1. **Combinatorics** [15 pts] Give a combinatoric proof that $3^n = \sum_{k=0}^{n} \binom{n}{k} 2^k$.

2. **Probability** [18 pts] Suppose $Pr$ is a probability measure on a sample space $S$, and $A$ is an event with $Pr(A) \neq 0$. We can define a new probability measure $Q$ on $S$ by the rule $Q(E) := Pr(E | A)$. Show that $Q$ is a probability measure on $S$.

In this question, you may use facts about sets without proof, but not facts about probability measures (besides the definitions). For example, you may use the fact that $A = (A \setminus B) \cup (A \cap B)$, but not the fact that $Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B)$.

3. **Automata** [22 pts] Complete the following proof:

**Claim:** the intersection of DFA-recognizable languages is DFA-recognizable.

**Proof:** Suppose $L_1$ and $L_2$ are DFA-recognizable languages. Then there exists automata $M_1 = (Q_1, \Sigma, \delta_1, q_{01}, A_1)$ and $M_2 = (Q_2, \Sigma, \delta_2, q_{02}, A_2)$ with $L(M_1) = L_1$ and $L(M_2) = L_2$. We want to build a new automata $M = (Q, \Sigma, \delta, q_0, A)$ that simulates both $M_1$ and $M_2$. We do this by making the states of $M$ pairs of states (one from $M_1$ and one from $M_2$).

(a) [3 pts] For example, if $M_1$ and $M_2$ are given by

```
1 1
start A > 0, 0
B
```

then $M$ would be given by the following diagram:

(b) [5 pts] Formally, we can define $M$ in general as follows:

- $Q := \phantom{|}$
- $q_0 := \phantom{|}$
- $A := \phantom{|}$
- $\delta := \phantom{|}$ is given by $\delta(\phantom{|}) := \phantom{|}$.

(c) [2 pts] Now, I claim that $M$ does simulate $M_1$ and $M_2$. More formally, I claim that for all $x$, $\hat{\delta}(q_0, x) = \phantom{|}$.

(d) [8 pts] Proof by induction on $x$:

(e) [4 pts] Finally, we use this to show that $L(M) = L(M_1) \cap L(M_2)$:
4. Modular numbers [15 pts]

Use Euler’s theorem and repeated squaring to efficiently compute $5^n \mod 21$ for $n = 5$, $n = 121$ and $n = 24010$.

Hint: you can solve this problem with six multiplications of one- or two-digit numbers (alternatively, you can use negative representatives to keep it to six single-digit multiplications). Please fully evaluate all expressions for this question (e.g. write 21 instead of $3 \cdot 7$).

5. Induction [15 pts] Suppose you are given a function $f : \mathbb{N} \to \mathbb{N}$, and are told that $f(1) = 1$ and for all $n$, $f(n) \leq 2f(\lfloor n/2 \rfloor) + 1$ (note: $\lfloor n \rfloor$ is the largest integer that is less than or equal to $n$).

Use induction to prove that for all $n \geq 2$, $f(n) \leq 2n \log_2 n$. Be sure to indicate where you are using your inductive hypothesis, and which inductive hypothesis you are using.

You may write log to indicate $\log_2$. Here are all of the facts about $\lfloor x \rfloor$ and $\log x$ that you will need:

- $\lfloor x \rfloor \leq x$
- $\log 1 = 0, \log 2 = 1$
- $\log(x/2) = \log x - 1$
- $\log(2^x) = x$
- $\log(x^2) = 2\log x$
- if $x \leq y$ then $\log x \leq \log y$


(a) [3 pts] Give a reasonable sample space for this problem.

For the remainder of the question, make sure that each random variable or event you use has a clear definition in terms of your sample space, and that each assertion is justified.

(b) [5 pts] What is the expected number of rolls that are less than or equal to 5?

**Hint**: use indicator variables.

(c) [5 pts] What is the variance of the number of rolls that are less than or equal to 5?

(d) [5 pts] Use Chebychev’s inequality to give an upper bound on the probability that all of the rolls are greater than 5.

7. Counting languages [18 pts] Let $\Sigma = \{0, 1\}$ and let $\Sigma^{10}$ be the set of strings with ten characters. How many strings are in each of the following languages? Briefly justify.

(a) [4 pts] $\Sigma^{10} \cap L((01)^* + (10)^*)$

(b) [4 pts] $\Sigma^{10} \cap L((01 + 10)^*)$

(c) [4 pts] $\Sigma^{10} \cap L(01^* + \varepsilon 0^*)$

(d) [6 pts] $\{x \in \Sigma^{10} | x \text{ has more 0’s than 1’s}\}$
8. **Equivalence relations** [15 pts] Let $\sim$ be the binary relation on $\mathbb{N} \times \mathbb{N}$ given by $(a,b) \sim (c,d)$ if $a + d = b + c$.

(a) [5 pts] Check that $\sim$ is an equivalence relation.

(b) [5 pts] Let $f : (\mathbb{N} \times \mathbb{N})/\sim \to \mathbb{Z}$ be given by $f([(a,b)_{\sim}]) := 2a - 2b$. Show that $f$ is well-defined.

(c) [5 pts] Show that $f$ as given above is injective.

9. **Quantifiers and the pumping lemma** [14 pts] Recall that the pumping lemma states the following:

$$\forall L \subseteq \Sigma^*, \text{ if } L \text{ is regular then } \exists n \in \mathbb{N} \text{ such that }$$

$$\forall x \in L, \text{ if } \text{len}(x) \geq n \text{ then } \exists u, v, w \in \Sigma^* \text{ such that } x = uvw \text{ and } v \neq \varepsilon \text{ and } \text{len}(uv) \leq n \text{ and }$$

$$\forall k \in \mathbb{N}, uv^kw \in L$$

(a) [6 pts] Give a similarly carefully quantified statement describing what it would mean for the pumping lemma to be false. You may not use the word “not” or the symbols $\neg$, $\exists$, or $\forall$, but you may use other crossed out symbols like $\neq$ or $\notin$.

(b) [4 pts] The following proof incorrectly uses the pumping lemma by using an inappropriate proof technique. Circle the first incorrect sentence and briefly explain why the technique does not apply.

**Claim:** $L := \{0^n1^m \mid n > m\}$ is not regular.

**Proof:**

- Assume $L$ is regular
- Then there exists $n$ as in the pumping lemma.
- Let $x = 0^n1^{n-1}$.
- By definition of $L$, $x \in L$, and clearly $\text{len}(x) \geq n$ so there exists $u, v, w$ as in the pumping lemma.
- Let $u = \varepsilon$, $v = 0^n$, and $w = 1^{n-1}$.
- Clearly $x = uvw$, $v \neq \varepsilon$ and $\text{len}(uv) = n \leq n$.
- By the pumping lemma, $uv^kw \in L$.
- But $uv^kw = 1^n$ has fewer 0’s than 1’s, so is not in $L$.
- This is a contradiction, so our assumption that $L$ was regular must be false.

(c) [4 pts] Explanation of error: