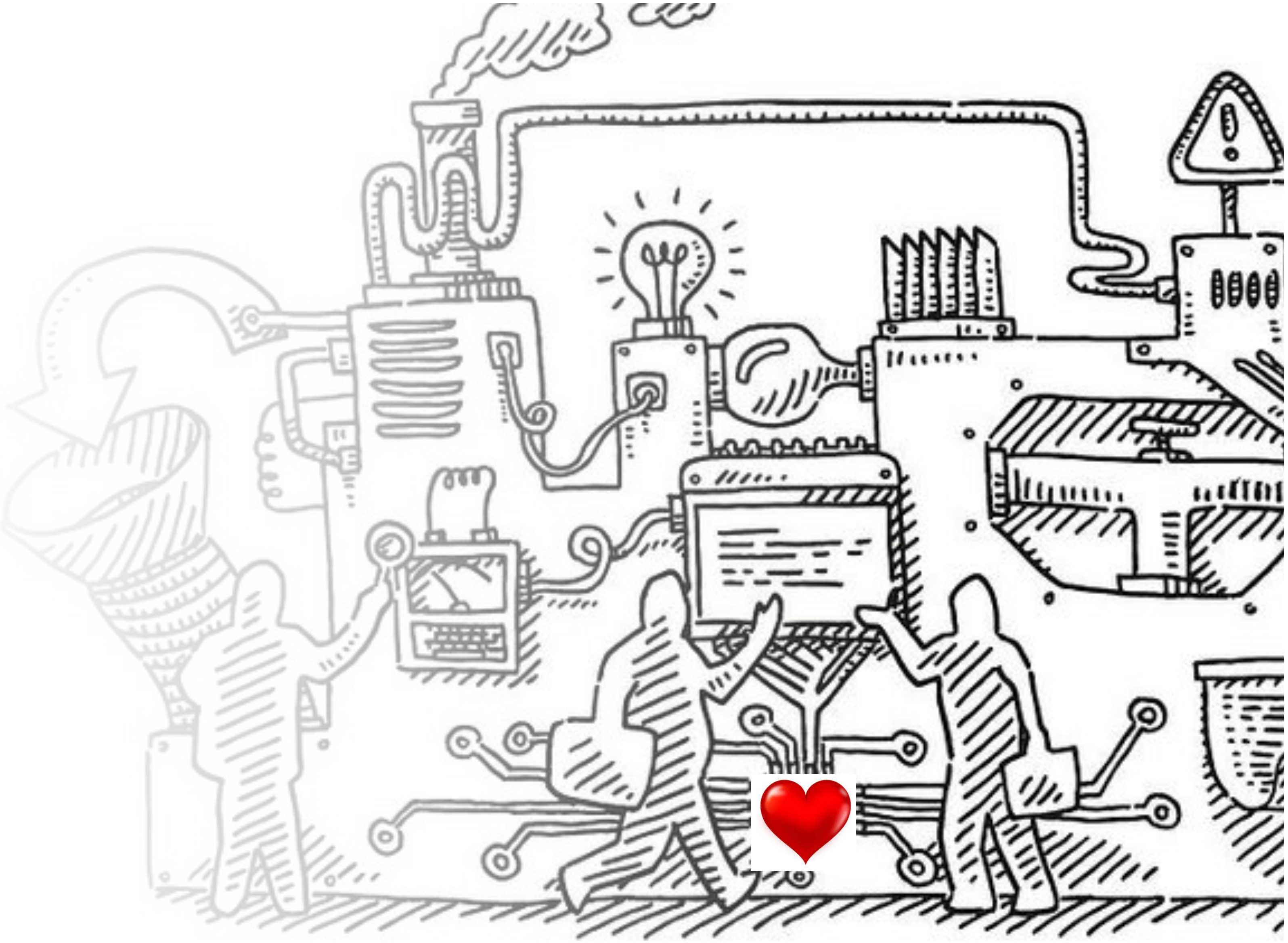
Linearity Testing and Low Degree Testing



