Jaroslav Hora

Eliminace kvantifikátorů v elementární teorii reálně uzavřených těles: pozoruhodná historie, aktuální současnost

In: Jindřich Bečvář (editor); Eduard Fuchs (editor): Matematika v proměnách věků. III. (Czech). Praha: Výzkumné centrum pro dějiny vědy, 2004. pp. 56–68.

Persistent URL: http://dml.cz/dmlcz/401595

Eliminace kvantifikátorů v elementární teorii reálně uzavřených těles: pozoruhodná historie, aktuální současnost

JAROSLAV HORA

Úvodem je třeba požádat čtenáře, aby se nedal odradit „podivným" názvem. Půjde o věci zcela praktické, mající vztah dokonce již i ke středoškolské matematice: nejdůležitějším modelem zmíněné teorie je totiž těleso reálných čísel. Cílem tohoto článku je popsat jednu fascinující kapitolu v historii lidského poznání, a to přístupně, s jistou mírou nutných zjednodušení. Z tohoto důvodu ani nebudeme uvádět soupis axiomů elementární teorie reálně uzavřených těles. Čtenář jej s mnoha dalšími informacemi nalezne např. v nedávno vydané knize [11]. Více pozornosti budeme věnovat aktuálním možnostem matematického software, které dnes mj. umožní zájemci studovat některé věci neobvyklou formou, kdy se lze „zeptat počítače". K výpočtům lze využít softwarový balík Mathematica® 5.0, který je prvním z velkých komerčních programů, realizujících eliminaci kvantifikátorů v tělese reálných čísel.[1]

Napišme nejprve několik jednoduchých formulí, obsahujících kvantifikátory a vypovídajících o reálných číslech:

$$(\forall x)\ (\forall y)\quad [x^2 + y^2 \geq 0] \tag{1}$$

$$(\forall x)\ (\exists y)\quad [x + y = 0] \tag{2}$$

$$(\exists x)\ (\forall y)\quad [x + y = 0] \tag{3}$$

$$(\forall x)\quad [x^2 \geq a] \tag{4}$$

$$(\exists x)\quad [x^2 + px + q = 0] \tag{5}$$

Ve formulích (1), (2), (3) jsou všechny proměnné vázané. Takovýmto formulím budeme říkat sentence. Formule (4) obsahuje jak jednu vázanou proměnnou x, tak i volnou proměnnou a. Formule (5) obsahuje kromě vázané proměnné x ještě dvě volné proměnné p, q. O pravdivosti sentencí lze rozhodnout: v daném případě jsou (1) a (2) pravdivé, (3) nikoli. Program Mathematica® 5.0 udělá rozhodnutí za nás: zapíšeme

[1] Program Mathematica® 5.0 byl uvolněn 23. 6. 2003 a patnáctidenní zkušební verzi lze získat na webovské stránce
`http://www.wolfram.com/products/mathematica/trial.cgi`.

```
FullSimplify [ForAll[x,y, x^2 + y^2 >= 0]]
```

a dostaneme odpověď

True

Čtenář může sám ověřit, že v případě (2) získá odpověď *True*, ve (3) *False*.

V dalších případech bychom povel **FullSimplify** mohli interpretovat jako příkaz, který by měl vrátit formuli ekvivalentní s formulí původně zadanou. Výsledná formule by již neměla obsahovat kvantifikátory. Podaří se to?

```
FullSimplify [ForAll [x, x^2 >= a]]
```

$a \leq 0$

Zdá se, že v konkrétních ukázkách se eliminace kvantifikátorů tělese reálných čísel, tj. ve „slovníku" $R = \langle \mathbb{R}, +, \cdot, 0, 1, < \rangle$ zdařila. Bude to možné vždy?

Odpověď na tuto obtížnou otázku nalezl jeden z největších logiků lidské historie.

