Theory of Computation

William Chu

November 10, 2018

1 Set Equality

Definition 1.1. Let A, B be sets such that $A = B$. To show $A = B$, we need to show two statements.

- $A \subset B$
- $B \subset A$

Definition 1.2. Let $p, q \in \digamma$. We say that p divides q (denote $p|q$) if $\exists k \in \digamma$ so that $pk = q$.

Proposition 1.1. Let $A = 6n : n \in \digamma$, $B = 2n : n \in \digamma$, $C = 3n : n \in \digamma$. So $A = B \cap C$.

Proof. We first show that $A \subset B \cap C$. Let $x \in A$. By definition of A, $x = 6k$ for some$k \in \digamma$. We show $x \in B$ and $x \in C$. We first observe $x = 2 \cdot (3k)$. Therefore, $x \in B$. Now ovserve$x = 3 \cdot (2k)$. So $x \in C$. Thus $x \in B \cap C$. As x was arbitrairy, we conclude that $A \in B \cap C$. We now show that $(B \cap C) \subset A$. Let $y \in B \cap C$. Let $n_1, n_2 \in \digamma$ such that $y = 2n_2 = 3n_2$. As 2 and 3 share no common factors, we have that $2 \cdot 3|y$. so $6|y$. Thus $y = 6h$ for some $h \in \digamma$. So $y \in A$. Thus , $(B \cap C) \subset A$. We showed that $A \subset (B \cap C)$ and $(B \cap C) \subset A$. So $A = B \cap C$. QED

Proposition 1.2. Let A, B, C be sets, Then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof. We first show $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$. Let $(x, y) \in A \times (B \cup C)$. We show that $(x, y) \in (A \times B) \cup (A \times C)$. We have two cases:

1. Suppose $y \in B$. Then $(x, y) \in A \times B$.
2. Suppose $y \in C$. Then $(x, y) \in A \times C$

So $(x, y) \in (A \times B)$ or $(x, y) \in A \times C$. Thus, $(x, y) \in (A \times B) \cup (A \times C)$. And We conclude $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$. We now show $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$. Let $(x, y) \in (A \times B) \cup (A \times C)$. To be continued QED

2 Autonoma Theory

Definition 2.1 (Alphabet)**.** Let Σ be a finite set, We refer to Σ as an alphabet.

Definition 2.2 (Kleene Closure)**.** Let Σ be an alphabet. The kleene closure of Σ, denoted Σ^* is the set:

$$\Sigma^* = \bigcup_{n\in\mathbb{N}} \sum^n$$

where $\Sigma^0 = \{\Sigma\}$. Note: Σ is the empty string.

Definition 2.3 (Language)**.** A language $L \subset \Sigma^*$

Definition 2.4 (Regular Language)**.** Let Σ be an alphabet. The following are perciesly the regular languages over Σ. (i) $\emptyset$ is regular. (ii) $\{a\}$ is regular, $\forall a \in \Sigma$. (iii) If L_1, L_2 are regular the $L_1 \cup L_2$, L_1^* is regular and $L_1 \cdot L_2 = \{xy | x \in L_1, y \in L_2\}$ is regular.

Definition 2.5. Let Σ be an alphabet. A regular expression defined recusively

1. $\emptyset$ is a regular expressiion with $L(\emptyset) = \emptyset$.
2. ϵ is a regular with $L(\epsilon) = \{\epsilon\}$.
3. For each $a \in \Sigma$, the regular expression a has language $\{a\}$. $(L(a) = a)$
4. For R_1, R_2 be regular expressions. Then:
   (a) $R_1 + R_2$ is a regular expression, where $L(R_1 + R_2) = L(R_1) \cup L(R_2)$.
   (b) $R_1 R_2$ is a regular expression, where $L(R_1 R_2) = L(R_1)L(R_2)$.
   (c) R_1^* is regular, and $L(R_1^*) = (L(R_1))^*$.

3 Graph Theory

Definition 3.1 (Simple Graph)**.** A simple graph $G(V, E)$ has a vertex set V (denote V(G) if the graph is not clear), and an edge set $E \subset \binom{V}{2}$. [$E \subset \binom{V}{2}$ is the set of 2-element subsets of V] Remark, for an edge i, h we write it as ij or ji.]

Definition 3.2 (Compelete Graph)**.** Let $n \in \mathbb{N}$. The complete graph on n verticies, denoted as k_n, has vertex set $V = [n]$, and edge set $\binom{E=[n]}{2}$.

Definition 3.3 (Path)**.** The path on n verticies, denoted P_n, has certe set V=[n], and edge set; $E = \{\{i, i+1\} | i \in [n-1]\}$.

Definition 3.4 (Null Graph)**.** $G(V, E)$ has $V = E = \emptyset$, $G = \emptyset$.