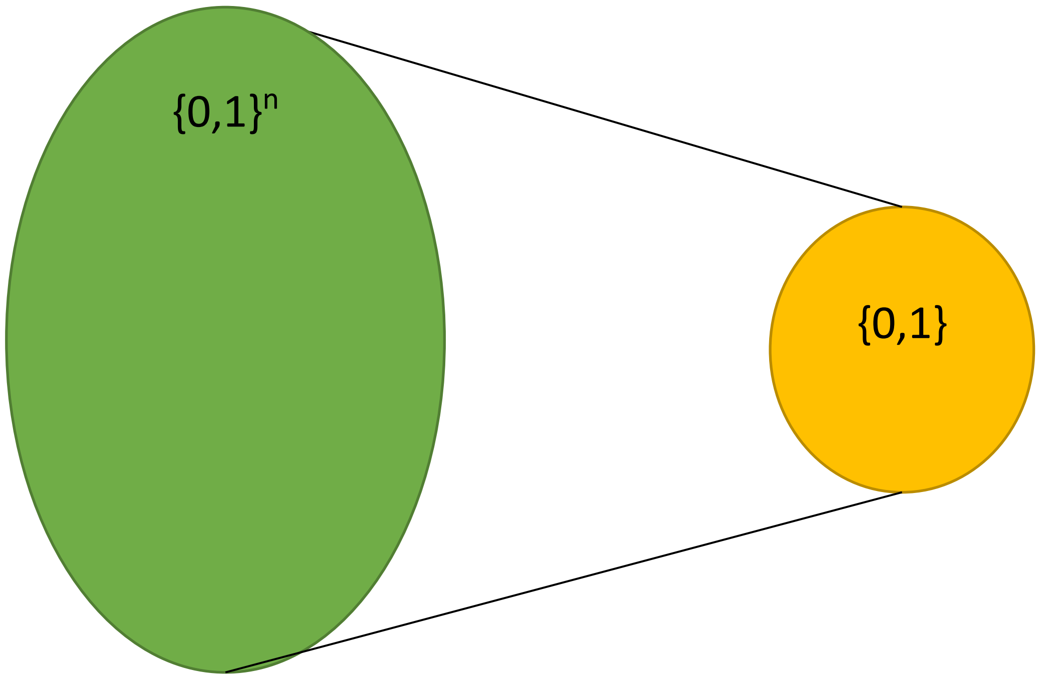
Dana Moshkovitz

UT Austin

Linear Functions

$h:\{0,1\}^n \to \{0,1\}$ is **linear** if $h(x) \equiv \Sigma a_i x_i$ for $a_1 \ldots a_n \in \{0,1\}$.

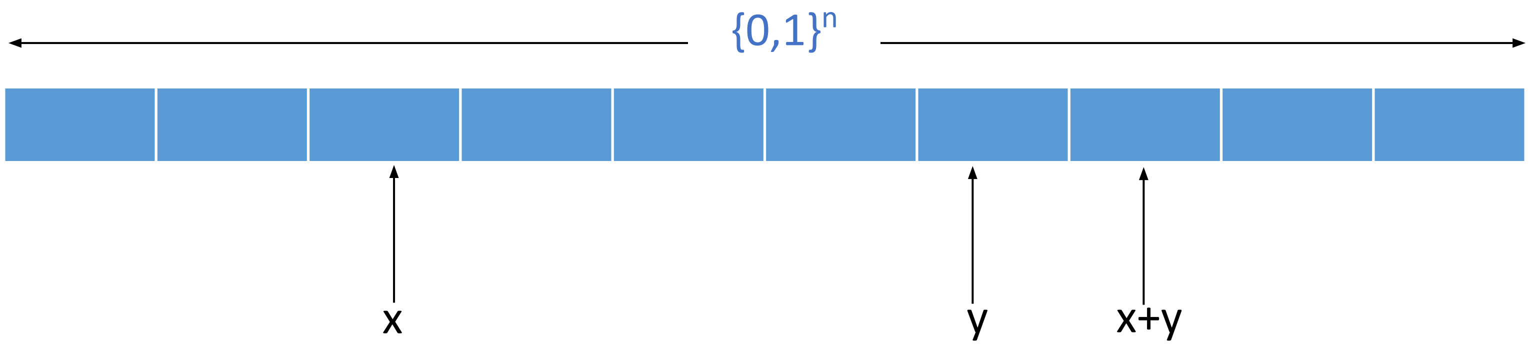
Equivalently, $h(x+y) = h(x)+h(y)$ for **all** $x,y \in \{0,1\}^n$.



