
# AIMS-VOLKSWAGEN STIFTUNG WORKSHOP ON INTRODUCTION TO COMPUTER ALGEBRA AND APPLICATIONS

Douala, Cameroon, October 6-13, 2017

October 6, 2017

# Contents

# Preliminary Tutorial 3: Introduction to Maxima

**Dr. Daniel Duviol Tcheutia**

**October 6, 2017, Douala, Cameroon**

1. Compute $h = \frac{(x^2+2^3\pi)(1+\sqrt{x})}{7}$ for $x = 3$ and $x = 9$. Give the numerical approximation of the result with 10 and 25 digit precision, respectively.

2. Write $\cos^9(t) - \sin^9(t)$ as a Fourier polynomial

$$a_0 + \sum_{k=1}^{N} a_k \cos(kt) + \sum_{k=1}^{N} b_k \sin(kt),\ N \in \mathbb{N}.$$

   In converse, write the output as a polynomial of the variables $\cos(t)$ and $\sin(t)$. Hint: you can use the commands `trigreduce, trigexpand, trigsimp`

3. Consider the rational expression

$$r = \frac{x^4 + x^3 - 4x^2 - 4x}{x^4 + x^3 - x^2 - x}.$$

   Determine its normal form, its factorized form and its partial fraction decomposition. Hint: you can use the commands `ratsimp, factor, partfrac`

4. Define the function

$$f : (x, y, z) \longmapsto \frac{z}{x^2 + y^2 + z^2},$$

   and check that $f$ is solution of the differential equation

$$\frac{\partial^2}{\partial x \partial y} f + \frac{4x}{x^2 + y^2 + z^2} \frac{\partial}{\partial y} f = 0.$$

5. Compute the following integrals:

$$\int \sqrt{x^2 - a^2} dx;\ \int_0^\infty \frac{\sin x}{x} dx;\ \int_0^\infty x e^{-ax} \cos(wx) dx \text{ for } a > 0.$$

6. Plot on [1/3, 1] the graph of

$$f(x) = e^x - \frac{1}{x},$$

   and use the `find_root` command to find a numerical approximation of the solution to the equation $f(x) = 0$.

7. Determine the following sums:

$$\sum_{k=0}^{\infty} \binom{n}{k},\ \sum_{k=0}^{\infty} a q^k \text{ for } |q| < 1 \text{ and for } |q| > 1,\ \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{k!};\ \sum_{k=0}^{\infty} \binom{n}{k} x^k y^{-n-k}.$$

   Hint: Use `simpsum` or `simplify_sum` after loading `load(simplify_sum)` to simplify the sum, `assume` for the assumption and `forget` to forget the assumption.

8. Compute the Taylor polynomial at $x_0 = 0$ of order 8 of the function

$$f(x) = \frac{\ln(x+1) - \tan(x) + \frac{1}{2}\sin^2(x)}{3x^2 \sin^2(x)},$$

and deduce the limit of $f(x)$ as $x \to 0$.

9. Compute the following limits:

$\lim_{x\to 0}(\cos x)^{\frac{1}{x^3}}$; $\lim_{x\to\infty}(2^x+3^x)^{\frac{1}{x}}$; $\lim_{n\to\infty}\frac{n!}{n^n e^{-n}\sqrt{2\pi n}}$, $\lim_{x\to\infty} e^{-ax}\cos(bx)$ assuming $a > 0$.

10. Consider the matrix

$$M = \begin{pmatrix} 0 & -\frac{4}{5} & -\frac{3}{5} \\ \frac{4}{5} & -\frac{9}{25} & \frac{12}{25} \\ \frac{3}{5} & \frac{12}{25} & -\frac{16}{25} \end{pmatrix}$$

defined in `Maxima` by
`M: matrix([0,-4/5,-3/5],[4/5,-9/25,12/25],[3/5,12/25,-16/25])`.
Determine the trace, determinant, the rank, the inverse, the transpose, the characteristic polynomial, the eigenvalues, the eigenvectors, the matrix exponential $e^M = \sum_{n=0}^{\infty}\frac{A^n}{n!}$ of the matrix $M$. Hint: you can use the commands `matrix`, `length`, `determinant`, `rank`, `invert`, `transpose`, `charpoly`, `eigenvalues`, `eigenvectors`, `matrixexp`.

## Preliminary Tutorial 6: Introduction to CoCoA
**John Anthony Abbott**
**October 6, 2017, Douala, Cameroon**

### Red Question

Use CoCoA to compute approximations to within $\epsilon = 10^{-20}$ to each of the real roots of the polynomial $f = x^5 - 5x^4 - 3x^3 + 4x^2 - x + 1$. Print out the appoximate roots as decimal numbers. Verify that evaluating $f$ at each of the approximate roots produces values close to zero.

Now repeat the exercise for the **Mignotte polynomial**: $g = x^{16} - (1000000x - 1)^2$. This polynomial has two real roots which are close to one another. Compute a good approximation to the *distance between these two roots*.

Useful CoCoA manual pages: `RealRootsApprox`, `FloatStr`, `eval`, `subst`.

### Green Question

A positive integer $p$ is a **Sophie Germain prime** if both $p$ and $2p+1$ are prime. Write a CoCoA function called `IsSGPrime` which takes one (integer) argument `P`, and returns true if `P` is a Sophie Germain prime, otherwise it returns false.

