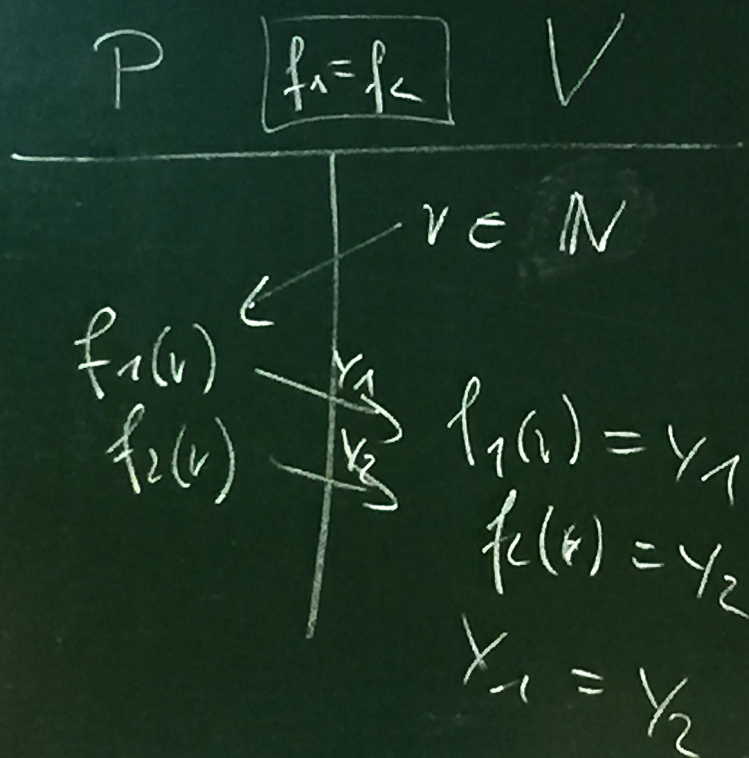


## Interactive Proof Systems



$$(x-2)(x-3) \stackrel{?}{=} x^2 - 6x + 7$$

Lemma A polynomial of degree  $d$  has

1. it could be 0
2. or it has at most  $d$  roots.

# 18 IP = PSPACE

$$f_1(x) - f_2(x) \stackrel{?}{=} 0$$

random  $x \in \mathbb{R}$

1.  $p_0(x) = c$

2.  $p_1(x) = ax + b$

3.  $p_2(x) = p_1(x)(x - x_0)$   
 or irreducible  
 $\vdots$   $64 \ 0$

## IP = PSPACE

1.  $IP \subseteq PSPACE$

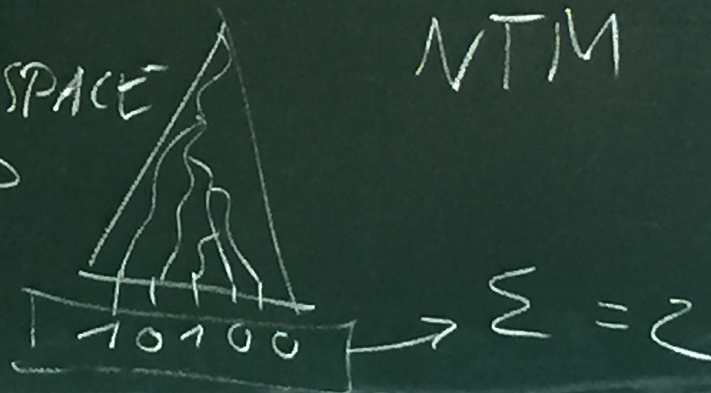
2.  $PSPACE \subseteq IP$

$\#P \subseteq IP$

$\#P \in PSPACE$

$NP \subseteq \#P$

NTM



# 18 IP = PSPACE

$$\#SAT = \left\{ (\bar{\Phi}, k) \mid \bar{\Phi} \text{ is a CNF} \right. \\ \left. \text{with exactly } k \text{ assignments} \right\}$$

$$\bar{\Phi} = (x_1 \vee x_2) \wedge (\bar{x}_1 \vee x_2)$$

$x_1$	$x_2$	$\bar{\Phi}(x_1, x_2)$
0	0	0
0	1	1
1	0	0
1	1	1

$$(\bar{\Phi}, 2) \in \#SAT$$

$$(\bar{\Phi}, 1) \notin \#SAT$$

# 18 IP = PSPACE

Arithmetization GF(2<sup>k</sup>)  
mod prime  
Σ<sub>p</sub>

Boolean functions operator	$\mathbb{R}$	$\neg$	$\wedge$
0	0	0 1	0 1
1	1	1 0	0 0
$x_1 \wedge x_2$	$x_1 \cdot x_2$		1 0
$\neg x$	$1 - x$		
$x_1 \vee x_2$ $= \neg(\neg x_1 \wedge \neg x_2)$	$1 - (1 - x_1)(1 - x_2)$		
	$x_1 * x_2$		

$x_1$	0	1
$x_2$	0	1
$*$	0	1
	1	1

# 18 IP = PSPACE

$$x_1 + x_2 \pmod 3$$

3, 5, 7, 11, 13...