Definition 3.5 (Empty Graph)**.** The empty graph on n verticies $G(VE)$ has vertex set $V = [n]$, and $E = \emptyset$.

Definition 3.6 (Cycle Graph)**.** For $n \in \mathbb{N}$, $n \geq 3$, the cycle graph on verticies, denoted as C_n, has vertex $E = i, i+1 | i \in [n-1]$.

Definition 3.7 (Wheel Graph)**.** Let $n \geq 4$. The wheel graph on n vertices, denoted as W_n is the graph $G(V, E)$, with vertex set $V = [n]$ and edge set.

$$E = \{\{i, i+1\} | i \in [n-2]\} \cup \{\{1, n-1\}\} \cup \{\{i, n\} | i \in [n-1]\}$$

.

Definition 3.8 (Bipartite graph)**.** A barpartite graph $G(V, E)$ is a graph s.t. V can be partitoned into two sets X, Y (i.e., $V = XUY$, $X \cap Y = \emptyset$ and $E \subset \{xy | x \in X, y \in Y\}$)

Definition 3.9 (Hypercube)**.** The hypercube of degree d, denoted Q_d, has vertex set $V = 0, 1^d$ (i.e., the set of binary strings of length d). Now $(w_1, w_2, ..., w_d)$ and $(\tau_1, \tau_2, ...\tau_d)$ are adjacent in Q_d if and only if there exists exactly one $i \in [d]$ s.t. $w_i \neq \tau_i$.

Definition 3.10 (Connected)**.** A graph is said to be connected if for every pair of vertices u, v there exists a path from u to v (i.e., $u - v$ path). A graph is disconnected if it is not connected. The connected subgraphs are called componenets.

Definition 3.11 (Tree)**.** A tree is a connected, a cyclic graph.

Definition 3.12 (Vertex Degree)**.** Let $G(V, E)$ be a graph. The degree of a vertex $v \in V$ is $deg(v) = |\{uv | uv \in E\}|$. A graph is d-regular if every vertex has degree d.

Definition 3.13 (Walk)**.** Let $G(V, E)$ be a graph. A walk in G is a sequence of verticies. $(v_0, v_1, ..., v_k)$ s.t. for all $i \in \{0, ..., k-1\}$, $v_i v_{i+1} \in E(G)$.

Definition 3.14 (Adjacency Matrix)**.** Let $G(V, E)$ be a graph. The adjacency matrix of G is a $|V| \times |V|$ matrix where A_{ij}=$\{1 : ij \in E(G), 0 : \text{Otherwise}\}$

Definition 3.15 (Closed Walk)**.** Let $G(V, E)$ and let $v_0, v_1, ...v_k$ be a walk. We say that the walk is closed if $v_0 = v_k$.

Definition 3.16 (Independent Set)**.** An independent set of a graph $G(V, E)$ is a set $S \subset V$ such that for every $i, j \in S$, $ij \notin E(G)$. Denote $\alpha(G)$ as the size of the largest independent set in G.

Definition 3.17 (Graph Vertex Coloring)**.** A vertex coloring of a graph $G(V, E)$ is a function $\varphi : V(G) \to [n]$ s.t. whenever $uv \in E(G), \varphi(u) \neq \varphi(v)$. The chromatic number of G denoted $\chi(G)$, is the smallest $n \in \mathbb{N}$ s.t. there exists a coloring

$$\varphi : V(G) \to [n]$$

.

Lemma 3.1 (Handshake Lemma)**.** Let $G(V, E)$ be a simple graph. Then

$$\sum_{v \in V} deg(v) = 2|E|$$

.

Proof. By double counting. $2|E|$ counts twice the number of edges.

$$\sum_{v \in V} deg(v)$$

we note that $deg(v)$ counts the number of edges incident to v. Each edge has 2 endpoints, u and v. So uv is counted twice once in $deg(v)$ and once in deg(u). So

$$\sum_{v \in V} deg(v) = 2|E|$$

QED

Lemma 3.2. Let $G(V, E)$ be a graph. Every closed walk of odd length at least 3, contains an odd cycle.

Proof. By induction on odd $k \in \mathbb{Z}^+$, $k \geq 3$. Base Case: Any closed walk of length 3 includes an odd cycle so the lemma holds. Inductive Hypothesis: Fix $k \in \mathbb{Z}^+$ odd, $k \geq 3$., and suppose the lemma holds. Inductive Step: Conside a closed walk of length $k+2$, $v_0, v_1, ..., v_k + 2$. If $v_0 = v_{k+2}$ are the only repeated verticies then the walk unduces an odd cycle, and we are done. Suppose instead there are only other repeated verticies in the walk. Let $0 \leq i < j \leq k+2$, where we don't have both $i = 0$ and $j = k + 2$. Suppose $v_i = v_j$, then $v_i, v_{i+1}, ..., v_k$ has odd length, then $v_i, ..., v_j$ contains an odd cycle by the inductive hypothesis. Suppose instead $v_i, ..., v_j$ has even length. Observe that $v_0, ..., v_i, v_{j+1}, ..., v_k + 2$ is a closed walk of odd length at most k. So by the Inductive Hypothesis, $v_0, ..., v_i, v_j + 1, ..., v_{k+2}$ has an odd cycle. Thus $v_0, ..., v_{k+2}$(The Original Walk) has an odd cycle. QED

Theorem 3.1. Let $G(V, E)$ be a graph, and let A be its adjcency matrix. For all $n \in \mathbb{Z}^+$, $(A^n)ij$ counts the number of $i - j$ walks of length n.

