

A recent trend in Computer Algebra?  
Let's chat!

Joachim von zur Gathen  
Universität Bonn, Germany  
gathen@bit.uni-bonn.de

25 September 2023  
Paris

## Recent trends in computer algebra

“Symbolic-Numeric Computation: Symbolic-numeric computation is an area that combines the strengths of symbolic and numeric computation. It involves developing algorithms and techniques that seamlessly integrate symbolic and numeric methods to solve mathematical problems. This approach is particularly useful when exact symbolic results are difficult to obtain, and numeric approximations are required.

Applications in Cryptography and Coding Theory: Computer algebra plays a crucial role in the fields of cryptography and coding theory. Cryptographic protocols rely on mathematical foundations, such as number theory and algebraic geometry, and computer algebra systems are used to perform computations in these areas.”

## Recent trends in computer algebra

“Cloud-Based and Web-Based Systems: The development of cloud-based and web-based computer algebra systems has made symbolic computation more accessible to a broader audience. These systems allow users to perform computations and access mathematical tools and libraries remotely through web interfaces. This trend has contributed to the democratization of computer algebra, enabling users to explore and utilize symbolic computation without the need for locally installed software. These are just a few of the recent trends in computer algebra. The field continues to evolve rapidly, with ongoing research efforts aimed at improving algorithms, enhancing performance, and exploring new applications in various domains.”

# Overview

- ▶ My personal acquaintance with AI.
- ▶ Chatbots.
- ▶ ChatGPT in computer algebra: RSA, Little Fermat, interpolation.
- ▶ Chatbots in teaching and research.
- ▶ A new kind of mathematics.
- ▶ Chatbots and society.

My goal today: chatbots are here to stay. What should our community do?

## My personal acquaintance with AI ...

... is basically nil.

But some of my colleagues at the University of Toronto are/were leaders in this field: Ray Reiter and Geoff Hinton. Also John Mylopoulos, Hector Levesque, many of their students.

**Raymond Reiter** (1939 - 2002): Canadian computer scientist and logician.



## Ray Reiter

Work on default logic, model-based diagnosis, closed-world reasoning, and truth maintenance systems.

One of the founders of the field of non-monotonic reasoning.

“Classical AI”, based on knowledge and reasoning.

Example: natural language translation. Build vocabularies for each language, a universal grammar, and translations between any language and the universal one.

For translations between any of  $n$  languages: need  $2n$  translations to/from universal.

# Geoffrey Everest Hinton

“Godfather of AI”.



Born 1947.

Professor at UofT since 1987, now an Emeritus.

Google 2013 - 2023.

Turing Award 2018. TIME AI-100, September 2023: top “thinker”.

Fundamental work on neural networks. Back-propagation, deep learning, multi-layer neural networks. “Modern AI”.

Great-great-grandson of George Boole and related to George Everest.

# Mount Everest





# Chatbots

Train your neural network with enormous amounts of information available on the internet.

Needs large amounts of resources, for example Nvidia's GPUs.

Translations between  $n$  languages: needs  $O(n^2)$  individual translators. Works very well.

# ChatGPT

“Generative pretrained transformer”.

Quote at beginning of talk: excerpt from answer to my question

“Tell me about recent trends in computer algebra”.

Prompt: “Write a maple program to compute an RSA-modulus.”

“Sure! Here’s a Maple program that computes an RSA modulus.”

```
# Function to check if a number is prime
```

```
isPrime := proc(n)
```

```
if n < 2 then return false; elif n = 2 then return true; elif n mod 2
```

```
= 0 then return false;
```

```
else for i from 3 to floor(sqrt(n)) by 2 do if n mod i = 0 then
```

```
return false; end if; end do; return true;
```

```
end if; end proc;
```

## ChatGPT RSA

```
# Function to find the greatest prime less than a given number
```

```
...
```

```
# Function to compute RSA modulus given two primes
```

```
computeRSAModulus := proc(p, q)
```

```
local modulus; if isPrime(p) and isPrime(q) then
```

```
modulus := p * q; return modulus;
```

```
else error "Both p and q must be prime."; end if;
```

```
end proc;
```

This is technically correct and works fine. Included in answer: tiny example and reasonable comments.

