6.897
L8.3
Mar. 1, 2005

Avoiding cancelation:

- conceptually want a symbolic matrix:

$$(\text{symb } A)_{ij} = \begin{cases} a_{ij}, & \text{if } A_{ij} \neq 0 \quad (\text{for us, } =1) \\ 0, & \text{if } A_{ij} = 0 \end{cases}$$

- det symb Z = polynomial in $\leq n^2$ variables of degree $\leq n$.
- $(\text{adj symb } (A+I))_{ij}$ = zero polynomial 0
  $\Leftrightarrow$ there's no edge from i to j
- instead settle for random matrix:

$$(\text{rand } A)_{ij} = \begin{cases} \text{independent random number chosen uniformly between } 0 \text{ \& } p-1, & \text{if } A_{ij} \neq 0 \\ 0, & \text{if } A_{ij} = 0 \end{cases}$$

Lemma: $\Pr\{$nonzero polynomial of degree d, evaluated at uniform random inputs $\equiv 0 \pmod p\} \leq d/p$ [Zippel 1979; Schwartz 1980]

(p: prime; d/p: independent of #variables)

$\Rightarrow$ if det symb $Z \neq 0$ then $\Pr\{\text{det rand } Z = 0\} \leq n/p$

- choose prime $p \geq n^c$ $\Rightarrow \leq 1/n^{c-1}$

$\Rightarrow \Pr\{$adj rand $(A+I)$ has more zeros than adj symb $(A+I)\}$
$\leq 1/n^{c-3}$ (by union bound)

$\Rightarrow$ if data structure runs for polynomial time, can make $\Pr\{\text{any errors}\} \leq 1/n^{c'}$ for any desired $c' > 0$
(correct with high probability)

- use rebuilding trick to allow DS to run longer than fixed polynomial & to allow n changing
- also, det symb $(A+I) \neq 0$
  so det rand $(A+I) \neq 0$ w.h.p.
  $\Rightarrow$ need to maintain dynamic adjugate, or inverse.