Linearity Tester

Given access to f:$\{0,1\}^n \rightarrow \{0,1\}$:

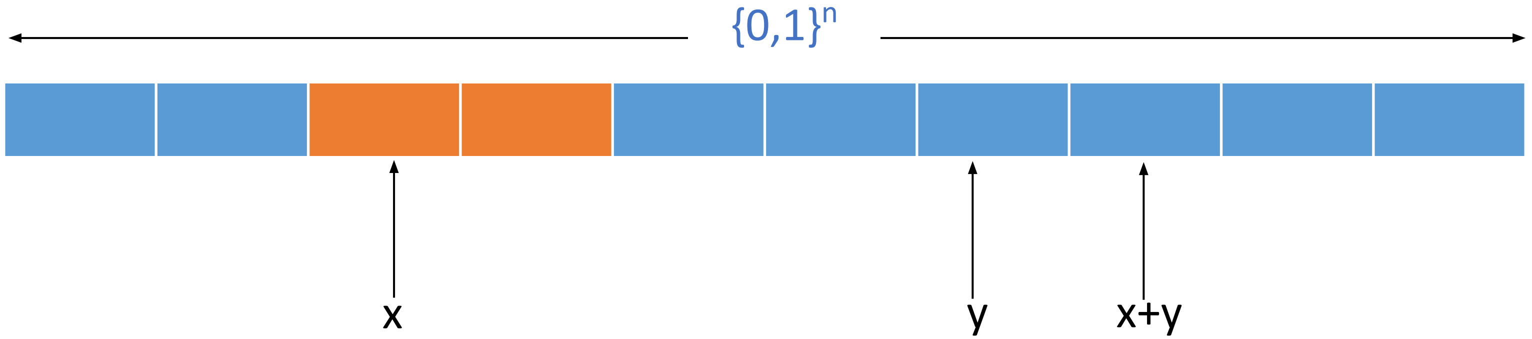
1. Pick $x,y \in \{0,1\}^n$ uniformly at random.
2. Accept iff $f(x+y) = f(x)+f(y)$.



Locally-Linear Non-Linear Functions

Take linear h and $f(x)=h(x)$ on exactly $1-\delta/3$ fraction of $x \in \{0,1\}^n$. Then, f is not linear but $f(x+y)=f(x)+f(y)$ with prob $\geq 1-\delta$ over $x,y \in \{0,1\}^n$.

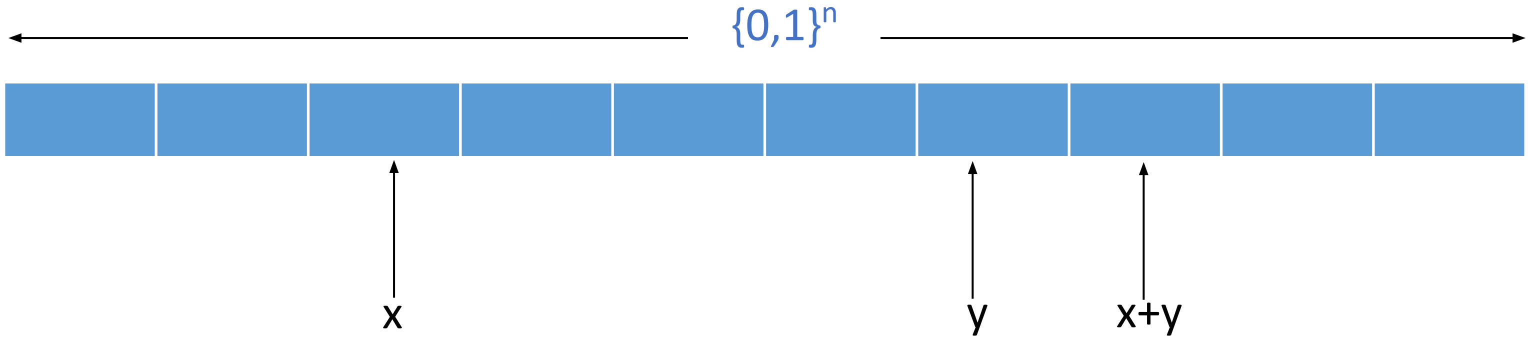
Coming up: Such functions are the **only ones** the test accepts with high probability



