Problem: Show that $MA_{2/3,1/3} = MA_{1,1/3}$.

Solution: Let $L \in MA_{2/3,1/3}$.

\[
x \in L \Rightarrow \exists y, Pr_r[V(x,y,r) = 1] \geq \frac{2}{3}
\]
\[
x \notin L \Rightarrow \forall y, Pr_r[V(x,y,r) = 1] \leq \frac{1}{3}
\]

Repeating $V$ polynomially many times and taking majority, we can get a verifier $V^*$ that uses $n^{O(1)}$ random bits, whose error probability is $2^{-n}$ (by the Chernoff bound).

By the theorem proved in class, if $x \in L$, there are $k = \text{poly}(n)$ strings $r_1, \ldots, r_k$ so that

\[
\forall r_0, \exists i \in \{1, \ldots, k\} \text{ s.t. } V^*(x, y, r_0 \oplus r_i) = 1
\]

Merlin gives Arthur the proof $(y, r_1, \ldots, r_k)$. Arthur picks $r_0$ at random and runs $V^*$ on strings $\{r_0 \oplus r_1, \ldots, r_0 \oplus r_k\}$ and accepts if any of these accept. If $x \in L$, there is a valid proof $(y, r_1, \ldots, r_k)$ so that Arthur always accepts.

On the other hand, if $x \notin L$, consider any alleged proof $(y, r_1, \ldots, r_k)$. Since the string $r_0 \oplus r_i$ is a random string for every $i$,

\[
Pr[V^*(x, y, r_0 \oplus r_i) = 1] \leq 2^{-n} \Rightarrow Pr[V^*(x, y, r_0 \oplus r_i) = 1 \text{ for some } i] \leq k2^{-n} < 1/2
\]

□

Problem: Show that $PSPACE \subseteq P/poly \Rightarrow PSPACE = \Sigma_2$.

Solution: We repeat the proof of the Karp-Lipton theorem using TQBF. If $PSPACE \subseteq P/poly$, there is a family of poly-size circuits $\{C_m\}$ that solves TQBF on instances of size $m$. We guess the circuit family and check the correctness of the circuit $C_m$ using $C_1, \ldots, C_{m-1}$ in as follows.

Let $\exists X_1 \forall X_2 \cdots X_k \phi(X_1, \ldots, X_k)$ be a TQBF instance of size $m$. Let $\phi_0 = \phi(0, X_2, \ldots, X_k)$ and $\phi_1 = \phi(1, X_2, \cdots, X_k)$ be the TQBF instances obtained by setting $X_1 = 0/1$ respectively. Note that both are of size strictly smaller than $\phi$. Hence we can check their satisfiability using $C_1, \cdots, C_{m-1}$. Since $\phi$ is satisfiable only if one of $\phi_0$ and $\phi_1$ is satisfiable, we can check if $C_m$ is correct for input $\phi$. A similar argument holds if the first quantifier is $\forall$.

Now gives any problem in $PSPACE$ of input size $n$, we can reduce it to a TQBF $\phi$ of size $m = \text{poly}(n)$. We then guess the circuits $C_1, \cdots, C_m$ and check them using the above procedure in
Σ2. We then use $C_m$ to decide $\phi$ and output the answer. □

**Problem:**

$$NC^i = NC^{i+1} \Rightarrow NC = NC^i$$

**Solution:** Assume that $NC^i = NC^{i+1}$. Let us show that $NC^{i+2} = NC^{i+1}$. Given a circuit of depth $\log^{i+2} n$, we can divide it into $\log n$ layers of depth $\log^{i+1} n$. The outputs of layer $j$ are inputs to layer $j+1$. Each layer contains $\text{poly}(n)$ bits. Now each bit at layer $j+1$ is computed from the bits at layer $j$ by a (non-uniform) $NC^{i+1}$ circuit. Since $NC^i = NC^{i+1}$, we can replace it by a $NC^i$ circuit of depth $\log^i n$ (the size may be larger, but it is still polynomial in $n$). This replacement gives a circuit of polynomial size, depth $\log^{i+1} n$ and fanin 2. Hence $NC^{i+2} = NC^{i+1} = NC^i$. The result now follows by induction. □

**Problem:** Assume that the problem of counting the number of matchings in a graph is $\#P$-complete. Show that counting the number of solutions to an instance of 2-SAT is $\#P$-complete.

**Solution:** Given a graph $G(V,E)$, introduce a variable $x_e$ for each edge $e \in E$. For any pair of edges $e, f$ that are incident on a common vertex, add the clause \( \overline{x_e} \lor \overline{x_f} \)

Note that a matching is precisely a solution to this 2-SAT formula, hence the number of solutions equals the number of matchings in $G$. □

**Problem:** Consider the following family of functions $F$ that map $\{0,1\}^n \rightarrow \{0,1\}^k$. Pick a $k \times n$ matrix $A$ with 0,1 entries at random. Pick $b \in \{0,1\}^k$ at random. Let

$$f(x) = Ax + b$$

where all arithmetic operations are over $\mathbb{Z}_2$.