Alfred Tarski
14. 1. 1902 Varšava – 26. 10. 1983, USA Berkeley, Kalifornie

Životní osudy tohoto muže byly komplikované. Narodil se v rodině zámožného obchodníka se dřevem Ignáce Teitelbauma. V době středoškolských studií Alfréda Teitelbauma bylo Polsko stále ještě rozděleno mezi tři mocnosti, totiž Prusko, Rusko a Rakousko-Uhersko. Centrální oblast Polska včetně Varšavy tehdy spadala do ruského záboru, tzv. Kongresovky. Klasické gymnázium (Szkoła Ziemi Mazowieckiej), které mladý Teitelbaum spolu se svým bratrem Václavem studoval, bylo kvalitní a Alfréd byl skvělým studentem. V určitém období se učil hned sedm jazyků najednou. Ruština byla vyučovacím jazykem, dále měl v rozvrhu němčinu, francouzštinu, řečtinu a latinu a hodiny polštiny pro polské studenty. Navíc měl ještě soukromé hodiny hebrejštiny. Logika, v níž později vynikl, ho nezaujala a neměl z ní ani jedničku, zato chtěl studovat na univerzitě biologii. Jenže Varšavská univerzita byla uzavřena a v hlavním městě fungovala pouze ruskojazyčná univerzita. Situace se však změnila po začátku první světové války. Rusové byli ze středního Polska vytlačeni a většinu země pak kontrolovalo Německo a Rakousko-Uhersko. Varšavská univerzita proto mohla být v r. 1915 opět otevřena. Profesory matematiky se tu stali Łukasiewicz a Mazurkiewicz. Alfréd Teitelbaum na univerzitu vstoupil v r. 1918 po krátké službě v polské armádě. Matematická škola na univerzitě rychle sílila, v roce 1919 získali profesorské místo Sierpinski a Leniewski. Posledně jmenovaný zveřejnil na svém semináři z teorie množin problém, který nebylo až tak těžké vyřešit, ale tento úspěch odlákal studenta od biologie k matematice. Teorie množin se pak stala první oblastí vědeckého zájmu A. Teitelbauma. Spolu s dalšími dvěma mladými matematiky S. Mazurkiewiczem a Z. Janiszevskim založil v r. 1919 časopis Fundamenta Mathematicae, věnovaný výhradně matematické logice a teorii množin. Jeho doktorská studia byla vedena Leniewskim. V roce 1924 absolvoval a získal doktorát a stal se nejmladší osobou, která kdy dosáhla doktorátu na Varšavské univerzitě. To už ale změnil jméno na Tarski, tedy na jméno, pod kterým ho zná odborná komunita a změnil i víru: od židovské konvertoval na římsko-katolickou. Bylo to v době vlny polského nacionalismu a zřejmě i doufal, že jeho univerzitní kariéra bude snazší. Uvidíme ovšem, že tomu tak nebylo.

Z roku 1924 pochází velice známý společný článek s Banachem o tom, co se dnes nazývá Banach-Tarského paradox. Ukazuje se, že při použití axiomu výběru lze kouli rozdělit na konečný počet částí a ty lze složit do koule o větším poloměru, nebo z těchto částí lze složit dvě koule o stejné velikosti, jakou má původní koule.

Tarski vyučoval logiku na polském Pedagogickém institutu ve Varšavě od r. 1922 do 1925, kdy byl jmenován docentem matematiky a

logiky na Varšavské univerzitě. Později se stal Łukasiewiczovým asistentem, ale toto univerzitní místo mu neposkytlo dostatek prostředků, takže byl nucen si vydělat na živobytí druhou prací. V r. 1925 se stal profesorem matematiky na eromského lyceu ve Varšavě. V červnu 1929 se Tarski oženil s Marií Witkowskou, která byla také učitelkou na eromského lyceu. Dva plné pedagogické úvazky musel zastávat až do r. 1939. Toto přetížení pedagogickou prací znamenalo i ztrátu některých odborných prvenství, kterých by byl býval patrně dosáhl. Nicméně z druhé strany se Tarského zájem přiblížil těm oblastem matematiky, které mají i dnes značný kontakt se středoškolskou výukou.

Toto konstatování se v plné míře týká hledání vhodné axiomatizace geometrie a též eliminace kvantifikátorů v tělese reálných čísel, což bude hlavní oblast našeho zájmu. Poznamenejme ještě, že v předválečné době sice vzrůstala Tarského mezinárodní reputace, ale jeho pokusy nalézt profesorské místo a tím i ekonomické zázemí zůstávaly neúspěšné.

Osud ale pomohl Tarskému alespoň zachovat holý život: v době vypuknutí druhé světové války byl shodou okolností na dvoutýdenním pobytu v USA. Vrátit domů se samozřejmě nemohl. Za války zahynuli jeho otec, matka, bratr a švagrová. S rodinou se mohl setkat až po válce, protože jeho pokusy zařídit s pomocí svých evropských přátel její vycestování neuspěly. Sám také dlouho nemohl najít ve Spojených státech odpovídající univerzitní post. Stálé místo získal až na Kalifornské univerzitě v Berkeley v r. 1942. Mimořádným profesorem se zde stal v r. 1945 a řádným profesorem matematiky v r. 1949. V Berkeley zůstal po zbytek své kariéry (emeritním profesorem se stal r. 1968). Vyučoval pak do r. 1973 a vedl doktorandy a výzkumné práce až do své smrti. (Více o této etapě Tarského života např. viz [5]).