The system is not yet perfect. I asked for statement and proof of Fermat's Little Theorem. ChatGPT answered with a correct statement and bullshit as a proof. Each line sounded like a mathematical argument, but the total was incoherent and incorrect.

# ChatGPT Fermat

**Fermat's Little Theorem** states that if  $p$  is a prime number and  $a$  is an integer not divisible by  $p$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

1. **Base Case:** When  $a$  is not divisible by  $p$ , the case  $a \equiv 1 \pmod{p}$  is trivially true. So, assume  $a \not\equiv 1 \pmod{p}$ .
2. **Inductive Hypothesis:** Assume that the theorem holds for all integers  $a$  not divisible by  $p$  such that  $1 \leq a < k$ , where  $k$  is a positive integer.
3. **Inductive Step:** Consider an integer  $k$  not divisible by  $p$ . We want to show that  $k^{p-1} \equiv 1 \pmod{p}$ . There are two cases to consider:
  4. **Case 1:**  $k \equiv 1 \pmod{p}$   
If  $k \equiv 1 \pmod{p}$ , then the congruence  $k^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{p}$  holds trivially.

## ChatGPT Fermat

### 5. Case 2: $k \not\equiv 1 \pmod{p}$

In this case, we can use the inductive hypothesis. By the induction assumption, for any integer  $a$  not divisible by  $p$  where  $1 \leq a < k$ , we have  $a^{p-1} \equiv 1 \pmod{p}$ . Now, consider the set of residues  $\{1, 2, \dots, k-1\}$  modulo  $p$ . Each of these residues is not divisible by  $p$  and is less than  $k$ , so by the inductive hypothesis, each of them satisfies  $a^{p-1} \equiv 1 \pmod{p}$ . Now, let's consider the product of all these residues:

$$S = 1 \cdot 2 \cdot \dots \cdot (k-1)$$

Since each term in  $S$  satisfies  $a^{p-1} \equiv 1 \pmod{p}$ , we have  $S^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{p}$ .

Now, consider the congruence  $kS \equiv S \pmod{p}$ . This is equivalent to  $k \equiv 1 \pmod{p}$  since  $S$  is not divisible by  $p$  (none of the residues in the product are divisible by  $p$ ).

However, we assumed  $k \not\equiv 1 \pmod{p}$  in this case, which leads to a contradiction.

Since both cases lead to a contradiction, the only possibility left is that  $k \equiv 1 \pmod{p}$ , which we already covered in Case 1.

Fermat's Little Theorem states that if  $p$  is a prime number and  $a$  is any positive integer not divisible by  $p$ , then the remainder of the division of  $a^{p-1}$  by  $p$  is always 1.

The proof of Fermat's Little Theorem is based on the concept of modular arithmetic. Let's go through the proof step by step:

Consider a prime number  $p$  and a positive integer  $a$  not divisible by  $p$ .

We can list the remainders when the positive powers of  $a$  are divided by  $p$ , starting from  $a^1$  up to  $a^{p-1}$ :

$a^1 \bmod p, a^2 \bmod p, a^3 \bmod p, \dots, a^{p-1} \bmod p$

Since  $p$  is a prime number, the remainders will be distinct for all values of  $a^k \bmod p$ , where  $k$  ranges from 1 to  $p-1$ .

...

## ChatGPT on interpolation

1. Standard polynomial interpolation. Correct answer on how many points are needed, Lagrange algorithm. Fine.
2. Interpolation with decomposables. Prompt: How many points are needed to determine an interpolation polynomial over a finite field when the interpolation polynomial is known to be a composite polynomial? Answer correct, namely  $q + r + 2$  in the notation below.
3. Please give an algorithm.

### Input:

- ▶ A set of distinct points  $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$  in the finite field, where  $x_i$  are the input values and  $y_i$  are the corresponding output values.
- ▶ The degrees  $q$  and  $r$  of the polynomials  $Q$  and  $R$  respectively, in the functional composition  $P(x) = Q(R(x))$ .

**Output:** The interpolation polynomial  $P(x)$  that satisfies  $P(x_i) = y_i$  for all  $i$ .

Recall:  $P(x_j) = Q(R(x_j)) = y_j$ .