Linearity Testing Theorem (Blum-Luby-Rubinfeld)

If $f(x+y) = f(x)+f(y)$ with probability $1-\delta$ over $x,y \in \{0,1\}^n$,

then there exists a linear function $h:\{0,1\}^n \rightarrow \{0,1\}$, such that $f(x) = h(x)$ for at least $1-(9/2)\delta$ fraction of $x \in \{0,1\}^n$.

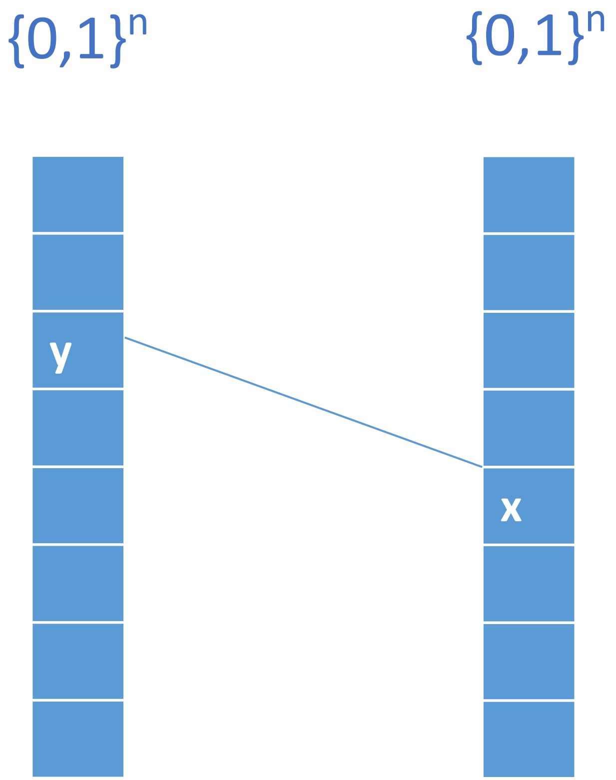


Majority Decoding

Assume $f(x+y) = f(x)+f(y)$ with probability $1-\delta$ over $x,y \in \{0,1\}^n$.

- Let $x \in \{0,1\}^n$. Every $y \in \{0,1\}^n$ has an "opinion" about $f(x)$, namely, $f(y)+f(x+y)$.
- Define $h(x)=\text{majority}_y\{f(y)+f(x+y)\}$.
- We will show:
  1. h is linear.
  2. $f(x)=h(x)$ for at least $1-2\delta$ fraction of $x \in \{0,1\}^n$.

If $f(x)\neq h(x)$, then $P_y(f(x+y)\neq f(x)+f(y)) > ½$.



From Majority to Super Majority

Assume $f(x+y) = f(x)+f(y)$ with probability $1-\delta>7/9$ over $x,y\in\{0,1\}^n$.

