V následujícím seznamu nabízím problémy a témata vhodná pro doktorandské práce; většina z nich má i snazší versi vhodnou pro diplomové práce. Osm z deseti témat spadá, více či méně, do tzv. logické teorie složitosti (t.j. do složitosti důkazů a omezené aritmetiky). Uvítám však i zájemce o zcela jiná témata, zejména pak z moderní teorie modelů.

Pár vět o "složitosti důkazů": Fakt, že výroková formule je tautologií, lze ověřit jednak postupným výpočtem její pravdivostní hodnoty pro všechna ohodnocení proměnných, jednak jejím důkazem ve výrokovém počtu. Základní, stále otevřenou, otázkou je, zda-li jsou tyto dva přístupy v zásadě stejně efektivní či zda-li lze v nějakém konkrétním výrokovém kalkulu najít vždy důkaz podstatně kratší než je počet všech pravdivostních ohodnocení.

Tento problém souvisí s mnoha na první pohled rozličnými oblastmi logiky a matematiky. Zejména je úzkém vztahu s otevřenými otázkami v teorii výpočetní složitosti a v aritmetice prvního řádu (speciálně v tzv. omezené aritmetice). Dílčí výsledky jsou známy a v řadě menších problémů lze doufat v brzký pokrok.

Jan Krajíček
krajicek@math.cas.cz

12. X. 1999

1. **Důkazy prvočíselnosti.** Pro přirozené číslo n lze napsat výrokovou formuli A_n, která je tautologií právě když n je prvočíslem. O délkách důkazů takových tautologií se ví velmi málo (jak spodní, tak horní odhady).

2. **Turnajový princip.** Turnaj je orientovaný graf na n vrcholech takový, že mezi každými dvěma různými vrcholy vede právě jedna hrana. Turnajový princip říká, že v každém turnaji existuje tzv. dominující množina D nejvýše $\log n$ vrcholů, t.j. taková množina, že pro každý vrchol $u \notin D$ existuje vrchol $v \in D$ a hrana z v do u.

   Výroková složitost souvisejících kombinatorických principů (jako např. Ramseyovy věty) je známa, ale o turnajovém principu se ví méně. Konkrétní problém: má turnajový princip polynomiálně dlouhé důkazy ve Fregeho systému omezené hloubky?

3. **Matematické důkazové systémy.** I v matematice mimo logiku se vyskytuje řada vět, které lze interpretovat tak, že v podstatě tvrdí, že nějaký důkazový systém je úplný a korektní. Příkladem je Hilbertova věta tzv. Nullstellensatz, která charakterisuje neřešitelné systémy polynomiálních rovnic jako ty, které generují triviální ideál. Bylo by velmi zajímavé sestavit větší soubor podobných příkladů a navzájem je porovnat z hlediska složitosti důkazů.

4. **Hranice efektivní interpolace.** Tzv. efektivní interpolace je metoda spodních odhadů délek důkazů založená na Craigově větě o interpolaci. Hranice její použitelnosti nejsou ještě zcela jasné, i když existují nadějné hypotézy. Tato otázka též souvisí s definovatelností základních kryptografických protokolů v omezené aritmetice.

5. **Komunikační složitost s reálnými čísly.** Jedním z přístupů k efektivní interpolaci (viz. předchozí problém) je založen na studiu her dvou hráčů a množství informace, kterou si v průběhu hry předávají (tzv. komunikační složitost). Lze formulovat obecná kritéria, která redukují efektivní interpolaci na komunikační složitost; v této souvislosti je ale ještě několik otevřených problémů.

6. **Modely omezené aritmetiky.** Důkazy většiny spodních odhadů pro výrokový počet a vět o nezávislosti v omezené aritmetice lze interpretovat jako konstrukce modelů omezené aritmetiky tzv. modelovým forcingem. Existuje celá řada problémů spojených s rozšířením této metody na silnější výrokové počty či teorie aritmetiky.

7. **Neklasické výrokové počty.** Složitost výrokových důkazů se intensivně studuje v klasické logice ale v neklasické (např. vícehodnotové) je málo známo. Existuje celá řada problémů od lehčích (dokázat věty analogické těm, co jsou známy v klasickém případě) až po těžké (vyřešit nějaký problém, který je v klasickém případě otevřený).

8. **Turingovy stroje a důkazové systémy nad R.** Existuje definice Turingova stroje nad obecnou strukturou M; obvyklá definice se dostane pro $M = \mathbf{N}$. Pro $M = \mathbf{R}$ byl tento pojem studován autory L. Blum(ová), M. Shub a S. Smale, kteří vytvořili teorii analogickou teorii NP-úplnosti v klasickém případě. Má tedy smysl definovat výrokové počty nad $\mathbf{R}$. V tom se zatím neudělalo nic.

9. **Eulerovské struktury.** Eulerovská struktura je struktura prvého řádu, v níž je možné přiřadit definovatelným množinám "velikost" tak, že obvyklé vlastnosti počítání s konečnými množinami stále platí (např. velikost disjunktního sjednocení je součet velikostí a pod.). Tato funkce "velikosti" (tzv. abstraktní Eulerova charakteristika) nemá nic společného s mohutností ve smyslu teorie kardinálních čísel. Tento pojem je relativně nový a řada přirozených otázek je otevřena.

10. **Konečná teorie modelů.** Teorie konečných modelů se odlišuje od obecné teorie modelů ve dvou aspektech. Jednak většina základních vět a konstrukcí obecné teorie modelů je infinitární a ve třídě konečných struktur neplatí. Do popředí se tak dostávají zajímavé metody založené na různých hrách (např. Ehrenfeucht-Fraisse hry či oblázkové hry) a pravděpodobnostní konstrukce. Druhým důležitým aspektem je přímý vztah mezi definovatelností v konečných strukturách a algoritmickou rozhodnutelností s omezenou výpočetní složitostí. Některé problémy teorie složitosti se tak dají zformulovat v teorii konečných modelů bez použití pojmu Turingova stroje. V této oblasti existuje mnoho problémů, od lehčích až po těžké.