Programming for mathematical research

Ken Jacobs, Luca Schaffler
University of Georgia

July 12, 2016

Motivation

Why would you use a computer to help your research?

Motivation

Why would you use a computer to help your research?

- To build intuition;

Motivation

Why would you use a computer to help your research?

- To build intuition;
- To actually prove a theorem (working case-by-case);

Motivation

Why would you use a computer to help your research?

- To build intuition;
- To actually prove a theorem (working case-by-case);
- To generate supporting examples for your theory.

Good and bad problems for programming

Good kinds of problems:

- Something that involves enumeration of finitely many cases;
- Visualization;
- Something you know there is an efficient package for already.

Good and bad problems for programming

Good kinds of problems:

- Something that involves enumeration of finitely many cases;
- Visualization;
- Something you know there is an efficient package for already.

Bad kinds of problems:

- something which is too simple;
- complicated expressions with many indeterminates;
- too much work to tell the computer how to do it.

Bad problem 1: too easy

Does the homogeneous polynomial

$$F(X, Y) = 3X^3Y + 3X^2Y^2 + X^4 - 6Y^4$$

factor over $\mathbb{Z}[X, Y]$?

Bad problem 1: too easy

Does the homogeneous polynomial

$$F(X, Y) = 3X^3Y + 3X^2Y^2 + X^4 - 6Y^4$$

factor over $\mathbb{Z}[X, Y]$?

- F is homogeneous and $Y \nmid F$, so it is enough to consider

$$G(X) := F(X, 1) = 3X^3 + 3X^2 + X^4 - 6$$

Bad problem 1: too easy

Does the homogeneous polynomial

$$F(X, Y) = 3X^3Y + 3X^2Y^2 + X^4 - 6Y^4$$

factor over $\mathbb{Z}[X, Y]$?

- F is homogeneous and $Y \nmid F$, so it is enough to consider

$$G(X) := F(X, 1) = 3X^3 + 3X^2 + X^4 - 6$$

- Reorder the terms

$$G(X) = X^4 + 3X^3 + 3X^2 - 6$$

Bad problem 1: too easy

Does the homogeneous polynomial

$$F(X,Y) = 3X^3Y + 3X^2Y^2 + X^4 - 6Y^4$$

factor over $\mathbb{Z}[X,Y]$?

- F is homogeneous and $Y \nmid F$, so it is enough to consider

$$G(X) := F(X,1) = 3X^3 + 3X^2 + X^4 - 6$$

- Reorder the terms

$$G(X) = X^4 + 3X^3 + 3X^2 - 6$$

- Eisenstein's criterion $\rightarrow$ $G(X)$ is irreducible $\rightarrow$ $F(X,Y)$ does not factor!

Bad problem 2: too general

Let $p(z) = a_d z^d + \dots + a_0$ be a polynomial, and let $p^{(n)}(z) = \underbrace{p \circ p \circ \cdots \circ p}_{n \text{ times}}(z)$. For certain k, compute

$$\lim_{n\to\infty} \frac{1}{d^n} \log \max(1, |p^{(n)}(k)|) \ .$$

Bad problem 2: too general

Let $p(z) = a_d z^d + \ldots + a_0$ be a polynomial, and let $p^{(n)}(z) = \underbrace{p \circ p \circ \cdots \circ p}_{n \text{ times}}(z)$. For certain k, compute

$$\lim_{n \to \infty} \frac{1}{d^n} \log \max(1, |p^{(n)}(k)|) \ .$$

Too general $\to$ look at special cases:

Bad problem 2: too general

Let $p(z) = a_d z^d + ... + a_0$ be a polynomial, and let $p^{(n)}(z) = \underbrace{p \circ p \circ \cdots \circ p}_{n \text{ times}}(z)$. For certain k, compute

$$\lim_{n \to \infty} \frac{1}{d^n} \log \max(1, |p^{(n)}(k)|) \ .$$

Too general $\to$ look at special cases:

- $p(z) = z^d$ or $p(z) = z + t$, and $k = 0$, then the limit is 0.