Existuje výrok, podle něhož Tarski patří spolu s Aristotelem, Fregem a Gödelem mezi čtveřici největších logiků v lidských dějinách. Byl velice činorodý, uvádí se, že počet stran v jeho článcích se blíží 2 500. Viděli jsme, že se nejprve zabýval různými oblastmi teorie množin. V dalších obdobích svého života se věnoval i výrokové logice, logice prvního řádu a nekonečné logice, rozhodovacím problémům, sémantice, teorii modelů, univerzální algebře, booleovské algebře a teorii svazů, algebraické logice, teorii míry, základům a metamatematice geometrie.

Řekněme teď trochu precizněji, co budeme nazývat eliminací kvantifikátorů v tělese reálných čísel. Pracujeme ve struktuře $R = \langle \mathbb{R}, +, \cdot, 0, 1, < \rangle$ a můžeme tedy vytvářet formule v $x, y, z, \ldots$ pomocí operací sčítání, (odčítání) a násobení, jsou „povoleny" celočíselné koeficienty (vzniknou z konstant 0, 1) a smíme užívat symbolu $<$ a $=$ (jde o teorii s rovností),

a tedy i $>$, $\geq$, $\leq$. Prakticky to znamená, že můžeme zapisovat polynomiální rovnice a nerovnice a z nich vytvářet logické kombinace pomocí logických spojek. Proměnné obsažené v těchto formulích lze kvantifikovat ($\exists$, $\forall$). Ovšem kvantifikovat lze jen individuální proměnné pro reálná čísla, nikoli jejich soubory, jakými jsou kupř. intervaly či množina všech přirozených čísel. Tarski dokázal, že platí tato věta:

Věta 1: Nechť $G = (Q_{m+1}x_{m+1}) \ldots (Q_n x_n) \quad F(x_1, x_2, \ldots, x_n)$ je kvantifikovaná formule zapsaná v prenexním tvaru, v níž jsou proměnné $x_1, x_2, \ldots, x_m$ volné a proměnné $x_{m+1}, x_{m+2}, \ldots, x_n$ vázané (tj. Q_i, $i = m+1, \ldots, n$ značí buďto existenční kvantifikátor $\exists$ nebo obecný kvantifikátor $\forall$). $F(x_1, x_2, \ldots, x_n)$ je přitom logickou kombinací polynomiálních rovnic a nerovnic s celočíselnými koeficienty v proměnných x_1, $x_2, \ldots, x_n$. Pak existuje formule H v proměnných $x_1, x_2, \ldots, x_m$, která již neobsahuje kvantifikátory a která je ekvivalentní formuli G. (Tuto formuli i důkaz ekvivalence lze získat výhradně s využitím axiomů platných pro tzv. reálně uzavřená tělesa, což jsou uspořádaná tělesa, v nichž platí věta o střední hodnotě pro polynomy).

Matematičtí logici mají za to (ostatně Tarského vyjádření z předmluvy k [16] to potvrzuje), že právě uvedenou větu musel Tarski znát již v r. 1930. Bez ní by sotva mohl dokázat jistý důsledek o aritmeticky definovaných množinách na číselné ose (viz [12]).

Precizní formulaci a jasný náčrt důkazu „Tarského věty o eliminaci kvantifikátorů“ můžeme nalézt v práci **The completness of elementary algebra and geometry**, což byl dokument z roku 1940, jehož publikování přerušila válka. Zůstaly jen dva exempláře sloupcových korektur. Klíčovou záležitostí je zobecněná forma Sturmovy věty, totiž kritérium pro řešitelnost soustavy $f(X) = 0$, $g_1(X) > 0$, $\ldots$, $g_k(X) > 0$ s racionálními koeficienty u polynomů f, g_1, $\ldots$, g_k, kde $X = (x_1, x_2, \ldots, x_n)$ je množina reálných proměnných. (Připomeňme, že Sturmova věta z r. 1835 umožňuje zjistit počet reálných kořenů polynomu f jedné neurčité x s reálnými koeficienty v intervalu $\langle a, b \rangle$, kde $a < b$ jsou reálná čísla taková, že $f(a) \neq 0$ a $f(b) \neq 0$. Ovšem i Sturmova věta je završením linie vedoucí od Descartova znaménkového pravidla (1637) přes věty Budana (1807) a Fouriera (1831)). Dále je vhodné zařadit Tarského objev z r. 1930 do celkového kontextu budování „obecné“ algebry, v níž měla algebraická konstrukce tělesa reálných čísel důležité místo. Sem patří zejména výsledky libereckého rodáka E. Artina a O. Schreiera, týkající se uspořádaných těles, resp. reálně uzavřených těles (viz [1]).

Získaného výsledku si zřejmě Tarski ani nijak zvlášť necenil: „Re-

lativně omezený dosah této látky ukazuje, že je třeba opustit budoucí zkoumání na tomto poli a zejména úsilí vedoucí k zesílení výsledků předkládané práce."