- Show that for any $x \in \{0,1\}^n$ and $y \in \{0,1\}^k$,

  $$Pr_{A,b}[f(x) = y] = \frac{1}{2^k}$$

- Show that for any $x_1, x_2 \in \{0,1\}^n$ and $x_1 \neq x_2$, and any $y_1, y_2 \in \{0,1\}^k$,

  $$Pr_{A,b}[(f(x_1) = y_1) \land (f(x_2) = y_2)] = \frac{1}{2^{2k}}$$

- Show that for any $x_1, x_2 \in \{0,1\}^n$ and $x_1 \neq x_2$,

  $$Pr_{A,b}[f(x_1) = f(x_2)] = \frac{1}{2^k}$$
The probability is taken over $f \in F$ picked uniformly at random (by choosing $A$ and $b$ randomly).

**Solution:** Let $a_1 \cdots, a_k$ denote the rows of the matrix $A$. Let $b = (b_1, \cdots, b_k)$.

Let $k = 1$. Note that

$$Pr_{A,b}[a_1^t x + b_1 = y] = 1/2$$

since the equation is satisfied for exactly one of 2 values of $b_1$. Also for $k \geq 2$,

$$Pr_{A,b}[Ax + b = y] = 1/2^k$$

since the events for different rows of $y$ are independent.

Let $k = 1$. Fix $x_1 \neq x_2$, $y_1$ and $y_2$. Let us analyze the event

$$a_1^t x_1 + b_1 = y_1 \text{ and } a_1^t x_2 + b_1 = y_2$$

Let $y = y_1 \oplus y_2$. Note that this event is the same as

$$a_1^t (x_1 \oplus x_2) = y \text{ and } b_1 = y \oplus y_1$$

This is easier to analyze since the first event depends purely on $a_1$ and the second on $b_1$. Note that $x_1 \neq x_2$ implies that $x_1 \oplus x_2 \neq 0$. Hence

$$Pr_A[a_1^t (x_1 \oplus x_2) = y] = 1/2, \quad Pr_b[b_1 = y \oplus y_1] = 1/2$$

Hence

$$Pr_{A,b}[a_1^t x_1 + b_1 = y_1 \text{ and } a_1^t x_2 + b_1 = y_2] = 1/4$$

Again when $k \geq 2$, the events for every row of $y$ are independent. Hence

$$Pr_{A,b}[(f(x_1) = y_1) \land (f(x_2) = y_2)] = \frac{1}{4^k}$$

The last statement follows by summing over all $2^k$ possible common values of $f(x_1) = f(x_2)$. □

**Problem:** In MANY-SAT We are given a SAT instance with $S$ satisfying assignments. We are told that either $|S| \geq 2^k$ (Yes case) or $|S| \leq 2^{k-100}$ (No case). We have to distinguish the Yes and No cases.

Consider the following AM protocol for MANY-SAT. Arthur picks a random hash function mapping $\{0, 1\}^n \rightarrow \{0, 1\}^{k+2}$, and a random target value $y \in \{0, 1\}^k$. Merlin tries to find $x$ such that $f(x) = y$ and $x$ is a satisfying assignment. Arthur accepts if indeed $x$ satisfies both conditions.

Show that this is a valid AM protocol for MANY-SAT.

**Solution:** Let $S$ be the set of satisfying assignments. Let $f$ be picked at random. Let $Im(S) \subset \{0, 1\}^k$ be the image of $A$ under $f$. The probability that Arthur accepts is $Pr_{y,A,b}[y \in Im(S)]$.

In the NO case, $|Im(S)| \leq |S| \leq 2^{k-100}$. Hence $Pr_{y}[y \in Im(S)] \leq 2^{-100}$.

In the YES case, for any fixed $y$ we can lower bound the probability that $y \in Im(S)$ using inclusion-exclusion.

$$Pr_{A,b}[y \in Im(S)] \geq \sum_{x \in S} Pr[f(x) = y] - \sum_{x_1, x_2 \in S} Pr[f(x_1) = f(x_2) = y]$$

$$= \frac{|S|}{2^k} - \frac{(|S|)}{2^k}$$

$$> 1/2 \quad \text{if } |S| = 2^k$$
When $|S| \geq 2^k$, the probability that $y \in \text{Im}(S)$ can only be larger. While $Pr_{A,b}[y \in \text{Im}(S)]$ need not be the same for all $y$, it is at least $1/2$ for every $y$. Hence it is at least $1/2$ for a random $y$. Hence

$$Pr_{y,A,b}[y \in \text{Im}(S)] \geq 1/2$$

\[\square\]