Bad problem 2: too general

Let $p(z) = a_d z^d + \ldots + a_0$ be a polynomial, and let $p^{(n)}(z) = \underbrace{p \circ p \circ \cdots \circ p}_{n \text{ times}}(z)$. For certain k, compute

$$\lim_{n\to\infty} \frac{1}{d^n} \log \max(1, |p^{(n)}(k)|) \ .$$

Too general $\rightarrow$ look at special cases:

- $p(z) = z^d$ or $p(z) = z + t$, and $k = 0$, then the limit is 0.
- $p(z) = z^d + t$ and $k = 0$ is tractable for a computer

Bad problem 3: too bothersome to ask a computer

Count the number of $\mathbb{Z}^2$ lattice points in the region bounded by $y = 2/3x + 4$, $y = 3/2x - 4$, $y = -2x + 2$, $y = -1/3x - 5$.

Sample problem 1: visualization

Let $p(z) = z^2 + c$ for $c \in \mathbb{C}$, and define

$$g(c) := \lim_{n\to\infty} \frac{1}{2^n} \log \max(1, |p^{(n)}(0)|) \ .$$

Sample problem 1: visualization

Let $p(z) = z^2 + c$ for $c \in \mathbb{C}$, and define

$$g(c) := \lim_{n\to\infty} \frac{1}{2^n} \log \max(1, |p^{(n)}(0)|) \ .$$

Question: How does $g(c)$ vary in c?

Sample problem 2: how many elements in a group

Consider the following two subgroups of S_7:

$$G_1 = \{\mathrm{id}, (34)(65), (47)(16), (37)(15), (156)(473), (165)(374)\},$$

$$G_2 = \{\mathrm{id}, (12)(56), (25)(16), (26)(15)\}.$$

Sample problem 2: how many elements in a group

Consider the following two subgroups of S_7:

$$G_1 = \{\mathrm{id}, (34)(65), (47)(16), (37)(15), (156)(473), (165)(374)\},$$

$$G_2 = \{\mathrm{id}, (12)(56), (25)(16), (26)(15)\}.$$

Question: How many elements does the subgroup of S_7 generated by G_1 and G_2 have?

Sample problem 3: rational points on curves

Consider the elliptic curve given in Weierstrass form by

$$E : y^2 = x^3 + 8 \ .$$

Sample problem 3: rational points on curves

Consider the elliptic curve given in Weierstrass form by

$$E : y^2 = x^3 + 8 \ .$$

Question:

- Over $\mathbb{Q}$, does the point $P(1, 3)$ have infinite or finite order?
- Over $\mathbb{Q}(\sqrt{2})$, does the point $Q(0, 2\sqrt{2})$ have infinite or finite order on E?

Sample problem 4: ray in a cone?

In $\mathbb{R}^5$, let C be the cone with vertex at the origin and whose extremal rays are generated by

$$(10, 1, 3, -1, 4),\ (-3, 0.5, 5, 7, 2),\ (1, 6, 3, 7, 11),$$

$$(9, 1, 1, 3, 5),\ (5, 0, 1, 4, -1),\ (6, 1, 2, 7, 3).$$

Sample problem 4: ray in a cone?

In $\mathbb{R}^5$, let C be the cone with vertex at the origin and whose extremal rays are generated by

$$(10, 1, 3, -1, 4),\ (-3, 0.5, 5, 7, 2),\ (1, 6, 3, 7, 11),$$

$$(9, 1, 1, 3, 5),\ (5, 0, 1, 4, -1),\ (6, 1, 2, 7, 3).$$

Question: Is the vector $(1, 1, 2, 2, 3)$ in C or not?

Free software

- Sage;
- GAP;
- Macaulay2;
- LRS, porta;
- Polymake;
- Python;
- C, C++.

Expensive software the department has for you

- Mathematica;
- Matlab;
- Maple;
- Magma;
- Geometer's Sketchpad;
- `vlab.uga.edu`

Expensive hardware the department / university has for you

- Your office computer (should have all licensed programs pre-installed)
- 6th floor computers – faster processors, more memory; requires access from `help@math.uga.edu`
- UGA cluster (requires remote access)

Documentation

- Mathematica: `http://reference.wolfram.com/language/`
- LRS: `http://cgm.cs.mcgill.ca/~avis/C/lrslib/USERGUIDE.html`
- Sage: `http://doc.sagemath.org/html/en/`
- GAP: `http://www.gap-system.org/Doc/doc.html`
- Polymake: `https://polymake.org/doku.php/documentation`
- Macaulay2: `http://www.math.uiuc.edu/Macaulay2/`
- Matlab: `http://www.mathworks.com/help/matlab/`
- Maple: `http://www.maplesoft.com/documentation_center/`
- Porta: `http://comopt.ifi.uni-heidelberg.de/software/PORTA/`