Compute a list of all the Sophie Germain primes up to 1000.

A positive integer $p$ is a **Twin Prime** if both $p$ and $p+2$ are prime. Write a CoCoA function called `IsTwinPrime` which takes one (integer) argument `P`, and returns true if `P` is a twin prime, otherwise it returns false.

Compute a list of all numbers (from 1 to 1000) which are both Sophie Germain primes and twin primes.

Useful CoCoA manual entries: `IsPrime`, `define` and `list constructors`.

### Blue Question

Use the CoCoA function `GroebnerFanIdeals` to compute all the different reduced Gröbner bases of the ideal $I = \langle x^2z + yz^2 + 1,\ x^3 + y^3,\ z^3 - y^2\rangle$

How many different reduced Gröbner bases are there?

Find a term-ordering for which the reduced Gröbner basis of $I$ contains just 3 elements. Remember that, in general, term orderings can be described by matrices (of integers); only very few term orderings have specific names.

Other useful CoCoA manual entries: `RingOf`, `OrdMat` and `list constructors`.

### Yellow Question

In each of the following cases determine which of these three relations holds $A < B$ or $A > B$ or $A = B$.

**case** $(\alpha)$ $A = \sqrt{86} + \sqrt{990}$ $\qquad B = \sqrt{165} + \sqrt{778}$

**case** $(\beta)$ $A = \sqrt{176} + \sqrt{195} + \sqrt{2025}$ $\qquad B = \sqrt{190} + \sqrt{398} + \sqrt{1482}$

**case** $(\gamma)$ $A = \sqrt{17}+\sqrt{833}+\sqrt{2873}+\sqrt{9261}$ $\qquad B = \sqrt{189}+\sqrt{1029}+\sqrt{2541}+\sqrt{7497}$

Hints:

- One possibility could be to compute approximations to the square roots, and then just evaluate the formulas. But how much precision do you need to be sure of getting the right answer? See the CoCoA manual page for `RealRootsApprox`.
- There is a more algebraic solution technique. Create a polynomial ring with one indeterminate for each square-root. Define an ideal with the minimial polynomials for each indeterminate: *e.g.* $I = \langle A^2 - 86,\ B^2 - 990,\ C^2 - 165,\ D^2 - 778\rangle$. This ideal will be useful for "reducing" expressions. Regroup the sums into two parts (say, $LHS$ and $RHS$) so that all multiples of one of the square-roots are in $LHS$, and everything else is in $RHS$. Now square both $LHS$ and $RHS$, and repeat the process until no square-roots are left. Useful CoCoA manual pages: `NF` and `NR`.

### White Question

There are 4 distinct pythagorean triples with hypotenuse 65. Use CoCoA to find them.

Using the obvious reflections and rotations, produce 32 distinct points in the plane with integer coordinates all lying on the circle of radius 65. Compute $I$, the ideal of polynomials vanishing at these points.

The reduced (`DegRevLex`) Gröbner basis of $I$ contains two polynomials: one is obviously $x^2 + y^2 - 65^2$. The other polynomial is reducible; what are its factors?

There are 40 distinct pythagorean triples with hypotenuse 32045. Use CoCoA to find them, and then repeat the steps above using these triples. Is there a quicker way to get the answer?

Useful CoCoA manual pages: `for`, `foreach`, `append`, `IdealOfPoints`, `factor`

### Black Question

You have a rectangular box of size 37-by-47, and a rectangular bar of chocolate of size 5-by-55. Can you fit the bar into the box?

Try also these cases:

- Box: 57-by-77 Bar: 4-by-92
- Box: 54-by-59 Bar: 4-by-76
- Box: 25-by-32 Bar: 7-by-34

Hints:

- Useful CoCoA manual pages: `ideal`, `elim`, `MinPolyQuot`
- Given a box of size $A$-by-$B$, and a bar of size $C$-by-$D$, use Groebner bases to find the longest bar of width $C$ which fits into a box $A$-by-$B$. If the longest bar has length greater than $D$ then the bar fits, otherwise it does not.
- Here is an approach using coordinate geometry. Place the box with one corner at $(0, 0)$ and the opposite corner at $(A, B)$. The maximal length bar will touch the box at 4 points $P_1 = (x, 0)$, $P_2 = (0, y)$, $P_3 = (A, B - y)$ and $P_4 = (A - x, B)$. We know the distance between $P_1$ and $P_2$. We know that the angle $P_1 - P_2 - P_4$ is a right-angle. The value we seek is the distance between $P_1$ and $P_3$ (or equivalently between $P_2$ and $P_4$). Use a new indeterminate $L$ to represent this length, then compute the minimal polynomial of $L$ (*e.g.* via elimination). Check that the minimal polynomial has a real root in the range 0 to $\sqrt{A^2 + B^2}$; if so, this is the maximal length.

## Pink Question

An ideal in a polynomial ring which can be generated by monomials is called a **monomial ideal**. We shall assume that all our ideals are *explicitly* monomial, *i.e.* the generators which we have are actually monomials. Such ideals enjoy a number of nice combinatorial properties; also, the *leading term ideal* of a general polynomial ideal captures several interesting proprties of the general ideal.

