Jeden za osmnáct a druhý bez dvou za dvacet
aneb Výhody a nevýhody záporných cifer

Jakub Lukeš; Martina Bekrová
Gymnázium Českolipská 737, Praha 9; Gymnázium Trutnov
Lukes.Jakub@gmail.com; To.Zapomenu@gmail.com

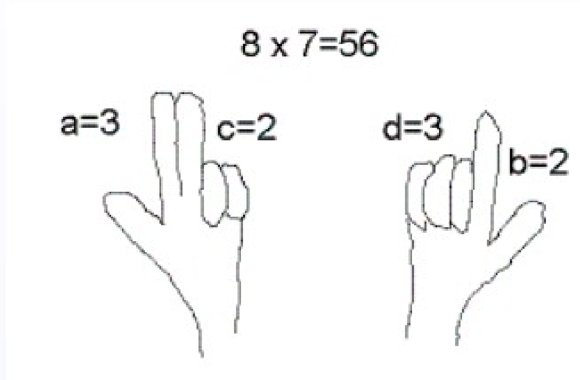
Abstrakt:
Už v šedesátých letech Algirdas Avižienis navrhl algoritmus pro paralelní sčítání v redundantních soustavách se zápornými ciframi. Cílem našeho projektu byl právě program umožňující 1) konverzi čísel z desítkové soustavy do redundantní desítkové soustavy se zápornými ciframi a naopak 2) provádějící Avižienisův algoritmus paralelního sčítání. Takový algoritmus může výrazně šetřit čas a skutečně se v současné době čím dál více algoritmy tohoto typu využívají.

1 Historie užití záporných cifer v zápisu přirozených čísel

Už od první třídy základní školy umíme počítat v desítkové soustavě s ciframi od nuly do devíti. Pokud připustíme více cifer, např. z množiny {-9, … , 0, … , 9}, pak číslo osmnáct má dva různé zápisy: 18 = 2(-2), kde zápis 2(-2) znamená $2\times10^1 - 2\times10^0$. Soustavám, které připouští nejednoznačné zápisy čísel, říkáme *redundantní*. I v soustavách, které připouští záporné cifry, mohou být zápisy čísel jednoznačné, např. v balancované desítkové soustavě, kde cifry bereme z množiny {-4, … , 0, ... , 5}. Pro násobení přirozených čísel v této soustavě nám stačí malá násobilka.

První, kdo si uvědomil tuto výhodu, byl anglický profesor matematiky John Colson (1680-1760), který využíval záporných cifer k urychlení aritmetických operací, nejen násobení. Profesor Colson nebyl jen vynikajícím matematikem, spíše je známý jako překladatel (angličtina, latina, italština, francouzština). Jeho nejvýznamnějším počinem je překlad Newtonova díla z latiny do angličtiny, cenným přínosem byly jeho vysvětlující komentáře. Zasadil se také o zpřístupnění počtů ženám ve viktoriánské Anglii, kde něžné pohlaví nesmělo navštěvovat školy.
I vynikající matematik francouzského původu Augustin Louis Cauchy (1789-1857) využíval záporných cifer s cílem předcházet chybám ve výpočtech. Ačkoli o jeho charakteru nekolují nejlepší zvěsti, jeho přínos matematice je nepopiratelný. Jeho Cours d´analyse (1821), ve kterém sepsal své přednášky z Ecole Polytechnique, je dodnes základem vysokoškolské matematické analýzy. Byl také plodným pisatelem matematických článků. Ve své době byl se 789 publikacemi téměř nepřekonatelný (více pouze Euler a Caley).

Výhod záporných cifer, ač nevědomky, využívali již středověcí obchodníci. Dochovaly se záznamy o tzv. cikánské násobilce, která se znalostí malé násobilky umožňovala násobit větší čísla. Její princip pochopíte z následujícího obrázku:



vztyčené prsty a, b
schované prsty c, d

$$\begin{aligned}(10 - c)(10 - d) &= 100 - (c + d)10 + cd \\ &= 10(10 - c - d) + cd \\ &= 10(a + b) + cd\end{aligned}$$

Pokud chceme násobit například 8×7, tak se zeptáme: Osm a kolik je deset? A dva. Schováme dva prsty na jedné ruce. To samé uděláme s číslem sedm. Na pozici desítek napíšeme součet vztyčených a na pozici jednotek součin schovaných prstů.

Dále se budeme zabývat využitím zápisu čísel pomocí záporných cifer v dnešní době.

2 Redundantní aritmetika

Binární soustava

Všechny moderní počítače používají k výpočtům binární soustavu. V této soustavě je násobení čísel prakticky jejich sčítáním, jak ukazuje následující obrázek, ve kterém násobíme 11×5.

		1	0	1	1
			1	0	1
		1	0	1	1
	0	0	0	0	
1	0	1	1		
1	1	0	1	1	1

Rychlost této operace je přímo úměrná počtu jedniček v násobiteli. Průměrný počet nul v klasickém binárním zápisu je 1/2. Pokud připustíme v binární soustavě cifry -1, 0, 1, pak existují přirozená čísla, která mají více možných zápisů. Např. číslo 31 lze napsat jako 1111 a 1000(-1). Když z možných zápisů vybereme ten s maximálním počtem nul, pak průměrný počet nul zvýšíme na 2/3. Z tohoto důvodu je výhodné násobení v redundantní binární soustavě.