Claim: For **all** $x\in\{0,1\}^n$,

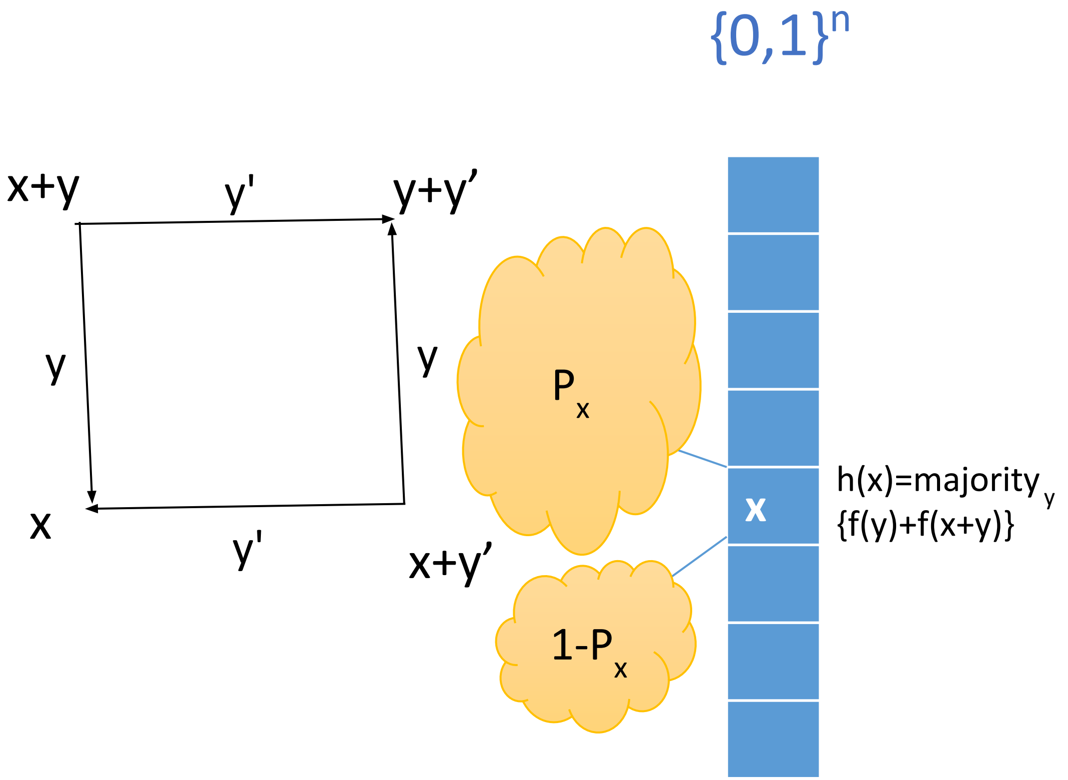
$P_x := P_y(\ h(x)=f(y)+f(x+y)\ ) > \mathbf{2/3}$.

Proof: Pick independent $y,y'\in\{0,1\}^n$.

$$P(\ f(x+y)+f(y) = f(x+y')+f(y')\ )$$

$= P_x^{\,2}+(1-P_x)^2$.