An ideal $I$ is monomial iff for every polynomial $f \in I$ each term in $\text{supp}(f)$ is in $I$, where $\text{supp}(f)$ is just the set of terms in $f$. (Prove this.)

Let $I = \langle t_1, \dots, t_s \rangle$ be an explicitly monomial ideal. Then for any term $t$ we have $t \in I$ iff there is an index $j$ such that $t_j \mid t$. (Prove this.)

Devise an algorithm to determine a **minimal set of generators** of a monomial ideal: given a set of terms $\{t_1, \dots, t_s\}$, the algorithm finds a minimal subset which generates the same ideal. Is the minimal subset unique?

It is a standard result that the intersection of two ideals is an ideal; show that the intersection of two monomial ideals is a monomial ideal. Devise an algorithm to compute a (minimal?) set of generators for the intersection of two monomial ideals. What result does it produce if you intersect a monomial ideal with itself?

Let $I$ be an ideal, then the **radical** of $I$ is $\sqrt{I} = \{f \in P \mid f^n \in I \text{ for some } n \in \mathbb{N}\}$. It is a standard result that the radical is also an ideal. Prove that the radical of a monomial ideal is again a monomial ideal. Devise an algorithm to compute the radical of a monomial ideal.

Implement your algorithms in CoCoA, and run them on some test cases. Here are some monomial ideals: $\langle x \rangle$, $\langle x^2y, yz^2 \rangle$, $\langle x^2y, xy^2 \rangle$, $\langle x^3y^2, x^2y^3, x^2, y^2 \rangle$, $\langle x^2y, yz^2, x^3, y^4, z^5 \rangle$.

## Orange Question

The CoCoA function `NumTerms` counts how many terms a polynomial has. We say that a polynomial $f$ is **dense** if $\text{NumTerms}(f) = 1 + \deg(f)$. For example, $\text{NumTerms}(x^9 - 1) = 2$, and $\text{NumTerms}(x^3 + 2x^2 + 3x + 4) = 4$.

Find a dense monic polynomial, $f$, of degree 4 such that $\text{NumTerms}(f^2) = \text{NumTerms}(f)$. Since $f$ is dense of degree 4 it necessarily has 5 terms.

Let $k$ be a positive integer, and define $g(x) = f(x)\, f(x^k)$. Show that there is at least one value of $k$ for which $\text{NumTerms}(g^2) < \text{NumTerms}(g)$. Use CoCoA to find which values of $k$ give the smallest ratio $\text{NumTerms}(g^2)/\,\text{NumTerms}(g)$.

A similar argument shows that there exists a positive integer $k_2$ such that the ratio $\text{NumTerms}(h^2)/\,\text{NumTerms}(h)$ is smaller than $\text{NumTerms}(g^2)/\,\text{NumTerms}(g)$ where $h(x) = g(x)\, g(x^{k_2})$. Use CoCoA to find which values of $k_2$ give the smallest ratio for $\text{NumTerms}(h^2)/\,\text{NumTerms}(h)$.

We can also find dense palindromic polynomials with sparse squares. We say that a polynomial $f$ is **palindromic** if $f(x) = x^{\deg(f)} f(\frac{1}{x})$. Find a dense palindromic monic polynomial $F$ of degree 6 such that $\text{NumTerms}(F^2) = \text{NumTerms}(F)$.

Prove that for any positive integer $k$ the polynomial $G(x) = F(x)\, F(x^k)$ is palindromic.

Find a palindromic polynomial $G$ such that $\text{NumTerms}(G^2) < \text{NumTerms}(G)$.

Hints:

- Useful CoCoA manual pages: `CoeffListWRT`, `subsets`, `foreach`, `ReducedGbasis`
- Use a CoCoA ring like `QQ[x,a[0..3]]`, then a generic monic dense polynomial of degree 4 is `x^4+a[3]*x^3+a[2]*x^2+a[1]*x+a[0]`.
- For the palindromic polynomial the coefficients are not rational.

### Violet Question

Write a CoCoA function `NaturalLog(X, N)` where `X` is a positive rational number, and `N` is a positive integer; the function should return a rational number $L$ such that $|L - \ln(X)| < 2^{-N}$.

Hints:

- Useful CoCoA manual pages: `FloorSqrt`, `FloorLog2`
- Find a power of 2 such that $1 \leq 2^{-k}X < 2$. Compute $\ln(2)$ to sufficient precision. Compute $\ln(2^{-k}X)$ to sufficient precision. Return $k\ln(2) + \ln(2^{-k}X)$.
- Recall that $\ln(1+x) = x - x^2/2 + x^3/3 - \cdots$ valid for $|x| < 1$.
- Using the power series to compute $\ln(1+x)$ accurately needs many terms unless $x$ is close to zero. We can use $\ln(1+x) = 2\ln(\sqrt{1+x}) = 4\ln(\sqrt[4]{1+x}) = \cdots$ We need the value $\sqrt{1+x}$ only approximately, and this can be found multiplying by a power of 2 and then using `FloorSqrt`.

### Brown Question

Below you will find a CoCoA function to compute the GCD of two univariate polynomials using Euclid's algorithm. It also prints out the leading monomial of each successive remainder. Try using this function to compute the GCD of some pairs of polynomials. Observe that the leading coefficients can quickly become much more complicated than the coefficients of the original polynomials.

