Counting Classes.

def $\#P$: $f(x) = |y : M(x,y)=1|$ // M det. poly. TM.

obs this is a class of functions, not decision problems. the analogue of P for functions is

def FP: $f(x) = M(x)$.

obs $\#P = FP \Rightarrow NP = P$.

standard $\#P$-complete problem: $\#SAT$.

th: even $\#2\text{-}SAT$ is $\#P$-complete!

th: permanent is $\#P$-complete. (Valiant)
contrast with determinant, which is in FP.
can define algebraic complexity classes VP, VNP centered on these functions, rich theory behind.

If we only want to know most significant bit we revisit an old friend:

$x \in L$ iff $|y : M(x,y)=1| > |y|/2$ is class PP.

If we only want LSB we get $\oplus P$.

$x \in L$ iff $|y : M(x,y)=1| \equiv 1 \pmod 2$.

Turns out $\oplus SAT$ is $\oplus P$-complete.
We also def $\#F = |\alpha : F(\alpha)=1|$ and $\oplus F = (\#F \bmod 2)$.

Evidence that $\#SAT$ way stronger than NP:
th (Toda): $PH \subseteq P^{\#SAT}$.

We'll now prove this.

Plan. 1. show $\forall c\ \exists f$ st F Σ^c formula then
F true $\Rightarrow f(F) \in \oplus SAT$ w. pr $1-2^{-m}$
false $\Rightarrow$ 2^{-m}.

2. derandomize algo.

Warmup th (Valiant-Vazirani): $USAT \in P \Rightarrow NP = RP$

we'll show $\exists f$ st F CNF formula then
F SAT $\Rightarrow f(F) \in USAT$ w. pr $1/8n$
F UNSAT $\Rightarrow f(F)$ 0.

idea: if S set of sat. assignments to F, we'll map all of them to a single element using a hash function.
let $h: 2^n \to 2^k$. if $2^k \approx |S|$ then should expect this to be true. more formally:

lem: let $h: 2^n \to 2^k$. pairwise hash function. $2^{k-2} \le |S| \le 2^{k-1}$.
then w. pr $\geq 1/8$ (over h) $\exists!\, x$ st $h(x)=0$.

given lemma we prove thm.
input F over n vars. sample $k \in [2, n+1]$ unif.
let $G = F \wedge [h(x)=0]$, written in CNF.

claim: $|G| = \text{poly}(|F|)$ // encode $ax+b=0$ over $\mathbb{F}_{2^n}$, truncated.

obs F SAT $\Rightarrow$ w/pr $1/n$ sample right k, and with pr. $1/8$ we apply lemma and have G has exactly one soln.
obs F UNSAT $\Rightarrow G$ UNSAT.

※.

proof of lemma: let $N = |h^{-1}(0)| \cap S$

$Pr(N=1) = Pr[N \geq 1] - Pr[N \geq 2]$

$Pr(N \geq 1) = \sum_{x \in S} Pr[h(x)=0] - \sum_{x,x' \in S} Pr[h(x)=0 \wedge h'(x)=0] + \_\_$

$\geq |S| \cdot 2^{-k} - \binom{|S|}{2} \cdot 2^{-2k}$.

$Pr(N \geq 2) = \sum_{x,x' \in S} \_\_\_ - \_\_ \leq \binom{|S|}{2} \cdot 2^{-2k}$.

$Pr(N=1) \geq |S| \cdot 2^{-k} - 2\binom{|S|}{2} \cdot 2^{-2k} \geq \underbrace{|S| \cdot 2^{-k}}_{\geq 1/4} \cdot \underbrace{\left(1 - |S| \cdot 2^{-k}\right)}_{\geq 1/2} \geq 1/8$.

※.

We can reduce error by repeating algo a few times, but we'll get different formulas each time. Could we instead have one G st $Pr[G \in USAT] \geq 1/2$?
We don't know!
But we'll able to do so with $\oplus SAT$.

Given F, G, we can build $F \cdot G$ st $\#(F \cdot G) = \#F \cdot \#G$
$F + G$ st. $\#(F+G) = \#F + \#G$.

→ $F \cdot G = F \wedge G$.
→ $F + G = (\bar{z} \wedge F) \vee (z \wedge G)$ // $z \notin vars(F) = vars(G)$.
→ $F + 1 = (\bar{z} \wedge F) \vee (z \wedge x_1 \wedge \dots \wedge x_n)$.

Use these to make $\oplus$ and $\wedge, \vee, \neg$ commute.

$(\oplus F) \wedge (\oplus G) \equiv \oplus(F \cdot G)$
$\neg(\oplus F) \equiv \oplus(F + 1)$
$(\oplus F) \vee (\oplus G) \equiv \neg(\neg(\oplus F) \wedge \neg(\oplus G))$.

Now we can make our plan for F a Σ^1 or Π^1 formula.

Say $F \in \Sigma^1$. Let $G_1 \dots G_m$ be the formulas from VV.
Then F SAT $\Rightarrow$ w/pr $1-2^{-m}$ at least one G_i USAT.
F UNSAT $\Rightarrow$ all G_i UNSAT.

hence $\bigvee G_i$ is good.

Obs since $\neg$ and $\oplus$ commute, $\oplus P = \overline{\oplus P}$, so we can also do Π^1 formulas.