$= P(\ f(x+y)+f(y') = f(x+y')+f(y)\ ) \geq 1-2\delta$



Majority Decoding is Linear

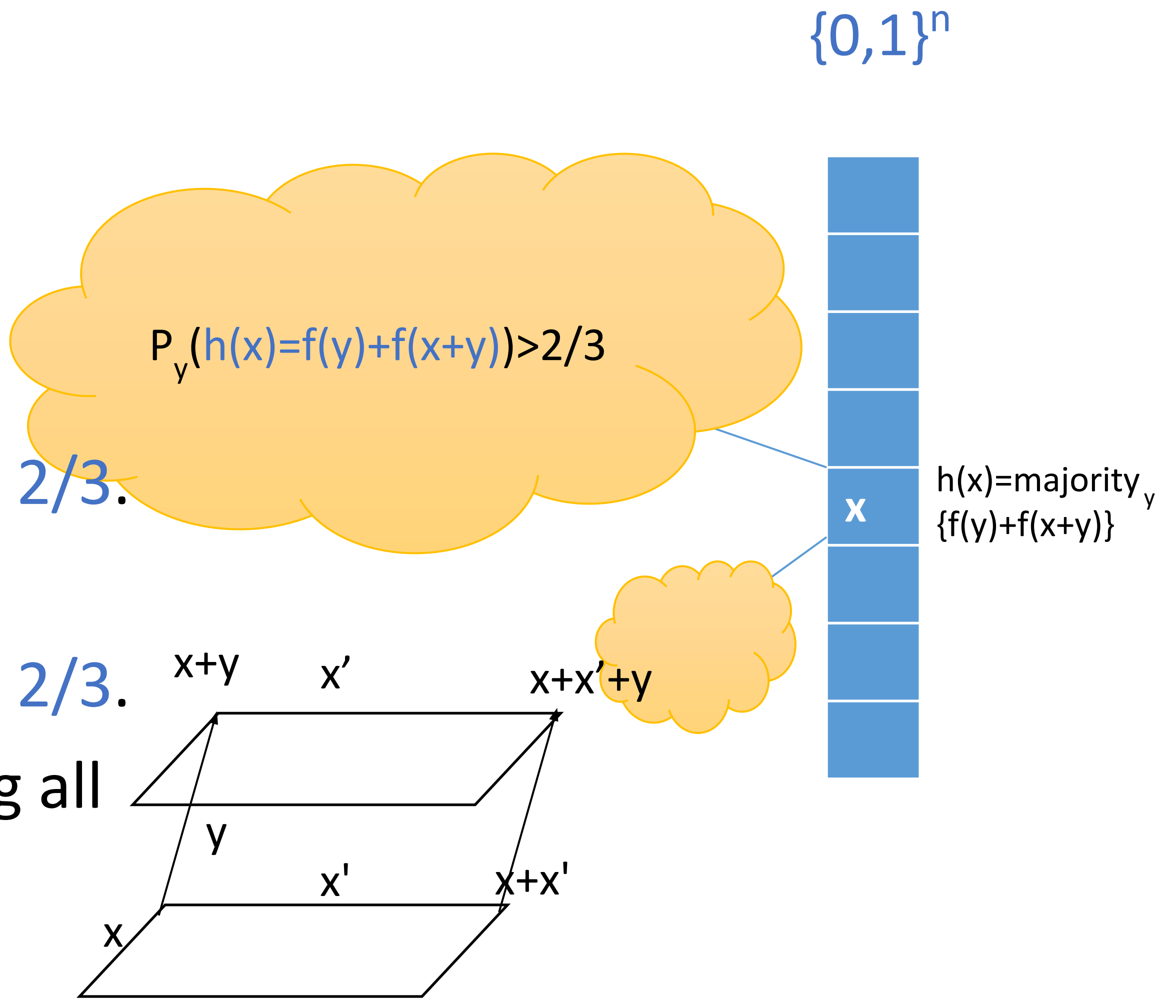
Claim: For **every** $x,x' \in \{0,1\}^n$,

$h(x+x')=h(x)+h(x')$. (*)

Proof: For a uniform $y \in \{0,1\}^n$,

- $h(x+x')=f((x+x')+y)+f(y)$ with probability > $2/3$.
- $h(x')=f(x'+y)+f(y)$ with probability > $2/3$.
- $h(x)=f(x+(x'+y))+f(x'+y)$ with probability > $2/3$.

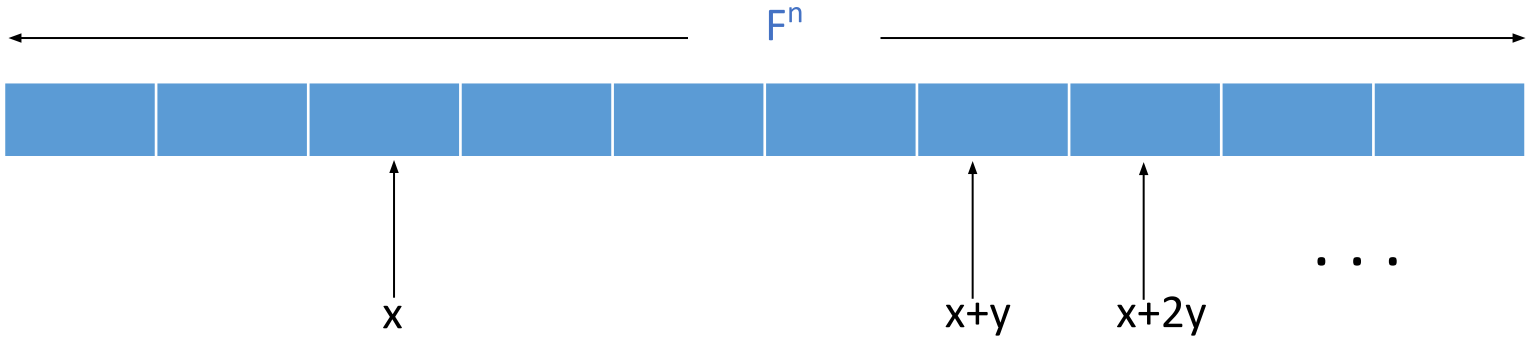
Hence, there must exist $y \in \{0,1\}^n$ satisfying all three equations. They imply (*).



