Počítačové algebraické systémy

J. Dvořák, M. Hanzík, M. Honek, R. Koběrský, J. Kuchyňka, Z. Sýkora
FJFI ČVUT, Trojanova 13, Praha 2
martin.hanzik@gmail.com

Abstrakt:

Počítačové algebraické systémy se vyvíjí už několik desetiletí. Jejich masovému rozvoji donedávna bránila jejich příliš vysoká cena, avšak v poslední době jejich funkci přejímají i některé kalkulačky za necelých tisíc korun. Některé programy jsou placené, ale jejich cena není tak vysoká jako dříve. Existuje řada těchto systémů jako aplikace na osobní počítače vydávaná pod freeware licencí a dokonce jsou i internetové aplikace bez nutnosti instalace. Zjednodušuje se také jejich ovladatelnost a přístup k průvodcům těmito systémy.

Na některé počítačové algebraické systémy jsme se zaměřili a nastínili vám jejich možnosti v tomto dokumentu.

1 Úvod

Rozhodli jsme se porovnat nám dostupné počítačové programy k řešení algebraických problémů. Programy které budeme porovnávat jsou Mathematica, Maple a webová databáze WolframAlpha.

Metoda porovnávání nebude nijak složitá. Vybereme několik ne zrovna jednoduchých funkcí a jejich grafy vytvoříme v už zmíněných algebraických systémech. Porovnávat budeme zejména schopnost vyřešit tyto funkce, jednoduchost práce se systémy a samozřejmě také dostupnost.

2 Co to jsou PAS?

Počítačové algebraické systémy (PAS) jsou určeny především k řešení matematických problémů. Stejně tak jako matematik systémy PAS ovládají pravidla algebry a matematické analýzy, které se učíte ve škole. PAS například umí řešit rovnice, zjednodušovat výrazy, počítat derivace či integrály a kreslit grafy. PAS pracují přímo se symboly, kterými jsou např. rovnice tvořeny, což znamená, že zachovávají obecnost tak dlouho, dokud nepotřebujeme číselnou odpověď. PAS umí vykreslovat nejen grafy dvojrozměrné či trojrozměrné, ale také v nich lze tvořit pokročilejší grafiku, jako např. animace, pole vektorů, parametrické křivky nebo dynamické systémy.

3 Mathematica

Mathematica představuje po dvacetiletém vývoji světově nejznámější programový systém pro provádění numerických a symbolických výpočtů a vizualizaci dat. Znamená zásadní průlom, který velkou měrou rozšíří možnosti a aplikovatelnost Mathematiky - umožňuje řešit projekty libovolného rozsahu od rutinních výpočtů až po velkosystémová řešení - a tím změnit naše dosavadní myšlení o výpočtech.

Klíčovými rysy nové verze Mathematica jsou automatizované numerické a symbolické výpočty, účinná adaptivní vizualizace, dynamická interaktivita a vysoce výkonné programovací prostředí.

Díky tomu nachází Mathematica široké uplatnění zejména v oblasti vědecko-technických výpočtů, statistickém zpracování dat, finančním managementu atd.

Práce s Mathematicou

I když syntaxe Mathematicy neni příliš intuitivní, se základní znalostí pojmů (a hlavně technické angličtiny) je možné s tímto programem jednoduše pracovat. Dokumentace je velmi kvalitní, takže pokud neznáte syntax žádných programovacích jazyků, kterým se jazyk Mathematicy podobá, není těžké začít zpracovávat matematické problémy s použitím zápisů a znaků, které nás vyučují ve škole. Navíc je možné použít syntaktický procesor Wolfram Alpha a zapisovat příkazy stejným způsobem – prostou angličtinou, pomocí internetu jsou převedeny na syntax Mathematicy.