Proof. By induction on $n \in \mathbb{Z}^+$. Base case: n=1. So $A^1 = A$. Now there exists a walk of length 1 from $i - j$ if and only if $ij \in ij \in E(G)$. This is counted by A^{ij}. Inductive Hypothesis: Fix $k \geq 1$, and supposse that $(A^k)ij$ counts the number of $i - j$ walks of length k. Inductive Step: Consider $A^{k+1} = A^K \times A$. By the Inductive Hypothesis, $(A^k)ij$ counts the number of $i - j$ walks of length k. Similarly Aij counts the number of $i - j$ walks of length k. Observe that:

$$(A^{K+1})ij = \sum_{x=1}^{n=|V|} ((A^k)_{ix} \times Axj)$$

Now $(A^k)ix$ counts the number of k-length walks from $i-x$. Now $Axj = 1$ if and only if $xj \in E(G)$. So we may extend a walk of length k from $i-x$, to walk of length $k+1$ from $i-j$ if and only if $xj \in E(G)$. By the rule of sum, we add up over all the $x \in V(G)$. QED

Theorem 3.2. A graph $G(V, E)$ is bipartite if and only if G contains no cycles of odd length.

Proof. Suppose G is bipartite with parts from X and Y.

$$V(G) = X \cup Y, X \cap Y = 0$$

Consider a walk of length$n$. As no two vertices in a fixed part are adjacent, only walks of even length can be closed. A cycle is a closed walk where only the endpoints are repeated. So G contains no odd cycles. Conversely, suppose G has no odd cycles. We construct a bipartition of G. Without laws of generality, suppose G is connected. For if G is not connected we apply the following construction to each connected component. Fix $v \in V(G)$. Let: $X = \{x \in v(G) | dist(v, x)$ is even$\}$, $Y = \{y \in V(G) | dist(v, y)$ is odd$\}$. So $V(G) = X \cup Y$, and $X \cap Y = \emptyset$. We show that as two verticies in the same part are adjacent. Suppose to the contrary that there exists a closed odd walk $(v_1, ...y_1, y_2, ...v)$ By Lemma 1, $(v_1, ..., y_1, y_2, ...v)$ contains an odd cycle, contradicting the assumption that G has no odd cycles .Similarly, no two vertices in X are adjacent. So G is bipartite. QED

Proposition 3.1. $2^{\mathbb{N}}$ is uncountable.

Proof. Suppose to the contrary that $2^{\mathbb{N}}$ is countable. Let $h : \mathbb{N} \to 2^{\mathbb{N}}$ be a bijection. We obtain a contradiction (contradicting the surjectivity of h). We construct a set: $S \in 2^{\mathbb{N}}$ s.t. $\forall n \in \mathbb{N}$, $h(n) + S$. Def: $S = \{i \in \mathbb{N} | i \notin h(i)\}$. We show that S is not in the range of h. Suppose $i \in h(i)$. Then $i \notin S$ Thus, $h(i) \neq S$. Similarly, if $i \notin h(i)$, then $i \in S$. So $h(i) \neq S$. Thus, S ins not in the range of h, contridicting the assumption that h was a bijection. QED

Proposition 3.2. $\mathbb{R}$ is uncountable.

Proof. We show $[0, 1]$ is uncountable. We represent $S \in 2^{\mathbb{N}}$ as a binary string w, where $w_i = \{1 : i \in S, 0 : i \notin S\}$ we map $w \mapsto 0$. w, which is an injection. So $[0, 1]$ is uncountable. QED

4 Asymptotics

Definition 4.1. Let

$$f, g : N \to L = \lim_{x \to \infty} \left(\frac{f(n)}{g(n)} \right)$$

We have: (i) If $0 \leq L < \infty$, then $f(n) \in O(g(n))$ (ii) $0 < L \leq \infty$, then $f(n) \in \Omega(g(n))$ (iii) If $0 < L < \infty$, then $f(n) \in \Theta(g(n))$

Definition 4.2. Let $f \circ g : \mathbb{N} \to \mathbb{N}$. We say that $f(n) \in \mathcal{O}(g(n))[f(n) = \mathcal{O}(g(n))]$ if $\exists c, k \in \mathbb{Z}^+$ such that $f(n) \leq c \circ g(n) \forall n \geq k$

Theorem 4.1. $f(n) = n$, $g(n) = n^2$. Then $f(n) \in O(g(n))$.