Low Degree Tester

Given access to f:$F^n \rightarrow F$, $|F|>d+1$:

1. Pick $x,y \in F^n$ uniformly at random.
2. Pick $d+1$ random points on the line $x+ty$ to query.
3. Accept iff queries satisfy interpolation condition.

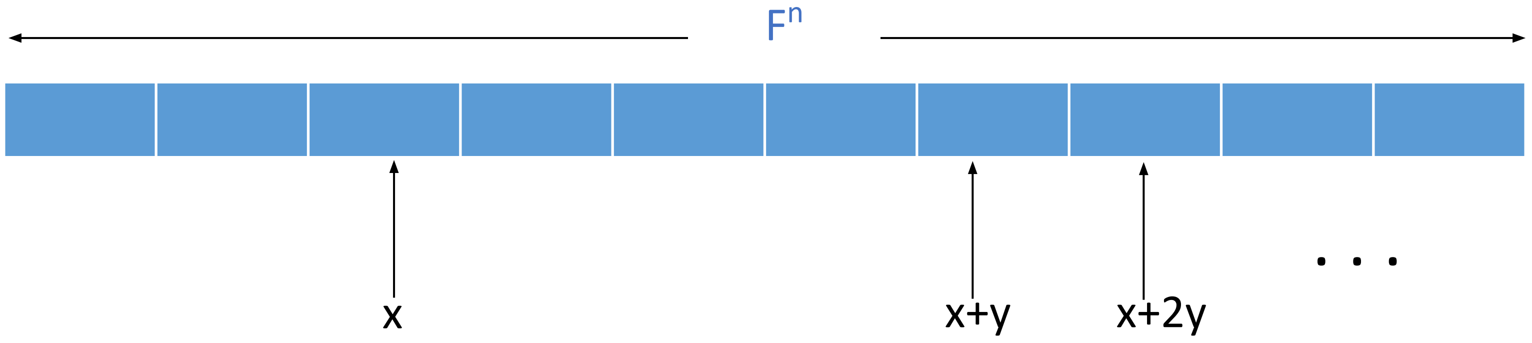


Low Degree Testing Theorem
(Gemmell-Lipton-Rubinfeld-Sudan-Wigderson)

For sufficiently small $0<\delta<<1/d^2$ and $|F|>d+1$:

If Low Degree Tester accepts with probability $\geq 1-\delta$,

then there exists a polynomial $h:F^n \to F$ of degree $\leq d$, such that $f(x) = h(x)$ for at least $1-O(\delta)$ fraction of $x \in F^n$.

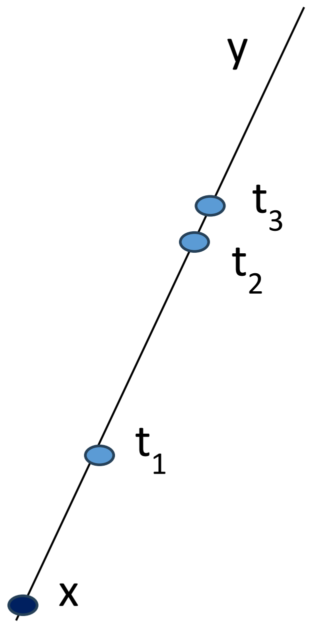


Randomized Decoding

Assume Low Degree Tester accepts with probability $1-\delta$ for $\delta<<1/d^2$.

