There are also oracles $C$ such that $NP^C \neq P^C$, so if $NP=P$ happens to be true, we won't be able to prove it by general techniques at the level of this course either.
 INSTANCE: Three n x n matrices A, B, C. We can say the problem belongs to \( \text{TIME}[O(n^3)] \).

**Goal:** Is \( A \cdot B = C \)?

**Double check matrix multiplication in time \( O(n^w) \) where \( w \leq 2.37327\ldots \)

**However:** if we can stand an exchange of saying “yes” when it’s false, we can get \( O(n^2) \) time.

**Fact:** Over any field \( F \), if

\[
A \neq C, \quad \text{then} \quad \Pr_{x \in F^n} \left[ (A \cdot x)(C \cdot x) \right] = \frac{1}{2}
\]

**Example:**

- \( \text{Found a vector } x, \text{ where } x \cdot C = 1 \) but \( x \cdot A = 0 \).

**Note:**

- \( \text{Exchange: } \) If we get “no,” say “I am unsure.”

- \( \text{Exchange: } \) If we get “yes,” say “I am sure about saying ‘yes.’”

- \( \text{Exchange: } \) If \( F = GF(q) \), \( q \) is a prime.

---

**Definition:** A language \( A \) belongs to \( \text{BPP} \) if there is a witness predicate \( R(x, y) \)

dealable in \( O(1 \cdot |x|^{O(1)}) \) time such that

\[
1/n = \Pr_{y \in \{0, 1\}^n} \left[ R(x, y) \right] \geq \frac{2}{3}
\]

**Case 1:** \( x \in A \) then \( \Pr_{y \in \{0, 1\}^n} \left[ R(x, y) \right] \geq \frac{2}{3} \).

**Case 2:** \( x \notin A \) then \( \Pr_{y \in \{0, 1\}^n} \left[ R(x, y) \right] < \frac{1}{3} \).

**If we get the witness \( y = 1^n \) in place of \( \geq \frac{2}{3} \), then \( A \in \text{RP} \).

**If we get this with \( y = 0^n \) in place of \( \geq \frac{2}{3} \), then \( A \notin \text{RP} \).

Note that the second condition makes \( x \in A \) as \( (y \cdot n) \) is equal to \( R \). RP.

---

**Proof:**

- **Claim:** A family \( \{R_i(x, y)\}_{i \geq 0} \) is \( \text{RP} \).

**Example:**

- **Claim:** A family \( \{R_i(x, y)\}_{i \geq 0} \) is \( \text{RP} \).

**Proof:** Is \( i \) it already done when multiplied out?