Recap. \[ G = (V, P, E) \] bipartite

\[ |V| = |P| = n \]

\[ B = n \times n \text{ matrix of formal variables} \]

\[ B_{ij} = \begin{cases} x_{ij} & \text{if } (ij) \in E \\ 0 & \text{if not} \end{cases} \]

\[ \det(B) \neq 0 \iff G \text{ has a perfect matching} \]

Schwartz–Zippel Lemma.

If \( P(x_1, \ldots, x_n) \) is a non-zero polynomial with coefficients in a field \( F \) and \( x_1, \ldots, x_m \) are sampled independently at random from \( S \subseteq F \) with \( |S| = s \),

\[ \Pr\left( P(x_1, \ldots, x_n) = 0 \right) \leq \frac{m^2}{s} \]
where \(d\) is the max exponent of any variable in any monomial.

\[ P(x_1, \ldots, x_n) = \sum_{i=0}^{e} Q_i(x_1, \ldots, x_{m-1}) \cdot x_i^d \]

**Proof** Induction on \(m\).

Base case: \(m = 0\).

\(P\) is a nonzero constant, so

\[ P(c, p = 0) = 0 \]

Induction step: \(m > 0\).

If \(P(x_1, \ldots, x_m) = 0\) one of two things must happen:

1. \(Q_c(x_1, \ldots, x_{m-1}) = 0\)
   \[ P_{\text{induct. hyp.}} \leq \frac{(m-1)d}{5} \]

2. \(Q_c(x_1, \ldots, x_{m-1}) \neq 0\) but
   \[ P(x_1, \ldots, x_m) = 0 \]
   Then \(x_m\) is one of the roots of
   \[ R(x) = \sum_{i=0}^{e} Q_i(x_1, \ldots, x_{m-1}) \cdot x_i^d \]
   This equation has \(\leq c\) solutions.
   So \(Pr(x_m\text{ is among the roots}) \leq \frac{c}{5} \leq \frac{1}{5}\)
Exercise: What goes wrong in the proof if the polynomial $P$ is defined over a ring rather than a field?

\[ P(x_1, x_2, x_3) = x_1 x_2 x_3 \]

in the ring $\mathbb{Z}/(8)[x_1, x_2, x_3]$.

Sample $x_1, x_2, x_3$ from $\{0, 2, 4, 6\}$.

Definition: Let $\omega$ be the smallest constant such that two $n \times n$ matrices can be multiplied in time $O(n^{\omega+\varepsilon})$ for all $\varepsilon > 0$.

For remainder of lecture $O^*(\omega)$ denotes "$O(n^{\omega+\varepsilon})$ as $\varepsilon \downarrow 0$".

Deciding $P$ det$(A) \neq 0$ in $O^*(\omega)$.

First obs: det$(A) \neq 0 \iff$ det$(A^T A) \neq 0$. 
From now on, $C$ is a symmetric positive semidefinite matrix. We attempt to invert $C$.

\[ C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} \]

\[ \begin{pmatrix} 1 & 0 \\ -C_{21}C_{11}^{-1} & I \end{pmatrix} C = \begin{pmatrix} C_{11} & C_{12} \\ 0 & C_{22} - C_{21}C_{11}^{-1}C_{12} \end{pmatrix} \]

\[ \begin{pmatrix} 1 & 0 \\ -C_{21}C_{11}^{-1} & I \end{pmatrix} C \begin{pmatrix} 1 & -C_{11}^{-1}C_{12} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} C_{11} & 0 \\ 0 & C_{22} - C_{21}C_{11}^{-1}C_{12} \end{pmatrix} \]

$T(n)$ is the time to invert an $n \times n$ SPD matrix. We have

\[ T(n) = 2 \cdot T\left(\frac{n}{2}\right) + O(n^\omega) \]

\[ = \Theta(n^\omega). \]

$2 \leq \omega < 2.373$
Example algorithmic applications:

1. Triangle detection in $O^*(n^4)$ time.
2. $k$-clique detection in

\[O^*(n^{(n/k)^{1/3}}) \leq O^*(n^{(n/k)^{1/3}}) \leq O(n^{0.8k}).\]

Mucka & Sankowski (2006) improved on Lovász's algorithm to be able to solve the perfect matching search problem in randomized $O^*(n^4)$ time.

Fact: \exists perfect matching containing edge $(i,j)$ if and only if the $(j,i)$ entry of $B^{-1}$ is nonzero and $B_{ij} \neq 0$.

Proof: $(B^{-1})_{ji} = \pm \frac{\det(B \text{ with row } i, \text{ col } j \text{ deleted})}{\det(B)}$.