4 Maple

Program *Maple* slouží k matematickým výpočtům, k simulacím (matematickým, fyzikálním, chemickým apod.) a k programování převážně matematických algoritmů. Hlavní nasazení programu Maple je v řešení soustav matematických rovnic a výrazů. Výsledkem těchto výpočtů mohou být vzorce, výsledná hodnota nebo graf. Pro všechny tyto možnosti je Maple dobře uzpůsoben.

Maple lze také s úspěchem využít pro řešení numerických příkladů. Zde se projeví takové možnosti, jako velký rozsah a přesnost zobrazení reálných čísel, možnost zobrazení výsledků pomocí zlomků, odmocnin a symbolických konstant. To je veliký rozdíl oproti jiným programům, které se pro tento účel také používají, ale číselný rozsah je přímo dán velikostí datových typů matematického koprocesoru (z těchto programů jmenujme například Excel firmy Microsoft).

Práce s Maple

Maple se ve svých možnostech hodně blíží Mathematice, v některých věcech, jako například v počtu možných funkcí, ji o hodně předbíhá. Syntax, kterou používá je jiná, blíží se více tůzným programovacím jazykům. S těmito jazyky má také lepší propojení a lépe pracuje s externími programy.

5 WolframAlpha

Wolfram Alpha je v současné době asi nejlepší online nástroj pro matematické výpočty, naleznete ho na adrese wolframalpha.com. Celé prostředí je v angličtině, ale obyčejně stačí do vstupního pole vepsat výraz, který chcete vypočítat a Wolfram Alpha už si s tím nějak poradí. Hodí se znát pár klíčových slov, jako že když chcete derivovat, stačí před výraz napsat „derive“.

Práce s WopframAlpha

První čeho si na WolframAlpha všimnete je, že spíš vypadá jako vyhledávač než algebraický systém. Je to svým způsobem pravda, WolframAlpha má obrovskou databázi ve které lze vyhledávat různé údaje o populaci, počasí, velkých firmách nebo třeba fyzikálních jevech. Řešení algebraických úkolů je taková třešnička na dortu, avšak má obrovskou výhodu proti ostatním algebraickým sytémům. WolframAlpha nemá striktní syntaxi, takže můžete psát naprosto intuitivně a tento program vám s největší pravděpodobností porozumí.

6 Výsledky

Program	Výhody	Nevýhody
Mathematica	kvalitnější optimalizace, větší možnosti grafického zobrazení, možnost použití angličtiny jako syntaxe (pomocí WolframAlpha)	placená licence
Maple	lepší numerický model, export do více programovacích jazyků	placená licence
WolframAlpha	snadná ovladetelnost, přístup odkukdoli z internetu, velká databáze a spousta dalších možností a využití	nedosahuje stejného výkonu

7 Diskuse

Podle výsledků můžeme tyto programy rozdělit na dvě části. Do první, pro nás zajímavější, bude patřit WolframAlpha. Tento program je zdarma přístupný odkudkoli z internetu, z toho vyplývá, že kdokoli má zájem, tak může s tímto porgramem pracovat. To podpoří i fakt, že práce s ním je velmi jednoduchá a intuitivní, navíc má mnoho dalších možností, než jen algebru.

Zbylé dva programy zařadíme do další skupiny, ty se vyznačují zejména striktní syntaxí a placenou licencí, což lajkům znemožňuje práci s nimi. Tyto programy jsou tedy vhodné spíše pro pokročilé. Mají mnohem více možností v algebraických operacích.

8 Shrnutí

Algebraické systémy jsou programy vytvořené pro řešení symbolických výpočtů. Existují už relativně dlouhou dobu, ale staly se využívanější a populárnější z důvodu snížení cen. Setkali jsme se s programy Mathematica, Maple a WolframAlpha. Nejznámějším z nich je Mathematica, která se využívá pro provádění numerických a symbolických výpočtů a vizualizaci dat. Na ni navazuje WolframAlpha, jakožto jednoduchý online nástroj, pracující na základě své ohromně rozsáhlé databáze. Maple je využíván převážně pro řešení matematických simulací, rovnic a k programováni matematických algoritmů.

