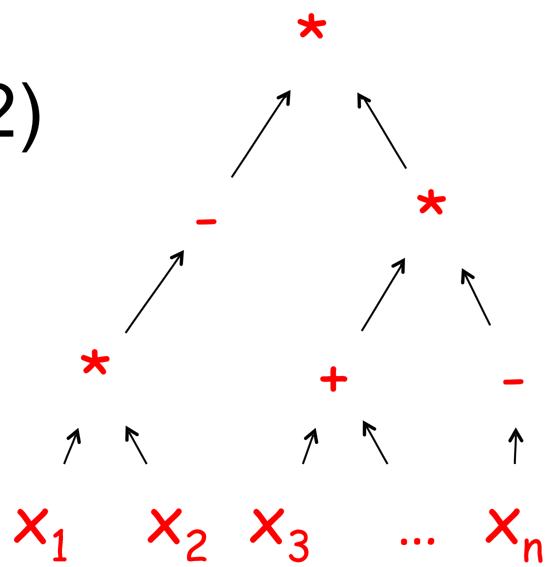
Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \dots, x_n)$ as arithmetic formula (fan-out 1):
  - multiplication (fan-in 2)
  - addition (fan-in 2)
  - negation (fan-in 1)



Polynomial identity testing

- Question: Is p identically zero?
  - i.e., is $p(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbf{F}^n$
  - (assume $|\mathbf{F}|$ larger than degree…)

- "polynomial identity testing" because given two polynomials p, q, we can check the identity $p \equiv q$ by checking if $(p - q) \equiv 0$

Polynomial identity testing

- try all $|\mathbf{F}|^n$ inputs?
  - may be exponentially many
- multiply out symbolically, check that all coefficients are zero?
  - may be exponentially many coefficients
- can randomness help?
  - i.e., flip coins, allow small probability of wrong answer

Polynomial identity testing

Lemma (Schwartz-Zippel): Let

$$p(x_1, x_2, \ldots, x_n)$$

be a total degree d polynomial over a field **F** and let S be any subset of **F**. Then if p is not identically 0,

$$\Pr_{r_1, r_2, \ldots, r_n \in S}[\, p(r_1, r_2, \ldots, r_n) = 0] \le d/|S|.$$

Polynomial identity testing

- Proof:
  - induction on number of variables n
  - base case: n = 1, p is univariate polynomial of degree at most d
  - at most d roots, so

$$\Pr[\, p(r_1) = 0] \le d/|S|$$

Polynomial identity testing

- write $p(x_1, x_2, \ldots, x_n)$ as

$$p(x_1, x_2, \ldots, x_n) = \Sigma_i \, (x_1)^i \, p_i(x_2, \ldots, x_n)$$

- k = max. i for which $p_i(x_2, \ldots, x_n)$ not id. zero
- by induction hypothesis:

$$\Pr[\, p_k(r_2, \ldots, r_n) = 0] \le (d-k)/|S|$$

- whenever $p_k(r_2, \ldots, r_n) \neq 0$, $p(x_1, r_2, \ldots, r_n)$ is a univariate polynomial of degree k

$$\Pr[p(r_1,r_2,\ldots,r_n)=0 \mid p_k(r_2,\ldots,r_n) \neq 0] \le k/|S|$$

Polynomial identity testing

$$\Pr[\, p_k(r_2, \ldots, r_n) = 0] \le (d-k)/|S|$$

$$\Pr[p(r_1,r_2,\ldots,r_n)=0 \mid p_k(r_2,\ldots,r_n) \neq 0] \le k/|S|$$

– conclude:

$$\Pr[\, p(r_1, \ldots, r_n) = 0] \le (d-k)/|S| + k/|S| = d/|S|$$

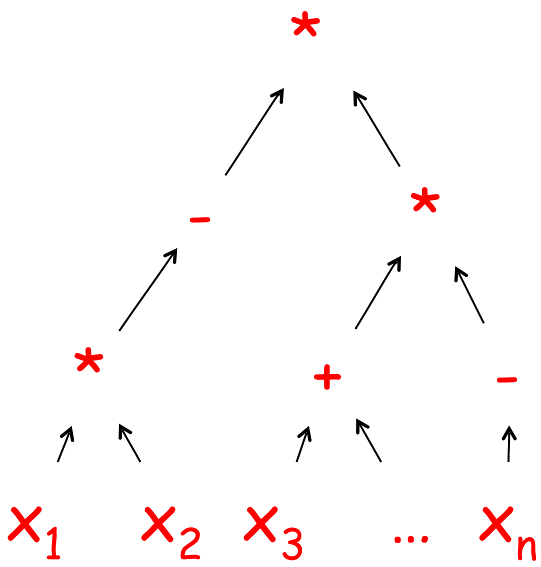
– Note: can add these probabilities because

$$\Pr[E_1] = \Pr[E_1|E_2]\Pr[E_2] + \Pr[E_1|\neg E_2]\Pr[\neg E_2]$$

$$\le \Pr[E_2] + \Pr[E_1|\neg E_2]$$

Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \ldots, x_n)$



- Is p identically zero?
- Note: degree d is at most the size of input

Polynomial identity testing

- randomized algorithm: field **F**, pick a subset $S \subset \mathbf{F}$ of size 2d
  - pick $r_1, r_2, \ldots, r_n$ from S uniformly at random
  - if $p(r_1, r_2, \ldots, r_n) = 0$, answer “yes”
  - if $p(r_1, r_2, \ldots, r_n) \neq 0$, answer “no”

- if p identically zero, never wrong
- if not, Schwartz-Zippel ensures probability of error at most ½