**Algorithm:**

1. Perform Lagrange interpolation on the given set of points to determine the polynomial  $R(x)$  of degree  $r$ . You need at least  $r + 1$  points to do this. The Lagrange interpolation formula is given by:

$$R(x) = \sum_{i=1}^{r+1} y_i \cdot \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

2. Next, perform Lagrange interpolation on the set of points  $\{(x_1, Q(y_1)), (x_2, Q(y_2)), \dots, (x_n, Q(y_n))\}$  to determine the polynomial  $Q(x)$  of degree  $q$ . Again, you need at least  $q + 1$  points for this. The Lagrange interpolation formula for  $Q(x)$  is the same as in step 1, but with the  $x_i$  values replaced by  $y_i$  and the  $y_i$  values replaced by  $Q(y_i)$ .
3. Construct the interpolation polynomial  $P(x) = Q(R(x))$ .



## Serious errors in ChatGPT

The “proof” of Fermat’s Little Theorem and the interpolation algorithm are seriously flawed, but in a manner that may not be easy to detect for a non-expert.

“Interpolation by decomposables” was solved recently by vzG & Guillermo Matera.

Motivation. vzG & Weiß 1995: solving kinematic equations for 6-joint robots involves finding certain decomposable polynomials by interpolation, where each interpolation point is costly to determine.

Some special cases of this interpolation are easy to solve, and for the general case, we construct a homotopy between it and a special case. A geometric solution of the algebraic curve presenting this homotopy provides an answer to the interpolation task.

Based on work of Joris van der Hoeven, Grégoire Lecerf, Éric Schost, and others. A “recent trend in computer algebra”?

# Chatbots in computer algebra

## Teaching

- ▶ Many of the easier methods and algorithms are described in books and on wikipedia. Now students can almost effortlessly turn them into code in their favorite computer algebra system.
- ▶ How far can this go? I would not be surprised if a cottage industry sprang up of producing targeted prompts for much more material, maybe for most of the usual contents of an introductory computer algebra course.
- ▶ Exercises and tests. An instructor usually has to give a grade to individual students. I typically used questions that require the understanding and application of class material in new environments. Simple example: With the RSA modulus 35 and the public exponent 11, what is the secret exponent?

## ChatGPT in the classroom

This fails now as a test! ChatGPT gives the correct answer (namely, 11) with perfectly correct reasoning.

What to do? I do not know.

- ▶ Think carefully about questions. Test them on the latest version of ChatGPT and friends.
- ▶ Talk about chatbots in class, let the students experiment, maybe find some limits or shortcomings.
- ▶ Ask students to prompt some chatbot for a proof of some (easy) theorem, and to check if it is valid. If not, can it be easily corrected? Great challenge for mathematically oriented students.
- ▶ Tell me about clever questions that you devise.

## A new kind of mathematics

**Fake mathematics:** Make some mathematical statement and “prove” it in eloquent mathematical language. Correctness of statement and “proof” are irrelevant.

Checks are left to the reader. Tool: overwhelm the reader with a deluge of such statements until she gives up.

Steve Bannon: “flood the zone with shit”.

Many students tend to believe what an instructor tells them, without checking.

New pedagogical tool: ask students to find errors in proofs. Say, chatbot-generated answers to own questions.

## AI in research

Will AI systems like chatbots impact research? If so, how?

The source of their power is the scraping of the internet, collecting publicly available information. In principle, it seems that answers to open research questions are out of their reach.

But I am sure they will be of help. If in your research project, you have some subproblem, they might furnish answers, with citations. And, who knows, one day “modern AI” based on the past may be integrated with entity-and-relation based “classical AI” and provide answers, hitherto unknown, to questions.

Pablo Picasso: “computers are useless, they only provide answers”. Imaginative new alleys of research and conjectures are likely to be beyond these systems for a long time.

## AI in computer algebra research

Classical connection: automated theorem proving.

Chatbots can write elegant prose. For grant applications, it may become the standard to use the right amount of promptology.

Wonderful. Good funding is essential for research, but can now researchers concentrate better on their real tasks? How big is the overlap between good researchers and good proposal writers? How do proposal reviewers now proceed? And the funding agencies? A healthy approach seems to me to look at past performance rather than promises for the future; some agencies already do this.