Jak je z názvu patrné, Tarski se zde soustředil na důsledky, které obdržíme, když větu 1 použijeme na sentence, tj. na formule neobsahující parametry. Po provedení eliminace kvantifikátorů tak obdržíme „jednoduchou" formuli obsahující jen konstanty, o jejíž pravdivosti lze, jak Tarski rovněž ukázal, snadno rozhodnout. (Ostatně ukázku toho, jak takové vyhodnocení v programu Mathematica® 5.0 dnes vypadá, jsme viděli při „zjednodušení" formulí (1), (2), (3) na začátku tohoto článku). Tarski tak dokázal, že **teorie** $\langle \mathbb{R}, +, \cdot, 0, 1, < \rangle$ **je úplná**.

Tento velký výsledek zůstal vinou válečných událostí nepublikován. Tarski, jak již víme, přesídlil do Kalifornie. Druhou šanci k publikování svých fundamentálních objevů výsledku dostal za velice zajímavých okolností.

Po skončení období, kdy byl vědecký a průmyslový výzkum orientován na potřeby války, vyvstala v USA potřeba řešit problémy poválečného období. Tehdy se od firmy Douglas Aircraft v Santa Monica v Kalifornii projekt oddělil RAND a dne 14. 5. 1948 byla vytvořena nezávislá a nezisková organizace RAND Co. (**r**esearch **and** **d**evelopment). Měla podporovat vědecké, výzkumné a charitativní cíle pro veřejné blaho a bezpečnost USA. Její pracovníci studovali mnohé otázky přírodovědné, sociologické, z oblasti zdravotní péče, odstranění chudoby a úpadku městských čtvrtí atd. Zaměstnání tu našli také matematici a fyzikové a tak vznikly první ideje z oblasti telekomunikační techniky, možností vyslání umělých družic a též i návrhy prvních počítačů.

Prostřednictvím svého amerického přítele J. C. C. McKinseye, který zde byl zaměstnán, se Tarski rozhodl přepracovat svůj předválečný text. Vznikla tak práce [15]. Jak bylo naznačeno, začínala se již pociťovat možnost sestrojení počítače, kterému se tenkrát ještě říkalo rozhodovací stroj (decision machine). V úvodu ke druhému vydání své práce v r. 1951 Tarski píše:

„Rozhodovací metody ... byly předloženy systematickým a detailním způsobem, takže přinášejí možnost zkonstruování fungujícího rozhodovacího stroje. Další více teoretické aspekty diskutovaného problému byly pojednány méně důkladně a pouze v poznámkách."

Název práce **A decision method for elementary algebra and geometry** signalizuje, že otázek úplnosti se tu přechází k rozhodnutelnosti. Citujme opět z úvodu k druhému vydání: „Často jsme se zabývali nikoli sentencí elementární algebry, nýbrž podmínkou obsahující

parametry a, b, c, ... a formulovanou v termech elementární algebry; ... zajímali jsme se o její redukci do standardního tvaru, ve kterém se objevuje kombinace algebraických rovnic a nerovností v a, b, c, ... Rozhodovací metoda vyvinutá níže dává jistotu, že takováto redukce je vždy možná."

Tarski nebyl prvním, kdo užil eliminaci kvantifikátorů, to učinili již před ním Löwenheim, Skolem a Langford při analýze jednodušších teorií. Tarski z ní však vytvořil obecnou metodu a objevil, že v těch případech, kdy studovaná teorie připouští eliminaci kvantifikátorů, ji lze použít k hlubší analýze této teorie.

Celkově však lze říci, že i když šlo o velké vědecké výsledky, nebyly Tarského práce publikovány v matematiky nejvíce čtených časopisech. Nebyly tedy zprvu ani doceněny a lze říci, že ani známy v široké matematické komunitě. Dále, i přes výše naznačenou snahu otevřít cestu k jejich implementaci, k tomu nikdy nedošlo, protože Tarského metoda nemůže obstát z pohledu výpočetní složitosti. První zjednodušení nalezl Tarského kolega z Berkeley, A. Seidenberg, který publikoval v r. 1954 jiný důkaz Tarského výsledku v Annals of Mathematics, tedy v dostupnějším pramenu pro matematickou komunitu (viz [9]). (Začalo se pak dokonce hovořit Seidenbergově větě či o Tarského-Seidenbergově větě). Přesto však i po následujícím vylepšení (Cohen 1969) vše mělo význam pouze z pohledu teoretického.