$$x_1 = x_2 \pmod 3$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$(x^2 - 2x + 1) \pmod p$$

RSA

# 18 IP = PSPACE

$$\# \text{assignments} = \sum_{x_1, \dots, x_n \in \{0,1\}} f(x_1, \dots, x_n) =: f()()$$

$f$  is a satisfication of  $\overline{\Phi}$

$$\overline{\Phi} = (x_1 \vee x_2) \wedge (\overline{x_1} \vee x_3)$$

$$f(x_1, x_2, x_3) = (1 - (1 - x_1)(1 - x_2)) \cdot$$

$$(1 - x_1 \cdot (1 - x_3))$$

# 18 IP = PSPACE

$$=: f_0 \quad f_2(x_1, x_2) := \sum_{x_3 \in \{0,1\}} f(x_1, x_2, x_3)$$

$$\begin{aligned}
 &= (1 - (1-x_1)(1-x_2))(1-x_1) \\
 &\quad + (1 - (1-x_1)(1-x_2)) \cdot 1 \\
 &= (2-x_1)(1 - (1-x_1)(1-x_2))
 \end{aligned}$$

$$f_1(x_1) = \sum_{x_2, x_3 \in \{0,1\}} f(x_1, x_2, x_3) = \sum_{x_2 \in \{0,1\}} f_2(x_1, x_2)$$

$$= (2-x_1)(1 - (1-x_1)) + (2-x_1)$$

$$f(1) = \sum_{x_1, x_2, x_3 \in \{0,1\}} f(x_1, x_2, x_3)$$

$$= \sum_{x_1 \in \{0,1\}} f_1(x_1)$$

$$= 2 \cdot 0 + 2 + 1 + 1$$

$$= 4$$

# 18 IP = PSPACE

$P(\mathbb{F}, k) \quad V$

---

claim  $f() = k$

send  $f_1(x_1)$   $\rightarrow$   $(-x_1^2 + x_1 + 2)$

check that  $f() = \sum_{x_1 \in \{0,1\}} f_1(x_1)$

$f() = f_1(0) + f_1(1)$

choose random  $v_1$

send  $f_2(v_1, x_2)$

coefficients  $\rightarrow$

$f_1(v_1) = \sum_{x_2 \in \{0,1\}} f_2(v_1, x_2)$

$= f_2(v_1, 0) + f_2(v_1, 1)$



# 18 IP = PSPACE

P	V
$f_3(v_1, v_2, v_3)$	random $v_2$
$\rightarrow f_2(v_1, v_2) = f_3(v_1, v_2, 0)$	
$\rightarrow f_3(v_1, v_2, v_3) = k ?$	random $v_3$

$P = \text{size of finite field}$

$$\frac{2}{P} + \frac{2}{P} + \frac{2}{P} \leq \frac{1}{3}$$

Prob to cheat in the 3rd round

$P \geq 18, P = 19$

# 18 $IP = PSPACE$

$PSPACE \subseteq IP$

$$QBF := \{ Q_1 x_1 Q_2 x_2 \dots Q_n x_n F(x_1 \dots x_n) \}$$

$Q_i \in \{\exists, \forall\}$ ,  $F$  is CNF

$$\{ Q_1 x_1 Q_2 x_2 \dots Q_n x_n F(x_1 \dots x_n) = 1 \}$$

$$\begin{aligned}
 & \text{" } \forall x_1 \exists x_2 \forall x_3 (x_1 \vee x_2) \wedge (x_1 \vee \overline{x_3}) \text{ " } \in QBF \\
 & \prod_{x_3 \in \{0,1\}} (1 - (1-x_1)(1-x_2)) \cdot (1 - (1-x_1)x_3)
 \end{aligned}$$

$QBF \in AP$ -complete ;  $AP = PSPACE$   
 $\in PSPACE$ -complete

$$f_i(x_1, \dots, x_n) = \begin{cases} 1, & Q_1 x_1 \dots Q_n x_n F(x_1, \dots, x_n) = 1 \\ 0, & \text{else} \end{cases}$$

$$f_0() = Q_1 x_1 \dots Q_n x_n \overline{F(x_1, \dots, x_n)}$$

Arithmetization.

# 18 IP = PSPACE

(\*) if  $Q_{i+1} = \forall$  :  $f_i(x_1, \dots, x_i) = f_{i+1}(x_1, \dots, x_i, 0) \cdot f_{i+1}(x_1, \dots, x_i, 1)$   
 if  $Q_{i+1} = \exists$  :  $f_i(x_1, \dots, x_i) = 1 - (1 - f_{i+1}(x_1, \dots, x_i, 0))(1 - f_{i+1}(x_1, \dots, x_i, 1))$

Prove  $f_0(1) = 1$

degree of  $f_i(x_1, \dots, x_m, x_i) \in \# \text{ clauses in } F = m$

how many rounds :  $n$

choose  $p \geq 3 \cdot n \cdot m$

$$\text{Prob. to cheat} \leq \frac{m}{3 \cdot n \cdot n} = \frac{1}{3 \cdot n}$$

$$\text{over } n \text{ rounds prob} \leq n \cdot \frac{1}{3 \cdot n} = \frac{1}{3}$$