9 Poděkování

Děkujeme panu Dr. Ing. Milanu Šiňorovi za vysvětlení problematiky počítačových algebraických systémů a všem organizátorům Týdne vědy na Jaderce.

10 Reference

http://www.matweb.cz/nastroje

https://wiki.metacentrum.cz/wiki/Mathematica

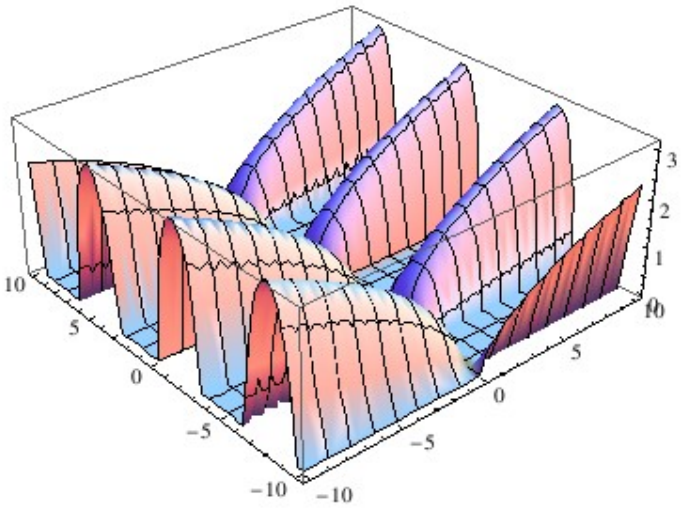
http://www.mathematica.cz/produkty.php?p_mathematica

http://www.fit.vutbr.cz/~tisnovpa/vyuka/PP1/maple/start.htm

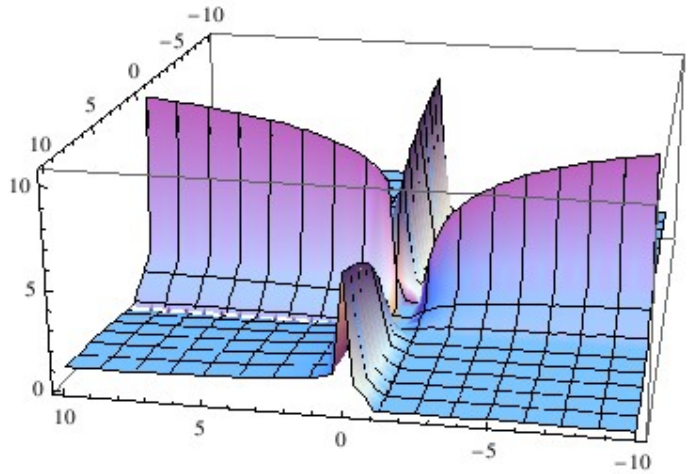
11 Příloha

Mathematica

```
Plot3D[Re[Sqrt[x Sin [y]]], {x, -10, 10}, {y, -10, 10}]
```

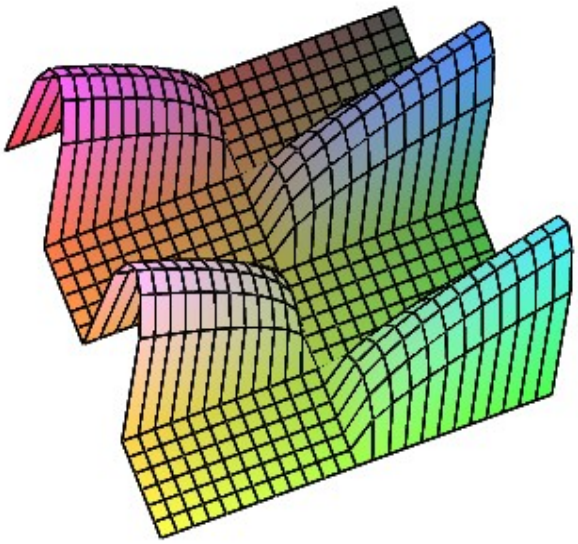



```
Plot3D[Re[Sqrt[(1 - Log[y]) Log[-x]]], {x, -10, 10}, {y, -10, 10 }]
```