Zásadní snížení výpočetní složitosti přinesla metoda **cylindrické algebraické dekompozice** (CAD), která byla navržena Georgem Collinsem (*10. 1. 1928 Iowa, USA) v r. 1973 (publikováno v r. 1975). Metoda CAD byla v pozdějších letech vylepšována zejména Hoon Hongem a byl vytvořen interaktivní program QEPCAD. Zásluhou prof. Christophera W. Browna nalezne zájemce bohatou dokumentaci o tomto programu na adrese *http://www.cs.usna.edu/~qepcad/B/QEPCAD.html.* O možném užití programu QEPCAD při řešení středoškolských úloh více v [7]. Naznačme stručně ideu CAD.

Příklad 1: Zjistěme, jakých znamének nabývá polynom

$$f(x) = x^4 - 3x^3 - 9x^2 + 23x - 12$$

na reálné ose, tj. určeme podmnožiny M_+, M_0, M_-, množiny reálných čísel takové, že $f(x) > 0$ pro všechna $x \in M_+$, resp. $f(x) = 0$ pro všechna $x \in M_0$, resp. $f(x) < 0$ pro všechna $x \in M_-$.

Řešení: Lze nahlédnout, příp. zjistit s využitím počítače, že

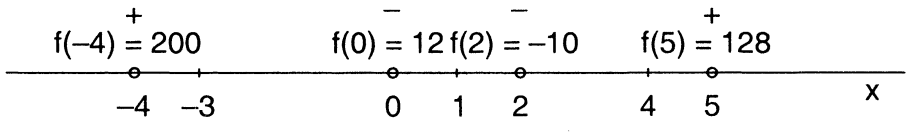
$$f(x) = (x+3)(x-1)^2(x-4).$$

Polynom f má tři reálné kořeny – 3, 1, 4, které si lze znázornit na číselné ose (viz obr.1). Přirozeným způsobem získáváme rozklad číselné osy na buňky (cell decomposition):

$$(-\infty,-3), \quad \{-3\}, \quad (-3,1), \quad \{1\}, \quad (1,4), \quad \{4\}, \quad (4,+\infty),$$

na kterých již má polynom f stálé znaménko sgn f. O znaménku polynomu $f(x)$ ve vzniklých otevřených intervalech lze rozhodnout výpočtem funkčních hodnot ve vhodně zvolených vnitřních bodech.

Vezměme kupř. testovací body $-4 \in (-\infty,-3)$, $0 \in (-3,1)$, $2 \in (1,4)$, $5 \in (4,\infty)$. (Testovací body jsou na obr. 1 znázorněny kroužky). Je $f(-4) = 200$, $f(0) = -12$, $f(2) = -10$, $f(5) = 128$.



Obr. 1

Můžeme učinit závěr, že polynom f nabývá kladných hodnot pro

$$x \in M_+ = (-\infty,-3) \cup (4,+\infty),$$

nulových pro

$$x \in M_0 = \{-3\} \cup \{1\} \cup \{4\},$$

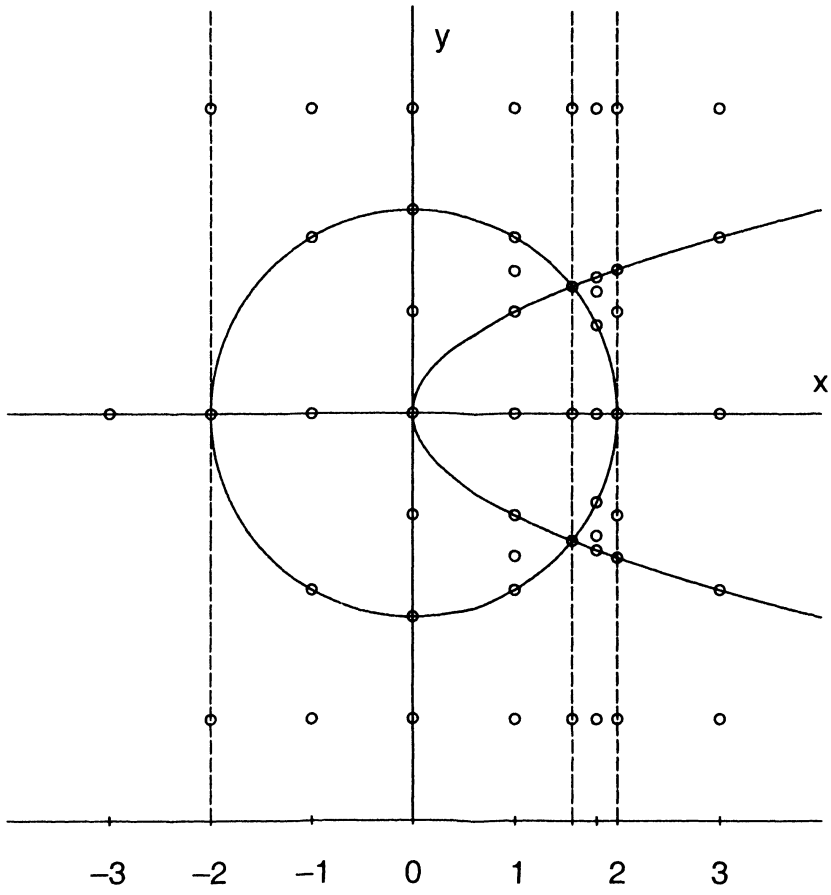
záporných hodnot pro

$$x \in M_- = (-3,1) \cup (1,4).$$

Poznamenejme, že tato technika je v případě rozkladu reálné osy dobře známa. Není ale zdaleka tak jasné, jak postupovat ve vyšší dimenzi.