Avižienisův algoritmus

Kromě násobení je nespornou výhodou redundantních soustav také možnost paralelního sčítání. Při klasickém sčítání se objevuje „carry“ – přenos jedničky, který znemožňuje provádět sčítání na každé pozici nezávisle na ostatních (viz. 9999 + 1). Francouzský matematik Frédéric Mazenc dokázal, že každý algoritmus pro paralelní sčítání vyžaduje redundantní soustavu. S prvním takovým algoritmem přišel litevský matematik Algirdas Avižienis. Jeho algoritmus je použitelný pro soustavy s bází $b \geq 3$ a ciframi od $-a$ do a, kde $a \leq b - 1$; $2a \geq b + 1$. Součet $s_{n+1}s_n\ldots s_1s_0$ čísel $x_n\ldots x_1x_0$ a $y_n\ldots y_1y_0$ se získá $s_i = w_i + t_i$, kde:

$$t_{i+1} = \begin{cases} -1 & \text{pro } x_i + y_i \leq -a \\ +1 & \text{pro } x_i + y_i \geq a \\ 0 & \text{pro } -a < x_i + y_i < a \end{cases}$$

$$w_i = x_i + y_i - bt_{i+1}$$

$$t_0 = 0 = w_{n+1}$$

My jsme se zabývali implementací tohoto algoritmu pro bázi b = 10 a a = 6, což je v tomto případě nejmenší možná hodnota a, která vyhoví výše uvedeným podmínkám. Součet čísel 4765 a 2672, které mají v redundantní desítkové soustavě popořadě zápisy 5(-2)(-4)5 a 3(-3)(-3)2, se pomocí tohoto algoritmu vypočítá následovně:

i	4	3	2	1	0
x_i		5	-2	-4	5
y_i		3	-3	-3	2
$x_i + y_i$		8	-5	-7	7
t_{i+1}		1	0	-1	1
w_i	0	-2	-5	3	-3
s_i	1	-2	-6	4	-3

Pro použití tohoto algoritmu potřebujeme převádět čísla z desítkové do redundantní soustavy a naopak podle následujícího příkladu:

- chceme zapsat 1723 v redundantní soustavě

$$1723 + 6666 = 8389$$

$$8 - 6 = 2 \quad 3 - 6 = -3 \quad 8 - 6 = 2 \quad 9 - 6 = 3$$

výsledek: $2(-3)23$

- chceme zapsat $2(-3)23$ ve standardní desítkové soustavě

$$2023 - 300 = 1723$$

Paralelní algoritmus sčítání existuje i pro binární redundantní soustavu s ciframi -1, 0, 1.

Výhody a nevýhody záporných cifer

PC s redundantní binární soustavou prozatím neexistují, protože zápisy pomocí záporných cifer mají pár „malých“ nevýhod. Kladou větší požadavky na paměť, nejednoznačnost zápisu způsobuje pomalejší porovnávání čísel a konverze je časově náročná (odpovídá náročnosti klasického sčítání). Výhoda paralelních aritmetických operací se projeví v momentě, kdy jich bude nutné provést větší počet. Proto v praxi existují speciální počítače, které neprovádí operace pomalé v redundantní soustavě, a také tzv. černé skříňky, které jsou součástí PC, vstupní a výstupní data se jim zadávají v klasickém formátu, ale výpočty provádějí v redundantní soustavě.

3 Budoucnost záporných cifer

První paralelní algoritmy se objevili koncem 70. let. Poté se dostaly do centra zájmu mnoha informatiků. Ménissier vytvořila knihovnu programů pro spolupráci s reálnými čísly s libovolnou přesností založenou na redundantní aritmetice (součást programovacího jazyka CAML). Tagaki a spol. v roce 1985 vyvinuli výkonný násobič (aplikace v šifrování). Müller a spol. programují „černé skříňky“ pro výpočet funkcí sin, cos, tg, cotg, exp, log, arctg pouze s využitím paralelního sčítání a dělení násobky dvou (což je jen posouvání binární zlomkové čárky). A z tohoto všeho plyne, že v budoucnosti se jistě ještě setkáme s redundantní aritmetikou.

Poděkování

Paní Ing. Balkové Lubomíře, Ph.D. a Prof. Ing. Pelantové Editě,CSc., které si s námi daly tu velkou práci a protáhly nás touto problematikou během jednoho dne.

A samozřejmě panu Ing. Vojtěchu Svobodovi, CSc., který společně s Monikou Mikšovskou pro nás tento, fyzikou a matematikou nabitý, týden zorganizovali.

A také Vám čtenářům, že jste vůbec ten sborník otevřeli. ☺

Reference:

[1] MÜLLER, J. M.: *Ordinateurs en quete d’arithmetique*, La Recherche, 1995 , Vol 26

[2] BAJARD, J. C. – MÜLLER, J. M.: *Calcul et arithmetique des ordinateurs* Hermes 2004