Use a modular approach to compute the GCD of the following polynomials: you can use CoCoA's own GCD function of compute the GCDs of polynomials with coefficients in a finite field.

Useful CoCoA Manual pages: `NewRingFp`, `CRTPoly`, `RatReconstructPoly`

```
define euclid(f,g)
  // First deal with the trivial cases
  if f=0 then return g; endif;
  if g=0 then return f; endif;
  if deg(f) = 0 then return f; endif;
  if deg(g) = 0 then return g; endif;
  if deg(f) < deg(g) then swap(ref f, ref g); endif;
  // Now deg(f) >= deg(g) >= 1, so enter general loop.
  P := RingOf(f);
```

```
  coeff := CoeffEmbeddingHom(P);
  x := indet(P, UnivariateIndetIndex(f));
  while g <> 0 do
    while f <> 0 and deg(f) >= deg(g) do
      delta := deg(f) - deg(g);
      f := f - coeff(LC(f)/LC(g)) * x^delta * g;
    endwhile;
    if f <> 0 then println "LM(rem) = ", LM(f); endif;
    swap(ref f, ref g);
  endwhile;
  return f;
enddefine; -- euclid


f1 := sum([random(-99,99)*x^k | k in 0..10]);
f2 := sum([random(-99,99)*x^k | k in 0..10]);
g := sum([random(-99,99)*x^k | k in 0..2]);

euclid(f1*g, f2*g);
-- The answer looks wrong: it should be just g.
factor(It); -- it is just g, but multiplied by an "ugly" scalar.
```

## Preliminary Tutorial 10: Programming with Maxima
## Dr. Daniel Duviol Tcheutia
## October 7, 2017, Douala, Cameroon

**Recall:**
(a) The `for` loop provides the ability to execute a statement repeatedly for a fixed number of times.
(b) If we want to repeat a statement, but we do not know how many times, we can use the `while` loop. The expression between `while` and `do` has to be a boolean expression (an expression returning `true` or `false`).
(c) Sometimes we want to make a case-by-case analysis. For this purpose we can use the `if` statement. The statements after `then` are only evaluated, if the condition is true.

1. Define the list $L = [1, 2, \ldots, 1000]$.
   (a) Derive the list $L1 = [2^p + 1, p \in L]$.
   (b) Count the number of primes in $L1$.
   (c) Derive the list of all the prime elements in $L1$.
   (d) Derive the list $L2 = [p \in L \ / \ 2^p + 1$ is prime$]$.

(e) Check that each element in $L2$ can be written as power of 2.

(f) Compute the arithmetic mean of the elements of $L$ and return its numerical approximation.

2. Let $a, b \in \mathbb{N}_{\geq}0$. The division with remainder gives the relation

$$a = b\,q + r,\ 0 \leq r < b. \tag{1}$$

Use the fact that $\gcd(a,b) = \gcd(b,r)$ and $\gcd(a,0) = a$ to implement the function `gcd1(a,b)` which computes recursively the greatest common divisor of $a$ and $b$. Hint: The remainder $r$ in (1) is `mod(a,b)` in Maxima.

Test your program for the computation of $\gcd(2^{400}+3; 3^{300}+8)$ and compare the timings with the internal function `gcd`.

3. Consider the matrix

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 5 \\ 7 & 8 & 9 \end{pmatrix}.$$

(a) Write a first recursive program `MatPow1(A,n)` to compute $A^n$ ($n = 0, 1, 2, \ldots$) using the relation $A^n = A \times A^{n-1}$. Apply this with $M^{10}$ and $M^{1000}$ (use `.` for matrix multiplication and `ident(n)` to get the identity matrix of order $n$).

(b) Write the second recursive program `MatPow2(A,n)` to compute $A^n$ ($n = 0, 1, 2, \ldots$) using the divide-and-conquer approach: $A^n = (A^2)^{n/2}$ if $n$ is even and $A^n = A \times A^{n-1}$ if $n$ is odd.

For each of the implementations, compare the timings with the internal function `A^^n` for $n = 10000$ for example.

4. Implement the procedures `PolyQuot(a, b, x)` and `PolyRem(a, b, x)` which compute, respectively, the quotient and the remainder of $a(x)$ by $b(x)$ for two polynomials $a(x)$, $b(x)$. Use your function to find the polynomial quotient and remainder of the division of $a(x) = 12x^6 - 8x^5 + 17x^4 + 5x^3 - 4x^2 + 3x + 5$ by $b(x) = 3x^4 + 5x - 1$ and $b(x)$ by $a(x)$ and check your results with the internal command `divide(a, b)`.
Hint: `coeff(p,x,n)` returns the coefficient of $x^n$ in the polynomial $p$, `hipow(p,x)` returns the degree of the polynomial $p$.