Příklad 2: Pomocí metody cylindrické algebraické dekompozice nalezněme formuli ekvivalentní s formulí $(\exists y)\ [x^2 + y^2 \leq 4 \ \wedge \ y^2 \geq x]$.

Řešení: Naznačíme (a budeme přitom sledovat obr. 2), jak lze tento úkol zvládnout.



Obr. 2

Pracujeme s polynomy $P_1(x,y) = x^2 + y^2 - 4$, $P_2(x,y) = y^2 - x$. Provedeme projekci do osy x, přičemž si zvláště všímáme bodů, v nichž mají křivky o rovnicích $P_1(x,y) = 0$, $P_2(x,y) = 0$ tečny rovnoběžné s osou y, resp. průsečíků těchto křivek. Tyto body mají x-ovou souřadnici $x = -2,\ 0,\ \frac{-1+\sqrt{17}}{2} = p,\ 2$. (I když vše můžeme sledovat na obr. 2, lze tyto body nalézt čistě algebraicky pomocí rezultantů a diskriminantů). Tím zároveň obdržíme rozklad reálné osy na následující 1D buňky:

$$(-\infty,-2),\quad \{-2\},\quad (-2,0),\quad \{0\},\quad (0,p),$$

$$\{p\},\quad (p,2),\quad \{2\},\quad (2,+\infty).$$

Uvnitř těchto buněk si zvolíme testovací body, např. -3, -2, -1, 0, 1, p, $\frac{9}{5}$, 2, 3. Tyto body (= algebraická čísla) tvoří pro reálnou osu tzv. cylindrický algebraický vzorek (cylindrical algebraic sample, CAS). Nyní se chceme vrátit do roviny a sestrojit rekurzivně odpovídající CAS v $\mathbb{R}^2$.

Představíme si, že nad každou 1D buňkou b_i je vybudován válec $b_i \times \mathbb{R}$. Tento válec je ještě rozdělen na 2D buňky tak, že v kterékoli z nich mají polynomy P_1, P_2 konstantní znaménko. Kupř. množina $(-\infty, -2) \times \mathbb{R}$ tvoří jedinou buňku a v ní můžeme zvolit testovací bod $[-3, 0]$. Válec $\{-2\} \times \mathbb{R}$ („přímku") rozdělíme na tři buňky $\{-2\} \times (-\infty, 0)$, $[-2, 0]$ a $\{-2\} \times (0, +\infty)$. V těchto buňkách si zvolíme testovací body: $[-2, -3]$, $[-2, 0]$, $[-2, 3]$.

Válec $(-2, 0) \times \mathbb{R}$ je rozdělen na pět 2D buněk: vždy je $x \in (-2, 0)$ a navíc je postupně

$$y < -\sqrt{4 - x^2}, \quad y = -\sqrt{4 - x^2}, \quad -\sqrt{4 - x^2} < y < \sqrt{4 - x^2},$$

$$y = \sqrt{4 - x^2}, \qquad y > \sqrt{4 - x^2}$$

(viz obr. 2). Zbývá zvolit pět testovacích bodů do CAS. Protože ale v 1D buňce $(-2, 0)$ jsme si již předtím zvolili testovací bod -1, je jejich první souřadnice již určena. Vezměme proto body $[-1, -3]$, $[-1, -\sqrt{3}]$, $[-1, 0]$, $[-1, \sqrt{3}]$, $[-1, 3]$.

