

# Back to the Polynomial Identity Test

The probability of a wrong answer in one run of the algorithm is  $1/100$ . Runs of the algorithms are **independent** (i.e., the probability of error in each run is independent of other runs.) It's enough to get a correct answer in one of the runs.

The probability of a wrong answer in  $k$  runs of the algorithm is  $(\frac{1}{100})^k$ .

# The Birthday Paradox

What is the probability that among  $m$  people no two have the same birthday?

Assumptions:

1. All birthdays are equally likely.
2. Birthdays are independent events.

The sample space is the set of all vectors  $S = \{(b_1, \dots, b_m) | b_i \in [1, \dots, N]\}$ .

We need to compute  $Pr(E)$  where  $E = \{(b_1, \dots, b_m) | b_i \neq b_j \text{ for all } i \neq j\}$ .

How many different atomic events are counted in  $E$ ?

The number of possible  $m$  different birthdays is  $N.(N - 1).(N - 2) \dots (N - m + 1)$

$$\Pr(E) = \frac{N.(N-1).(N-2)\dots(N-m+1)}{N^m}$$

$$= \prod_{i=0}^{m-1} (1 - i/N)$$

$$\leq \prod_{i=0}^{m-1} e^{-i/N} = e^{-\sum_{i=0}^{m-1} i/N} = e^{-m(m-1)/2N}$$

For  $m = \sqrt{2N} + 1 \leq 28$ ,

$$\Pr(E) < 1/e < 1/2.$$

## Alternate Analysis

Assume that we choose one birthday after the other independently and uniformly at random from  $[1 \dots N]$ .

Let  $E_i$ : "the  $i$ th choice is different from the first  $i - 1$  choices".

$$\Pr(\cap_{i=1}^m E_i) = \Pr(E_1) \Pr(E_2|E_1) \Pr(E_3|E_2 \cap E_1) \dots \Pr(E_m | \cap_{i=1}^{m-1} E_i) = \prod_{i=1}^m (1 - \frac{i-1}{N})$$

### Principle of Deferred Decisions.

# Verifying Matrix Multiplication

Given three  $n \times n$  integer matrices  $A$ ,  $B$ , and  $C$ , verify whether

$$AB = C$$

Simple matrix multiplication takes  $\Theta(n^3)$  steps. There exist a  $\Theta(n^{2.37})$  algorithm.

# Randomized Algorithm

Choose a random vector  $\bar{r} = (r_1, r_2, \dots, r_n) \in \{0, 1\}^n$ .

Compute  $A(B\bar{r})$  and  $C\bar{r}$ .

If  $A(B\bar{r}) \neq C\bar{r}$ , then output  $AB \neq C$ .

Else output  $AB = C$ .

Takes  $\Theta(n^2)$  time.

## Bounding the Error Probability

**Theorem 1.** *If  $AB \neq C$ , and  $\bar{r}$  is chosen uniformly at random from  $\{0, 1\}$ , then*

$$\Pr(AB\bar{r} = C\bar{r}) \leq 1/2$$

**Proof.** Let  $D = AB - C \neq 0$ .  $D$  has some non-zero entry. W.l.o.g let it be  $d_{11}$ .

For  $D\bar{r} = 0$ , we should have

$$\sum_{j=1}^n d_{1j}r_j = 0, \text{ i.e.,}$$

$$r_1 = -\frac{\sum_{j=2}^n d_{1j}r_j}{d_{11}}$$

Set  $r_n, \dots, r_2, r_1$  one by one.

The equality holds in at most one choice of  $r_1$ .  $\square$