Administrivia

Course website:
cs.sfu.ca/~rgandrew/courses/cmpt981-fa26

Office hours: Thurs 3-4pm,
TASC1 9405

Crowdmark for HW, CourSys for discussion & communicating w/ course staff

Responsibilities

1) Homework.

5 assignments, 40% of grade.
Collab okay, write individually.
No genAI.

Released after lecture on Wed, due 2 weeks later

Homework 0 due in one week

2) Project

In groups of 2 or 3, read a paper, present it, write about what you learned.

Presentations during final exam slot, time TBD.

Course Topics

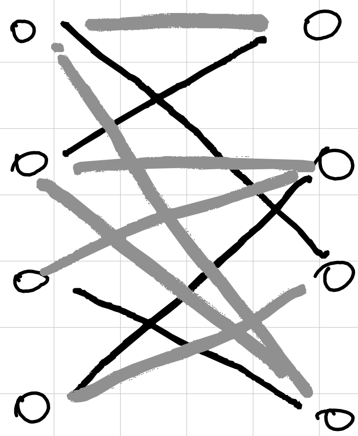
- Algorithms for basic tasks in algebra
  - Polynomial arithmetic
  - Polynomial GCD & Resultants
  - Systems of polynomial equations
  - Matrix multiplication & linear algebra

- Algebraic complexity theory
  - Permanent vs determinant
  - Algebraic circuits
  - Polynomial identity testing & derandomization.

- Surprising applications.
  - Fast exponential-time algos
  - Coding theory
  - Combinatorial optimization
  - Space complexity.

Motivating example: bipartite matching

Input: bipartite graph G



Output: maximum-cardinality <u>matching</u>

Classic algo: augmenting paths
$O(nm)$ time, but
highly sequential

Question: find max matching in parallel?

Answer: $O(\log^2 n)$ parallel time using algebra

Integer Multiplication

Input: n-digit integers a, b

Output: product ab.

$O(n^2)$ time - grade school algo

$O(n^{\log_2 3}) \approx O(n^{1.58})$ Karatsuba 1960

$O(n^{1+\varepsilon})$ Toom & Cook 1963

$O(n \log n \log\log n)$ Schönhage & Strassen 1968

$O(n \log n \log \cdots \log n)$ Fürer 2007

$O(n \log n)$ Harvey & van der Hoeven 2019

Karatsuba. D & C

$$a = a_1 2^{n/2} + a_0$$

$$b = b_1 2^{n/2} + a_0$$

$$ab = a_1 b_1 2^n + (a_0 b_1 + a_1 b_0) 2^{n/2} + a_0 b_0.$$

Obvious: 4 multiplies

$$T(n) \leq 4 \cdot T(n/2) + O(n^2)$$

$$\Rightarrow T(n) \leq O(n^2).$$

Clever: 3 multiplies

$$m_1 = a_0 b_0 \qquad m_2 = a_1 b_1$$

$$m_3 = (a_0 + a_1)(b_0 + b_1)$$

$$a_0 b_1 + a_1 b_1 = m_3 - m_1 - m_2$$

What is going on? Polynomial interp.

define $a(x) := a_1 x + a_0$

$$b(x) := b_1 x + b_0$$

$$c(x) := a(x) b(x)$$

$$= a_1 b_1 x^2 + (a_0 b_1 + a_1 b_0) x + a_0 b_0.$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} c(0) \\ c(1) \\ c(2) \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix}^{-1} \begin{pmatrix} c(0) \\ c(1) \\ c(2) \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ -3/2 & 2 & -1/2 \\ 1/2 & -1 & 1/2 \end{pmatrix}$$

Toom-Cook: use higher degree polynomials!