- Pick uniformly at random $y \in F^n$ and distinct non-zero field elements $\underline{t}=t_1..t_d$. For every $x \in F^n$, let $h_{y,\underline{t}}(x)$:= interpolation of $f(x+t_1y),\ldots,f(x+t_dy)$.
- We will show:
  1. **Degree d:** With prob $1-o(1)$ over $y,\underline{t}$; $h_{y,\underline{t}}$ of deg d.
  2. **Agreement:** With prob $1-o(1)$ over $y,\underline{t}$, $f(x)=h_{y,\underline{t}}(x)$ for at least $1-O(\delta)$ fraction of $x \in F^n$.

Immediately follows

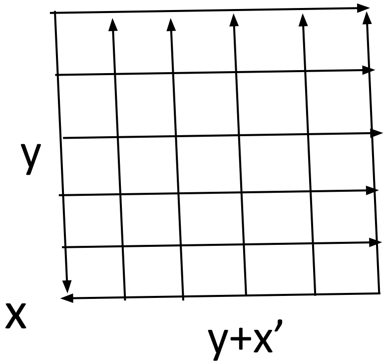


Low Degree

Assume Low degree tester accepts with prob $\geq 1-\delta$ for $\delta \ll 1/d^2$.

Claim: For **any** $x, x', s_1 .. s_{d+1}$ with prob $1-o(1)$ over $y, \underline{t}$;
$h_{y,\underline{t}}(x+s_1 x'), \ldots, h_{y,\underline{t}}(x+s_{d+1} x')$ of degree d.

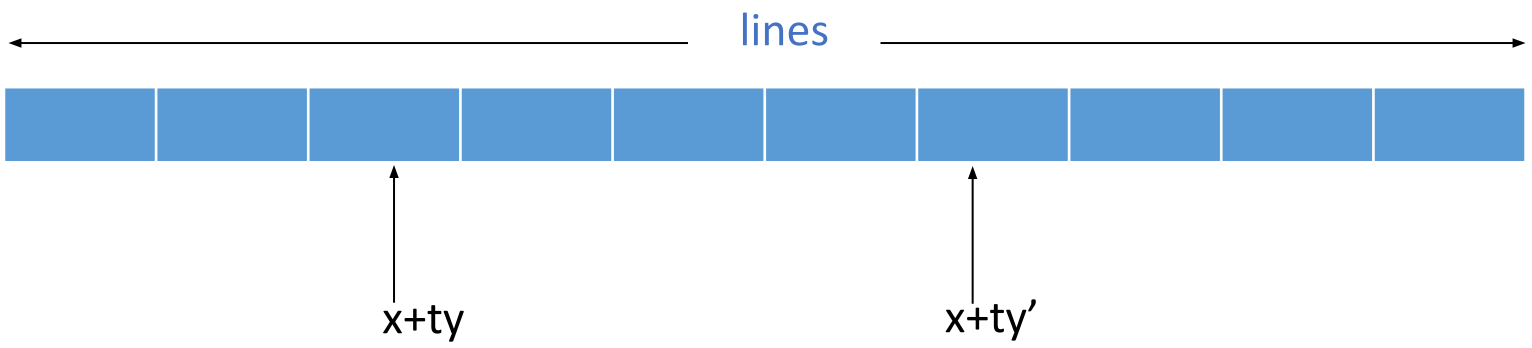
Proof:



Line vs. Line Low Degree Tester

Given access to A:lines→univariate deg-d polynomials:

1. Pick $x,y,y' \in F^n$ uniformly at random.
2. Query poly for $x+ty$ and for $x+ty'$.
3. Accept iff polynomials agree on x.



Low Degree Testing Theorem (Rubinfeld-Sudan, Arora-Lund-Motwani-Sudan-Szegedy, Friedl-Sudan)

For sufficiently small $0<\delta<1/8$ and $|F|>>d$:

If Low Degree Tester accepts with probability $\geq 1-\delta$,

then there exists a polynomial $h:F^n \rightarrow F$ of degree $\leq d$, such that $f(l) = h_{|l}$ for at least $1-O(\delta)$ fraction of the lines l in F^n.