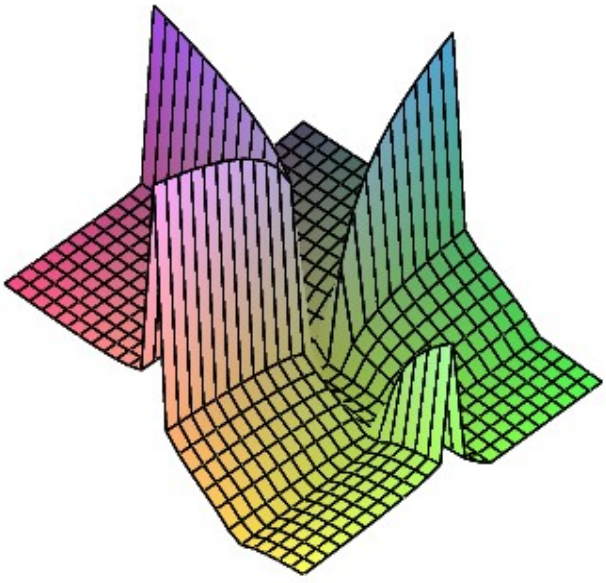


Maple

$f := \mathrm{Re}(\mathrm{sqrt}(x \cdot \sin(y))) \rightarrow$



$f := \mathrm{Re}(\mathrm{sqrt}((1 - \ln(y)) \cdot \ln(-x))) \rightarrow$



WolframAlpha

Wolfram

f(x,y)=√(x*sin(y)

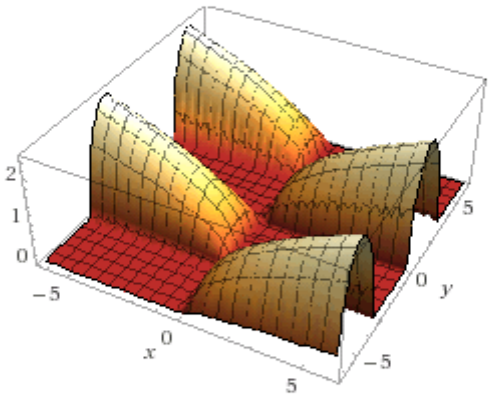
An attempt was made to fix mismatched parentheses, brackets, or braces.

Input:

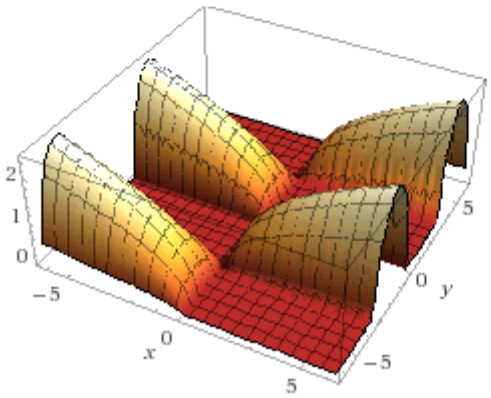
$$f(x, y) = \sqrt{x \sin(y)}$$

3D plots:

Real part:



Imaginary part:



Wolfram

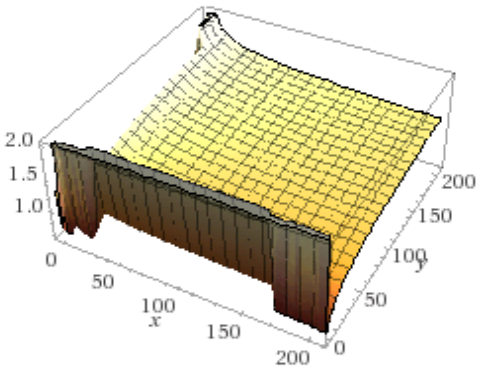
f(x,y)=√((1-lny)*ln(-x))