5. The Chebyshev polynomials $T_n(x)$ are defined by

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),\ T_0(x) = 1 \text{ and } T_1(x) = x; \tag{2}$$

and have the property

$$\begin{cases} T_n(x) = 2\left(T_{\frac{n}{2}}(x)\right)^2 - 1, \text{ if } n \text{ is even} \\ T_n(x) = 2T_{\frac{n-1}{2}}(x)T_{\frac{n+1}{2}}(x) - x, \text{ if } n \text{ is odd} \\ T_0(x) = 1,\ T_1(x) = x. \end{cases} \tag{3}$$

Implement each of the above recurrence equations and compare their complexities by taking higher values of $n$.

# Tutorial sessions 4 & 15: Algorithms and Algorithmic Proving in Mathematica

**Prof.Dr. Bruno Buchberger**

**October 9 & 10, 2017, Douala, Cameroon**

1 Look at Mathematica 'Help'

Check the Mathematica Help Facility (Menu 'Help → 'Wolfram Documentation') for one of your favorite topics and play with the examples given there.

For example, if your are intested in machine learning: Search for "machine learning" and go to the examples in the notebook that pops up:

**trainingset = {1 → A, 2 → A, 3.5 → B, 4 → B};**

***c* = Classify[trainingset]**

Use the classifier function to classify a new unlabeled example:

***c*[2.6]**

A

Obtain classification probabilities for this example:

***c*[2.6, "Probabilities"]**

A → 0.999618, B → 0.000381686

.....

Try to understand how to use the Mathematica functions in this section by experimenting with the examples and your own examples.

2 Write a Recursive Mathematica Program for Merge Sort

## The Task

Write a recursive Mathematica program ' **mergeSort'** for sorting by merging.

**Input**: a list X (of, say, natural numbers).

**Output**: a list Y of natural numbers such that Y is in ascending order and X and Y contain the same elements (the same number of times).

In the program, you will need sub-programs 'left', 'right', 'merge', and 'length':

**'merge'**:

**Input**: two sorted lists X and Y.

**Output**: a list Z such that Z is sorted and contains the same elements as X and Y (the same number of times).

**'left'** and **'right'**:

**Input**: a list X.

**Output**: left[ X] and right[ X] should be sublists of X of length shorter than X (if length of X is bigger than 2) such that the concatenation of left[ X] and right[ X] contains the same elements as X the same number of times).

**'length':**

**Input**: a list X.

**Output**: the length of X.

Write recursive Mathematica programs also for 'left', 'right', 'merge', and 'length' and test your programs in sufficiently many well chosen examples.

For lists, use the Mathematica notation '{1,2,3,4}' etc.

Compare the speed of your program 'mergeSort' with the speed of the built-in Mathematica program 'Sort'.

3 (Try to) Give a Proof of the Correctness of the Program

In the proof, for reducing writing effort, use abbreviated names 'mS', '| ...|', 'l', 'r', 'm' for the long names 'mergeSort', 'length', 'left', 'right', 'merge'.

You will need the predicates 'isSortedVersion', 'isSorted', 'containSameElements' abbreviated by 'isSV', 'isS', '$\sim$':

Use 'X', 'Y', 'Z' etc. as variables for lists.

**'isSortedVersion'**:

isSV[ X, Y] $:\Longleftrightarrow$ ( isS[Y] $\wedge$ X $\sim$ Y ).

**'isSorted'**:

isS[ X] $:\Longleftrightarrow$ X is sorted (in ascending order) (try a definition by giving Mathematica program!)

**'containSameElements'**:

X $\sim$ Y $:\Longleftrightarrow$ X and Y contain the same elements the same number of times (try definition by giving Mathematica program!)

**Correctness Statement to be proved:**

$\forall_X$ isSortedVersion[ X, mergeSort[ X]].

For the proof, use the following **induction principle:** For any property P,

i **n order to prove** $\forall_X$ P[ X]

take X* **arbitrary but fix,**

**assume** $\forall_Y$ ($|Y| < |X^*| \Longrightarrow$ P[ X] )

and **prove** P[ X*].

In our case, the property P is

P[ X] $:\Longleftrightarrow$ isSortedVersion[ X, mergeSort[ X]].

In the proof, you may use the following **lemmas** (without proving them):

|X| $\leq 1 \Longrightarrow$ isSorted[X]

X $\sim$ X, X $\sim$ Y $\Longrightarrow$ Y $\sim$ X, X $\sim$ Y $\wedge$ Y $\sim$ Z $\Longrightarrow$ X $\sim$ Z

| X| $> 1 \Longrightarrow$ ( | left[ X] | $<$ | X| $\wedge$ | right[ X] | $<$ | X| )

( | X| $> 1 \wedge$ Y $\sim$ left[ X] $\wedge$ isSorted[ Y] $\wedge$ Z $\sim$ right[ X] $\wedge$ isSorted[ Z] )

$\Longrightarrow$ ( merge[ Y, Z] $\sim$ X $\wedge$ isSorted[ merge[ Y, Z] ] )

(Instead of proofs, give intuitive arguments why these lemmas are true. Use diagrams!)

4 (Try to) Give an Automated Proof for the Correctness of the Program

For this, extend / modify the simple automated reasoner presented and discussed in the lecture.