Teď je již zřejmé, jak by se zkonstruoval CAS v $\mathbb{R}^2$. V obr. 2 byly ještě vzaty body

$[0, -3], [0, -2], [0, -1], [0, 0], [0, 1], [0, 2], [0, 3],$

$[1, -3], [1, -\sqrt{3}], \left[1, -\frac{7}{5}\right], [1, -1], [1, 0], [1, 1], \left[1, \frac{7}{5}\right], [1, \sqrt{3}], [1, 3],$

$[p, -3], [p, -\sqrt{p}], [p, 0], [p, \sqrt{p}], [p, 3],$ kde $p = \frac{-1+\sqrt{17}}{2}$,

$\left[\frac{9}{5}, -3\right], \left[\frac{9}{5}, -\frac{3\sqrt{5}}{5}\right], \left[\frac{9}{5}, -\frac{6}{5}\right], \left[\frac{9}{5}, -\frac{\sqrt{19}}{5}\right], \left[\frac{9}{5}, 0\right], \left[\frac{9}{5}, \frac{\sqrt{19}}{5}\right], \left[\frac{9}{5}, \frac{6}{5}\right], \left[\frac{9}{5}, \frac{3\sqrt{5}}{5}\right], \left[\frac{9}{5}, 3\right],$

$[2, -3], [2, -\sqrt{2}], [2, -1], [2, 0], [2, 1], [2, \sqrt{2}], [2, 3],$

$[3, -3], [3, -\sqrt{3}], [3, 0], [3, \sqrt{3}], [3, 3].$

V bodech tohoto vzorku bychom my nebo raději počítač zkontrolovali splnění podmínek $P_1(x, y) \leq 0$, $P_2(x, y) \leq 0$. Tím by se zároveň rozhodlo o jejich platnosti v celé buňce. A protože naše původní formule měla tvar $(\exists y)\ [P_1(x, y) \leq 0 \ \wedge \ P_2(x, y) \leq 0]$, je třeba najít takové buňky b_i na ose x, že ve válci $b_i \times \mathbb{R}$ se nachází alespoň jedna 2D buňka, v níž současně platí $P_1(x, y) \leq 0$, $P_2(x, y) \leq 0$. Zjistíme tak nakonec, že $0 \leq x \leq 2$, tj. zadaná formule je ekvivalentní s formulí $\varphi(x) \sim x \geq 0 \ \wedge \ x \leq 2$. Stejný výsledek obdržíme i v programu Mathematica® verze 5.0:

```
Resolve[Exists[y, x^2 + y^2 <= 4 && y^2 <= x ]]
```

$0 \leq x \leq 2$

Pro podrobný popis metody odkažme čtenáře na [18]. Obecně probíhá metoda válcové algebraické dekompozice v následujících fázích:

1. normalizační fáze (polynomy P_i se faktorizují, resp. normalizují)
2. projekční fáze
3. fáze „zdvižení“
4. konstrukce formule φ (sestavení otevřené, tj. kvantifikátory neobsahující formule)

Z předchozí ukázky bylo zřejmé, v čem je Achillova pata metody. Zranitelným místem je zejména výpočetní složitost, která je mj. dvojnásobně exponenciální v počtu proměnných. (Uvědomme si jen, jak by se zkomplikoval výpočet pro formuli obsahující tři proměnné x, y, z. Museli bychom postupně realizovat dvě projekce (tj. nejprve kupř. eliminovat z, pak y), přičemž by obecně podstatně vzrostl počet buněk, stupně polynomů, komplikace s případnými reálnými kořeny polynomů vyšších stupňů atd.). Je proto nezbytné minimalizovat počet proměnných ještě před zahájením výpočtu, což někdy lze dosáhnout vhodnou substitucí, změnou systému souřadnic atd. Nepříjemné a časově velmi náročné mohou být výpočty v algebraických rozšířeních tělesa racionálních čísel (v našem ilustračním případě k těmto problémům vede výskyt čísla $\frac{-1+\sqrt{17}}{2} = p$, ale obecně může být nutné pracovat s reálnými kořeny polynomů vyšších stupňů a tyto kořeny separovat, tj. mít k dispozici interval s racionálními koncovými body, v němž tento kořen leží. Zaokrouhlovat ve výpočtech však nelze). Metoda cylindrické algebraické dekompozice samozřejmě není všemocná, může se velice snadno stát, že zdánlivě jednoduchá úloha nebude řešitelná v rozumném čase.

Z druhé strany jsme však získali pozoruhodný pohled na vlastnosti tělesa reálných čísel, které je zřejmě nejpoužívanější matematickou strukturou. Určité úlohy středoškolské či vysokoškolské matematiky mohou být zvládnutelné. Některé ukázky výpočtů v programu QEPCAD nalezne čtenář v [7]. Může jít např. o problémy vyžadující řešení algebraických nerovnic a jejich soustav, příp. můžeme dokonce získat počítačové důkazy jednodušších vět.

