministický Turingův stroj M, který rozhoduje problém $PARITY\ \ GAME$. Vstupní páska stroje má tvar $\triangle\langle V\rangle\#\langle E\rangle\#\langle s\rangle\#\langle\alpha\rangle\triangle\triangle^{\omega}$, kde $\langle V\rangle$ je kód množiny vrcholů, $\langle E\rangle$ je kód množiny hran, $\langle s\rangle$ je kód počátečního vrcholu, $\langle\alpha\rangle$ je kód váhové funkce. Průběh hry $PARITY\ \ GAME$ je možné charakterizovat *AND/OR* stromem, kde Hráč 1 využívá *OR* uzly a Hráč 2 používá *AND* uzly. Průchod stromem do hloubky je simulován na druhé pásce. Strom hry je generován po částech. Prohledané větve se odstraní. Na třetí pásce se uchovává sekvence hodnot navštívený vrcholů dle váhové funkce α. V listovém uzlu stromu hry na pásce 2 je vyhodnoceno, zda je nejmenší číslo na třetí pásce liché, pak je list ohodnocen jako ***true***, v opačném případě jako ***false***. Lze vidět, že $PARITY\ \ GAME \in PSPACE$.

Redukce $QSAT$ na $PARITY\ \ GAME$:

Redukci ukážeme na příkladu. Je zřejmé, že redukce funguje i pro jeho zobecnění. Mějme instanci $QSAT$:

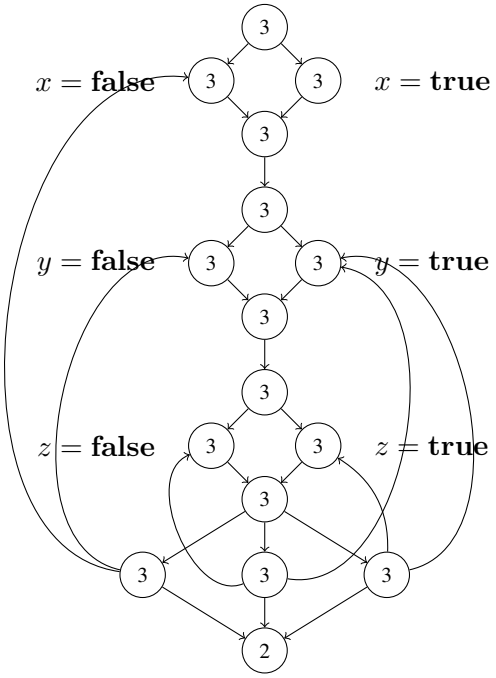
$$\exists x \forall y \exists z : \big((\neg x \vee \neg y) \wedge (y \vee z) \wedge (y \vee \neg z)\big)$$

Pro každou proměnnou vytvoříme diamant v grafu, kde všechny vrchly budou mít váhu 3.



Obrázek 1: Diamant pro proměnnou x.

Vytvořené diamanty propojíme hranami v pořadí odpovídajícímu pořadí kvantifikátoru ve formuli. K poslednímu uzlu sekvence přiřadíme tolik nových *konjunkčních* uzlů s váhou 3, kolik obsahuje formule konjunkcí (v našem případě tři). Z těchto uzlů vedeme hrany k uzlů odpovídajícím disjunkcím ve vybrané konjunkci (pro $(\neg x \vee \neg y)$ vedeme hrany do uzlů $x = \mathbf{false}$ a $y = \mathbf{false}$). Dále vytvoříme jeden *fail* uzel s váhou 2, do kterého povedou hrany ze všech *konjunkčních* uzlů vytvořených v předešlém kroku.



Obrázek 2: Formule reprezentovaná grafem v $PARITY\ GAME$

Každá cesta v grafu vždy vybere jednu stranu každého diamantu. Hráč 1 reprezentuje existenční kvantifikátory a Hráč 2 univerzální. Lze vidět, že pokud je cesta zvolena tak, že existenční hráč (Hráč 1) nemůže provést poslední krok do uzlu s hodnotou 3, protože cílový uzel již byl navštíven, pak musí zvolit přechod do uzlu s váhou 2 a prohrává, protože podle $PARITY\ GAME$ musí být nejnižší navštívená váha lichá, aby Hráč 1 vyhrál.

Bylo tedy dokázáno, že problém $PARITY\ GAME$ je $PSPACE$-úplný. □

Příklad 2

Let $G = (V, E)$ be a finite undirected graph, i.e., $E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$. A set of vertices $S \subseteq V$ is a *k-clique* of G iff $|S| = k$ and $\{\{i, j\} \mid i, j \in S, i \neq j\} \subseteq V$. The problem $\oplus CLIQUE$ is defined as follows:

$$\oplus CLIQUE = \{((V, E), k) \ : \ |\{S \subseteq V : S \text{ is a } \textit{k-clique} \text{ of } G\}| \ mod\ 2 = 1\},$$

i.e., it is the set of graphs that have an *odd* number of *k-cliques*. Show that $\oplus CLIQUE$ and $co \oplus CLIQUE$ are $PSPACE$-interreducible (i.e., that there is a polynomial reduction in both directions).