## Tutorial session 5: Solving in Computer Algebra
## Dr. Daniel Duviol Tcheutia
## October 9, 2017, Douala, Cameroon

1. Solve the system of equations

$$\begin{cases} x^2 + y^2 = 5 \\ xy = y^2 - 2, \end{cases}$$

the equation $|x| = 7$, and the inequalities $x^2 - 2x - 3 < 0$, $x^2 - 3x + 1 < 0$ and $|x - 3| \cdot |3 - x| > |x|$. Hint: One can use the command `solve`, `to_poly_solve` after loading `load(to_poly_solve)`, and `solve_rat_ineq` after loading `load(solve_rat_ineq)`

2. Solve the differential equations

$$xy' = y\ln(xy) - y,\ y(1) = e,$$
$$y'' + 5y' + 6y = 0,\ y(0) = 2,\ y'(0) = 3;$$

the Legendre polynomial differential equation

$$(1 - x^2)y'' - 2xy' + n(n+1)y = 0;$$

and the system of differential equations

$$\begin{cases} y_1'(x) = 2y_1(x) - 2y_2(x) \\ y_2'(x) = -2y_1(x) + 2y_3(x) \\ y_3'(x) = 2y_2(x) + 2y_3(x) \\ y_1(0) = 2,\ y_2(0) = 1,\ y_3(0) = -2. \end{cases}$$

Hint: You can use the commands `desolve`, `ode2`, `ic1, ic2, atvalue`, `contrib_ode` after loading `load(contrib_ode)`.

3. Solve the recurrence equation

$$F(n) = -3F(n-1) - 2F(n-2),\ F(1) = 1,\ F(2) = 1.$$

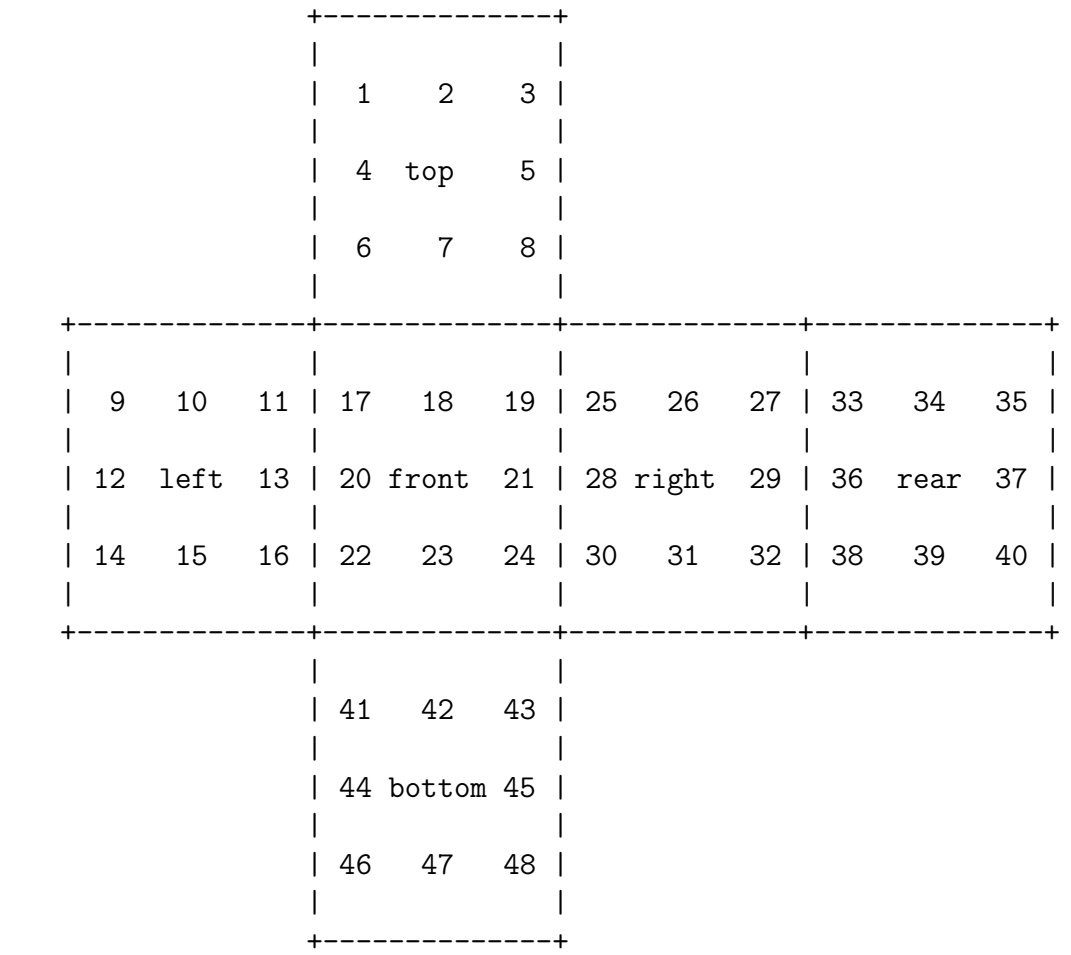
4. Solve the equation $7x \equiv 1 \pmod{218}$ and the system of equations

$$\begin{cases} x \equiv 2 \pmod{12} \\ x \equiv 8 \pmod{10} \\ x \equiv 10 \pmod{14}. \end{cases}$$

Hint: You can use `inv_mod` or `power_mod` and `chinese`.