Závěrem ještě předveďme několik výpočtů v Mathematica® 5.0, kde je mj. nově implementován povel **CylindricalDecomposition**. Poznamenejme ještě, že při zápisu formulí lze v tomto programovém balíku užít i odmocniny a funkci **Root**. Zařazujeme variaci na příklad 2, aby čtenář mohl sledovat integrační oblast na obr. 2.

```
CylindricalDecomposition
                [{x^2 + y^2<=4, y^2<=x, y>=0},{x,y}]
```

x == 0 && y == 0 || 0 < x ≤ $\frac{1}{2}(-1+\sqrt{17})$ && 0 ≤ y ≤ $\sqrt{x}$ ||
$\frac{1}{2}(-1+\sqrt{17})$ < x < 2 && 0 ≤ y ≤ $\sqrt{4-x^2}$ || x == 2 && y == 0

Připomeňme si problematiku výpočtu dvojného integrálu (integrace přes oblast zadanou algebraickými nerovnostmi) a Fubiniovu větu. Míru rovinného útvaru vymezeného podmínkami $x^2+y^2 \leq 4$, $y^2 \leq x$, $y \geq 0$ spočteme v Mathematica® 5.0 jako součet dvou dvojnásobných integrálů následovně:

```
Integrate[1,x,0,1/2*(-1+Sqrt[17]),y,0,Sqrt[x]] +
+ Integrate[1,x,1/2*(-1+Sqrt[17]),2 , y,0,
Sqrt[4-x^2]]
```

Novinkou je, že po zadání

```
Integrate[Boole[x^2 + y^2<=4 && y^2<=x && y>=0],
{x,-∞,∞}, {y,0,∞}]
```

dostaneme stejný a dosti komplikovaný výsledek. Tentokrát však byla veškerá práce s nalezením mezí a užitím Fubiniovy věty předána počítači.

Literatura

[1] Artin, E., Schreier, O., *Algebraische Konstruktion reeller Körper*, Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität, vol. **5**, 83–99.

[2] Caviness, B. F., Johnson, J. R., editors., *Quantifier Elimination and Cylindrical Algebraic Decomposition.* Texts and Monographs in Symbolic Computation. Springer-Verlag, 1998.

[3] Collins, G., E., *Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition.* Lecture Notes on Computer Science, **33** (1975), 134–183.

[4] Davenport, J. H., Heintz, J., *Real quantifier elimination is doubly exponential.* Journal of Symbolic Computation, 5–35, 1997.

[5] Givant, S. R., *Portrét Alfréda Tarského*, Pokroky MFA, **4** (1992), 185–205.

[6] Givant, S. R., *Unifying Threads in Alfred Tarski's Work, Math.* Intelligencer **21**/1, (1999), 47–58.

[7] Hora, J., Pech, P., *Využití programu QEPCAD při řešení středoškolských úloh obsahujících parametry.* Učitel matematiky, **12** (2003), 31–38.

[8] Mishra, B., *Algorithmic Algebra.* Springer-Verlag, New York, Inc., 1993.

[9] Seidenberg, A., *A New Decision Method for Elementary Algebra.* Annals of Math. II. ser. 60, 365–374, 1954.

[10] Strzebonski, A., *Solving Algebraic Inequalities.* The Mathematica Journal 7, 525–541, 2000.

[11] Švejdar, V., *Logika: neúplnost, složitost a nutnost.* Academia, Praha, 2002.

[12] Tarski, A., *Über definierbare Mengen reeller Zahlen,* Rocznik Polskiego Towarzystwa Matematycznego, vol. 9, 206–207. (Abstrakt práce [13].)

[13] Tarski, A., *Sur les ensembles définissables de nombres réeles. I,* Fundamenta Mathematicae 17, 210–239, 1931. (Anglický překlad je zařazen jako Article VI v [17]).

[14] Tarski, A., *The completeness of elementary algebra and geometry,* Institut Blaise Pascal, Paris, (1967) iv+50pp. (Reprint pořízený ze stránkových korektur práce, která měla vyjít v r. 1940 v Actualités scientifiques et industrielles, Hermann & Cie, Paříž, ale jejíž vydání se neuskutečnilo vzhledem k válečným podmínkám.)

[15] Tarski, A., *A Decision Method for Elementary Algebra and Geometry.* (prepared for publication by J. C. C. Mc Kinsey), U. S. Air Force Project RAND, R-109, the RAND Corporation, Santa Monica, California, (1948) iv + 60pp.

[16] Tarski, A., *A Decision Method for Elementary Algebra and Geometry.* University of California Press, Berkeley, 1951. second ed., rev. (Přetištěno ve [2].)

[17] Tarski, A., *Logic, semantics, metamatematics.* Claredon Press, Oxford, 1956.

[18] Winkler, F., *Polynomial Algorithms in Computer Algebra,* Springer Verlag, Wien, 1996.

Příprava textu byla podpořena grantem FRVŠ F6 1371 (2004) *Počítačové dokazování matematických vět a jeho didaktické aplikace.*

Jaroslav Hora
Katedra matematiky FPE ZČU Plzeň
e-mail: horajar@kmt.zcu.cz