**Research papers.** It is common to use information from wikipedia, say, for research. Some authors cite this, many do not. In my opinion, this is acceptable, because technical or scientific statements on wikipedia enjoy a high degree of reliability.

Chatbots do not, as shown above. They will improve over time, but the main problem remains: they make false statements with the same degree of conviction as for correct ones.

## AI in computer algebra research

**Research outlets.** Conference SYNASC, two weeks ago.  
Matthew England: “Can Explainable AI Give Insights for Symbolic Computation?” Machine-learning for variable ordering in CAD.  
JSC: Special Issue for this conference.

**Editors and reviewers of non-AI journals.** Demand clear statements of the use of chatbots? To which detail? Sanctions? For long and difficult papers with important claims it is often difficult to find competent and willing referees: Wiles & Taylor for Fermat’s Last Theorem, Mochizuki’s claimed proof of the *abc*-conjecture. How to deal with very long papers? In general? And in particular: can a chatbot obfuscate things?

# AI and society

What do these recent developments mean for society at large? I do not know.

- ▶ Job market. New jobs will be created, like promptologists. Other jobs will go away. Newspaper articles about local car crashes may be taken over by AI with access to police files, but serious investigative journalism will not.
- ▶ (Un)Social networks have done a lot of damage to the real social network. Democracy is under attack. The possibility of easily faking texts, images, and videos will do more damage.
- ▶ Windfall profit.





Caribbean island of Anguilla.



## IMMOBILIEN

Die Verkäufer  
müssen zittern

## OLYMPIA IN EXTREM

Wie alle  
dopen dürfen

## TARANTINO

Die neue Karriere des  
Hollywoodstars



# Das Ende der Wahrheit

Politik, Liebe, Musik: Wie uns  
**künstliche Intelligenz**  
täuschen kann



## AI and society

Unlike myself, Geoff Hinton is an expert on AI. He worked for Google, since 2016 as Vice President.

In May 2023, he resigned from Google to be able to “talk about the dangers of AI without considering how this impacts Google”. “A part of myself now regrets my life’s work” due to his concerns. “It is hard to see how you can prevent the bad actors from using AI for bad things”.

Already in 2017, Hinton called for an international ban on lethal autonomous weapons.

Now: “It’s not inconceivable that AI could wipe out humanity”. “We have to think hard about how to control” AI systems capable of self-improvement.

He is “worried that AI technologies will in time upend the job market” and take away more than just “drudge work”.

## AI and society

Strike of screen actors in Hollywood: against one-time payment of extras for arbitrary reproduction by AI. “Existential threat”.

IP rights: is it ok for chatbots to use protected IP? Should OpenAI pay for the use of a book?

[Btw: I do not think that it used Jürgen's and my book mca, because on prompting for the “iterated Frobenius algorithm” it returned mathematically-sounding gibberish.]

## Attempts at IP protection

### **“The Battle Over Books<sup>3</sup> Could Change AI Forever.**

Copyright activists are on a mission to wipe a popular generative AI training set from the internet. Success could alter the industry—and who controls it.”

They identified 150 books in this large data set and the authors filed Digital Millennium Copyright Act takedown notices in the US against a hosting organization—which then complied.

Last week: Authors Guild with John Grisham, George R.R. Martin, David Baldacci, Jonathan Franzen, and others filed a complaint at a Federal Court in New York. They accuse OpenAI of “systematic theft at a large scale” of copyright-protected material.

One “effect”: Amazon’s Kindle Direct program limits new submissions of an author—to three books per day.

## AI and society

Intransparent systems.

Job description by OpenAI: “**Introducing Superalignment.** We need scientific and technical breakthroughs to steer and control AI systems much smarter than us. To solve this problem within four years, we’re starting a new team and ... looking for excellent ML researchers and engineers to join us.”

Will this help? Whom?

EU: plans to require disclosure of copyrighted material used, and labelling of AI-generated output.

US: some big players agreed to watermark AI-generated content.  
Several controversies.

## Take-home messages

- ▶ Chatbots are here to stay.
- ▶ Computer algebra community: what are benefits and backdraws for us? Play with ChatGPT!
- ▶ And for society in general?

Thank you