## Tutorial Session 13: GAP session - Rubik's cube
## Prof. Dr. Bettina Eick
## October 10, 2017, Douala, Cameroon

Number the faces of the Rubik's cube:




The elementary moves of the cube are then given by the following permutations:

$$a = (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19),$$
$$b = (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35),$$
$$c = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11),$$
$$d = (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24),$$
$$e = (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27),$$
$$f = (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)$$

**Exercise 1:** Define the permutation group $C$ defined by $\langle a, b, c, d, e, f \rangle$ in GAP.

**Exercise 2:** How many elements does $C$ have?
(Try $Size(C)$)

**Exercise 3:** Is it possible to turn one corner in $C$?
(For example, try $(6, 11, 17)$ in $C$.)

**Exercise 3:** Is it possible to flip one edge in $C$?
(For example, try $(7, 18)$ in $C$.)

**Exercise 4:** How does $C$ act on corners (or edges)?
(One corner is $[6, 11, 17]$. Get the other corners via $Orbit(C, [6, 11, 17], OnSets)$. Now investigate the action on them using ActionHomomorphism. Similar for edges.)

**Exercise 5:** What can you say about the $2 \times 2$-cube and the $4 \times 4$-cube?

## Tutorial sessions 14 & 21: Symbolic Computation with (Integro)-Differential Operators
**Dr. Georg Regensburger**
**October 10 & 11, 2017, Douala, Cameroon**

In some of the exercises, we use the computer algebra system SageMath. For computing with differential operators, we use the optional package `ore_algebra`. It can be installed on your computer by running on the command line the command

```
sage -i ore_algebra-0.3.spkg
```

(You need an internet connection so that the package can be downloaded.)

We will mention the commands from the package needed in the exercises below. For further details on the package, see the tutorial https://arxiv.org/abs/1306.4263.

In the two tutorial sessions, we will discuss the following exercises.

1. Use the command `desolve` to find a solution of the homogeneous differential equation $y'(x)+y-1$ and the inhomogeneous differential equation $y'(x)+y-1 = e^x$. You first need to introduce the function $y(x)$ in Sage by the command

   ```
   y = function('y')(x)
   ```

   You can also try to solve some other first and second order differential equations with `desolve`.

2. Let $(R, \partial)$ be a commutative differential ring, that is, $\partial\colon R \to R$ is additive and satisfies the Leibniz rule

   $$\partial(fg) = \partial(f)g + f\partial(g)$$

   for all $f, g \in R$. Verify that the constants of $R$ given by

   $$C = \{c \in R \mid \partial(c) = 0\}$$

   form a subring of $R$ and that the derivation $\partial$ is linear over the constants $C$.

3. Load the package `ore_algebra` and set up the algebra of integro-differential operators with rational coefficients with the following commands:

   ```
   from ore_algebra import *

   R.<x> = PolynomialRing(QQ)
   K=R.fraction_field()
   B.<Dx>=OreAlgebra(K)
   ```

   Multiply the differential operator `Dx` with the multiplication operator `x` to obtain:

   ```
   Dx*x
       x*Dx + 1
   ```

   Define the differential operator

   ```
   L=Dx^2 + ((-x + 1)/x)*Dx + (-x - 1)/x^2
   ```

   and try to solve the differential equation $L(y) = 0$ with the command `desolve`.

4. Let $(R, \partial)$ be a commutative differential ring and let $y \in R$ be invertible. Find an element $r \in R$ such that $y$ solves the differential equation defined by the monic differential operator

   $$B = \partial - r \in R\langle\partial\rangle$$

   that is, such that $B(y) = 0$.

5. Use the command `rational_solutions()` to compute a rational solution $y \in \mathbb{Q}(x)$ of the differential operator $L$ above. Construct a monic differential operator

   ```
   B=Dx-r
   ```

   with a rational function $r \in \mathbb{Q}(x)$ such that $B(y) = 0$.

6. Use the command `L.quo_rem(B)` to compute a differential operator $Q$ such that we obtain a factorization
   $$L = QB$$
   of differential operator $L$ and verify your result in Sage.

7. Compute with Sage a solution $\varphi$ of the differential operator $Q$ and a solution of the inhomogeneous differential equation $B(z) = \varphi$. Verify with Sage that $z$ and $y$ constructed in the two previous exercises are two solutions of the differential operator $L$, that is, $L(z) = 0$ and $L(y) = 0$.

8. We consider the two linear maps defined on the basis $(t^n)_{n\in\mathbb{N}}$ of the polynomial ring $k[t]$ by
   $$t\colon t^n \mapsto t^{n+1} \qquad \partial\colon t^n \mapsto n\,t^{n-1}.$$
   They correspond respectively to the multiplication operator $p \mapsto t\,p$ and the derivation $p \mapsto \frac{dp}{dt}$ on polynomials $p$. Verify on the basis elements $t^n$ that the two linear operators satisfy the Leibniz rule
   $$\partial \circ t = t \circ \partial + \mathrm{id},$$
   where id denotes the identity map on $k[t]$.