Input:

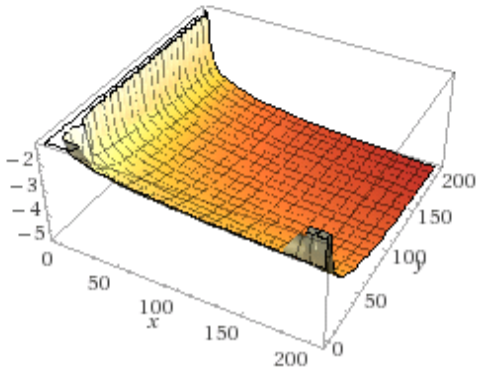
$$f(x, y) = \sqrt{(1 - \log(y)) \log(-x)}$$

3D plots:

Real part:



Imaginary part:



RSA šifrování v programu Mathematica-J. Dvořák

Princip RSA šifrování je založen na asymetrickém šifrovování s veřejným klíčem . Jedná se o jeden z nejpoužívanějších algoritmů současnosti v oblasti bezpečných komunikací. Používá se zejména ve finančnictví, ale nepoužívá se pro běžné šifrování, např. přenos po síti, protože tato metoda je mechanicky i časově náročná. Používá se i pro elektronické podpisy.

Bezpečnost RSA je postavena na předpokladu, že neexistuje efektivní způsob faktorizace součinu velkých prvočísel, bezpečnost je de facto neprolomitelná v rozumném čase, bez pořádné procesorové síly, jíž v dostatečné síle nedisponuje nejspíš nikdo. Tato metoda šifrování se také opírá o dělení se zbytkem.

Ukážeme si princip na jednoduchém příkladu. Nejdříve vygenerujeme nějaká dvě prvočísla p a q, v praxi se vyskytují prvočísla o počtu cifer kolem 100: *p=31 a q=43*. Poté vypočítáme součin čísel *n*: *n=p*q=1333* a dopočítáme Eulerovu charakteristiku: *Phi(n)=(p-1)*(q-1)=1260*. Pro velká čísla p a q není možné faktorizovat jejich součin na ně samé v rozumně krátkém čase, a tudíž ani dopočítat Eulerovu charakteristiku a tím dopočítat soukromý klíč, potřebný k dešifrování zprávy.

Nyní si zvolíme veřejný klíč r nesoudělný s Eulerovou charakteristikou, obvykle se volí 65537, nyní volíme 667, a dopočítáme s podle rovnice : *Reduce[{Mod[r*s,Phi(n)]==1},s,Integers]*. Výsledek vypadá takto: *C[1]∈ Integers&&s＝67+120 C[1]*, kde s=1243 a 1260C[1] je konstanta.

Nyní volíme zprávu, kterou chceme poslat. Můžeme jí zvolit podobný principem, jaký uvádím: [„“, “a“, “b“, …] zaměnit za [„10“, „11“, „12“, …]. Pro příklad volím w=666, protože je důležité, aby zpráva byla menší než n, a byla s ním nesoudělná. Zprávu zašifrujeme umocněním na r, dle: : *Reduce[{PowerMod[w,r,n]==z},z,Integers]*, z toho: z=106 a to je šifra. Zprávu dešifrujeme umocněním šifry na soukromý klíč s: *Reduce[{PowerMod[z,s,n]==y},y,Integers], y=50* a protože platí y=w zprávu jsme zašifrovali správně.

RSA je velmi bezpečný šifrovací algoritmus s použitím velkých čísel p a q, a za předpokladu, že budou veřejnosti známá pouze čísla n a r, který lze prolomit spíše jen silou za netriviální čas.