Řešení 2

Víme, že $\#CLIQUE$ je známý problém v $PSPACE$. $\oplus CLIQUE$ pouze k výsledku $\#CLIQUE$ přidává kontrolu na modulo, takže lze vidět, že i $\oplus CLIQUE$ je v $PSPACE$. Důkaz interreducibility $\oplus CLIQUE$ a $co \oplus CLIQUE$

ukážeme ve dvou krocích. Nejprvé provedeme redukci z $\oplus CLIQUE$ na $co \oplus CLIQUE$ a poté v opačném směru.

Důkaz. Pro důkaz předpokládejme, že se nemusí jednat o souvislý draf. (K zobecnění důkazu pro libovolný graf by bylo potřeba propojit pouze jeden nově přidaný vrchol s libovolným vrcholem dosavadního grafu. Navíc pro případ $k = 2$ by se musel přidat pouze jeden nový vrchol a nikoliv 2.)

Redukce $\oplus CLIQUE$ na $co \oplus CLIQUE$:

Mějme redukční funkci f, která je definovaná následovně:

$$f(\langle V\rangle\#\langle E\rangle\#\langle k\rangle) = \langle V'\rangle\#\langle E'\rangle\#\langle k'\rangle$$

Pokud je $\langle V\rangle\#\langle E\rangle\#\langle k\rangle$ neplatnou instancí $\oplus CLIQUE$, pak:

- $V' = \{a, b\}$
- $E' = \{\{a, b\}\}$
- $k' = 2$.

Jinak:

- $V' = V \cup V_k$, kde $V \cap V_k = \emptyset$ a $|V_k| = k$, V_k je množina nových vrcholů
- $E' = E \cup \{\{u, v\} \mid u, v \in V_k, u \neq v\}$
- $k' = k$.

Redukce $co \oplus CLIQUE$ na $\oplus CLIQUE$:

Mějme redukční funkci f, která je definovaná následovně:

$$f(\langle V\rangle\#\langle E\rangle\#\langle k\rangle) = \langle V'\rangle\#\langle E'\rangle\#\langle k'\rangle$$

Pokud je $\langle V\rangle\#\langle E\rangle\#\langle k\rangle$ neplatnou instancí $co \oplus CLIQUE$, pak:

- $V' = \emptyset$
- $E' = \emptyset$
- $k' = 2$.

Jinak:

- $V' = V \cup V_k$, kde $V \cap V_k = \emptyset$ a $|V_k| = k$, V_k je množina nových vrcholů
- $E' = E \cup \{\{u, v\} \mid u, v \in V_k, u \neq v\}$
- $k' = k$.

Lze vidět, že redunkční funkce f použita v obou případech je polynomiální, protože kontrolu správnosti vstupu lze provést v $\mathcal{O}(n^2)$ (provádíme také kontrolu, zda vrcholy hran existují v množině všech vrcholů) a vytvoření nové kliky lze také provést v $\mathcal{O}(n^2)$ (propojíme každý vrchol s každým).

Bylo dokázáno, že $\oplus CLIQUE$ a $co \oplus CLIQUE$ jsou $PSPACE$-interreducibilní. □

Příklad 3

Let $\Sigma = \{0, 1\}$ and $f : \Sigma^* \to \Sigma^*$ be a one-way function such that $\forall x \in \Sigma^* : |f(x)| = |x|$. Consider the following language L_f:

$$L_f = \{(x, y, c) \in \Sigma^* \times \Sigma^* \times \mathbb{N} : |x| = |y| \wedge \exists z \in \Sigma^{|y|} : f(z) = y \wedge popcount(x \oplus z) \leq c\},$$

where $x \oplus y$ denotes the XOR of binary strings x and y and $popcount(x)$ denotes the number of occurrences of the symbol "1" in x.
Prove that $L_f \in UP \setminus P$.

Řešení 3

Pro důkaz je potřeba ukázat, že $L_f \in UP$ a $L_f \notin P$.

Důkaz. Důkaz $L_f \in UP$:

Existuje jednoznačný TM M (protože funkce f je injektivní), který pro vstup (x, y, c) nedeterministicky uhádne z délky $|y|$ a zkontroluje, jestli $f(z) = y$ a $popcount(x \oplus z) \leq c$. Pokud ano, pak M akceptuje, jinak zamítne.

Důkaz $L_f \notin P$:

Důkaz povedeme sporem. Předpokládejme, že pro L_f existuje polynomiální algoritmus, potom můžeme invertovat na základě x a c funkci f za použití například binárního prohledávání, to by ale znamenalo, že funkce f není jednosměrná, což je spor s předpokladem, tedy nemůže existovat polynomiální algoritmus pro L_f.

Bylo dokázáno, že $L_f \in UP \setminus P$.

□