9. Consider the linear map on the polynomial ring defined by
   $$\int\colon t^n \mapsto \frac{1}{n+1}\,t^{n+1}$$
   corresponding to the integral operator
   $$p(t) \mapsto \textstyle\int_0^t p(s)\,ds.$$
   Verify on the basis elements $t^n$ that the integral operator and the derivation satisfy the fundamental theorem of calculus
   $$\partial \circ \textstyle\int = \mathrm{id}\,.$$

10. We define the evaluation by
    $$\mathtt{E} = \mathrm{id} - \textstyle\int \circ\, \partial.$$
    It corresponds to the evaluation $p(t) \mapsto p(0)$ at 0. Verify directly that the evaluation and the multiplication satisfy the identity
    $$\mathtt{E} \circ t = 0.$$

11. We considered in the lecture the $k$-algebra

$$\mathbb{I} = k\langle T, D, I, E\rangle / J$$

where $J$ is the two-sided ideal generated by the relations

$$D\,T - T\,D - 1, \quad D\,I - 1, \quad I\,D + E - 1, \quad E\,T.$$

Compute some S-polynomials between the relations and interpret them in terms of the corresponding identities between the linear operators $t, \partial, \int, \mathtt{E}$ from the three previous exercises.

For example, the S-polynomial between

$$D\,I - 1 \quad \text{and} \quad I\,D + E - 1$$

is given by

$$S(D\,\underline{I}, \underline{I}\,D) = 1\,D - D\,(1 - E) = D\,E$$

It corresponds to the fact the the evaluation $\mathtt{E}$ maps to constants $k$.

12. We consider the boundary problem

$$\begin{aligned} y''(t) &= f(t), \\ y(0) &= y(1) = 0, \end{aligned}$$

which we can specify in terms of integro-differential operators by the corresponding differential operator and boundary conditions (evaluating at 0 and 1) as

$$(L = \partial^2, (\mathtt{E}_0, \mathtt{E}_1)).$$

The Green's operator $G$ mapping a right-hand side $f$ to the unique solution $y$ is given as an integro-differential operator by

$$G = -\int t + t \int - t\,\mathtt{E}_1 \int + t\,\mathtt{E}_1 \int t.$$

It acts on a function $f(t)$ as

$$G(f) = -\int_0^t s\,f(s)\,ds + t\,\left(\int_0^t f(s)\,ds + \int_0^1 (s-1) f(s)\,ds\right).$$

Implement the action of the Green's operator using the command `integrate` in Sage. Compute and verify the solution $y(x)$ of the boundary problem for some concrete functions $f(x)$.

## Tutorial Session 27: GAP session - Classification of groups
## Prof. Dr. Bettina Eick
## October 10, 2017, Douala, Cameroon

The SmallGroups Library of GAP contains the groups of various orders. It can be accessed via $SmallGroups(n, i)$ and $NumberSmallGroups(n)$.

**Exercise 1:** Find the smallest order $n$ so that there exists a non-solvable group of order $n$.

**Exercise 2:** Find the smallest order $n$ so that there exists a group without any normal Sylow subgroup.

**Exercise 3:** Determine the numbers of groups of orders $2^n$ for all $n$ that are available in the SmallGroups library.

**Exercise 4:** Determine the groups of orders $2p$ and $2p^2$ and $2p^3$ for as many odd primes $p$ as you wish. Based on your experiments can you suggest a formula for the numbers of groups of these orders?

**Exercise 5:** Determine the groups of order 2016.
(Use $RequirePackage("grpconst")$ and $ConstructAllGroups$)

## Tutorial session 35: Algorithmic summation
## Dr. Daniel Duviol Tcheutia
## October 13, 2017, Douala, Cameroon

1. Consider
$$F_k = \frac{1}{k(k+1)}.$$
   (a) Use the command `Gosper` of the package `SpecialFunctions` (to be loaded) to find the rational function $S_k$ such that $F_k = S_{k+1} - S_k$ and check that we really have $F_k = S_{k+1} - S_k$.
   Hint: You should create a folder named `maxima` in `C:\Users\your_name` (if it doesn't exist) in which you copy the file `SpecialFunctions.mac`, then you input `batchload(SpecialFunctions)` in your Maxima file to load the package.
   (b) Deduce from (a) the sum $\sum_{k=0}^{n} F_k$. You can also use `nusum` which is Gosper's implementation.

2. Show that:
$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{3n+k}{2n} = \binom{3n}{n}^2,$$

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}^2 = \begin{cases} 0 & \text{if } n \text{ is odd} \\ \frac{(-1)^{n/2}n!}{(n/2)!^2} & \text{otherwise.} \end{cases}$$

Hint: Using the Zeilberger algorithm implemented by the *Maxima* command `SumRecursion` of the package `SpecialFunctions`, find the recurrence equation satisfied by the left-hand side divided by the right-hand side. Even and odd $n$ must be treated separately in the second case.

3. Consider the sum

$$s_n = \sum_{k=0}^{\lfloor n/3 \rfloor}\binom{n-2k}{k}\left(-\frac{4}{27}\right)^k.$$

   (a) Using Zeilberger's algorithm, find a recurrence equation satisfied by $s_n$.

   (b) Use Petkovšeks algorithm to find hypergeometric term solutions of the recurrence equation of Question (a).

   (c) Write $s_n$ as linear combination of hypergeometric terms.

   (d) Check your answer for $n = 0, 1, \ldots, 15$. ($\lfloor n/3 \rfloor$ is obtained in Maxima using `floor(n/3)`).