Proof. Let c = k = 1. We show by induction on $n \in N$ that $n \leq n^2$. Inductive Hypothesis: Fix $k \leq 0$. Suppose $k \leq k^2$. Inductive Step: Consider k+1. By the Inductive Hypothesis, $k \leq k^2$. So $k + 1 \leq k^2 + 1 > k^2 + 2k + 1 = (k + 1)^2$ So we have by induction that $n \leq n^2$ for all $n \in N$ Thus, $n \in O(n^2)$. QED

5 Combinatorics

Definition 5.1 (Rule of Sum)**.** If A and B are disjoint sets, then $|A \cup B| = |A| + |B|$.

Definition 5.2 (Rule of Product)**.** If A and B are sets, then $|A\ B| = |A| \cdot |B|$

Definition 5.3 (Permutation)**.** Let X be a set. A permutation is a bijection $f : x \to x$.

Definition 5.4 (Restricted Permutation)**.** Given an n-element set and $r \in 0, ..., n$, there are $P(n, r) = \frac{n!}{n!(n-r)!}$

Definition 5.5 (Σ alphabet)**.** Let Σ be a finite string we refer to as an alphabet. A word of length n is an element of Σ^n

Definition 5.6 (Countabliity)**.** A set X is said to be countable if there exists an injection $f : X \to \mathbb{N}$. That is, X is countable if and only if $|X| \leq |\mathbb{N}|$.

Definition 5.7 (Multiset)**.** A multiset S is an unordered collection of elements, which may be distinct.

Definition 5.8 (Intuition)**.** A multiset is a set, with possible repeated elemtents.

Definition 5.9 (Binomial Theorm)**.** For $x, y \in \mathbb{C}$,

$$(x + y)^n = \sum_{n=1}^{\infty} \binom{n}{i} x^i y^{n-1}$$

Theorem 5.1. There exists $n!$ permutations on $[n]$.

Proof. We define a permutation $\pi : [n] \to [n]$. Observe that $\pi(1)$ can take on any value [n]. So we have n choices for $\pi(1)$. This leaves $n - 1$ possible values to which $\pi(2)$ can map. The selections of $\pi(1) and \pi(2)$ are independent. So by the rule of product, we multiply to obtain $n(n - 1)$ ways of selecting $\pi(1)$ and $\pi(2)$. Proceeding in this manner, there are $n(n - 1)(n - 2)...2 \cdot 1 = n!$ permutations. QED

Theorem 5.2.

$$\sum_{i=0}^{n} 2^i = 3^n$$

Proof. By double countiing, $3n^2$ counts the number of ternary strings of length n. Fix $i \in [n] \cup 0$. We first count the number of ternary string of length n with exactly i binary digits. We select the positions for the binary digits in $\binom{n}{i}$ ways. There are 2^i ways of populating the selected i positions with binary digits. Our selection of binary digits fixes the rest of the positions to contain 2's Denote A, as the set of ternary strings length n with exactly i binary digits. For $\neq j, A_i \cap A_j = \emptyset$. So by rule of sum, we add

$$\sum_{i=0}^{n} 2^i$$

This counts all the ternary strings of length n. QED

Theorem 5.3 (Rule of Sum)**.** Let A and B be disjoint sets, then $|A \cup B| = |A| + |B|$.

Proof. Let $n = |A| + |B|$. We map $F : A \cup B \to [n]$. Let $g : A \to [|A|]$, $h : B \to [|B|]$ be bijections. Define: $f(x) = g(x) : x \in A, h(x) + |A| : x \in B$. As $A \cap B = 0$, x will be evaluated under g or under k, but not both, As g and h are functions so is f. We verify that f is a bijection. Injection: Let x_1,x_2, $\in X \cup Y$ s.t. $f(x_1) = f(x_2)$. Observe that f takes on values from $1, ...|A|$ if $x \in A$, and f takes on values from $|A| + 1, ..., |A| + |B|$ if $x \in Y$. if $x \in B$. Since f(x_1)=f(x_2), we have that x_1,$X_2 \in A$ or x_1,$x^2 \in B$. If x_1, $x_2 \in B$. If $x_1, x_2, \in A$, then $f(x_1) = g(x_1) = f(x_2)$. As g is a bijection, it follows that $x_1 = x_2$ Similarly, if x_1, $x_2 \in B$, then we have: $f(x_1) = h(x_1) = h(x_2)$. As h is a bijection, $x_1 = x_2$ So f is an injection. Surjection: As g is a surjection, $\forall n \in [|A|], \exists x \in A$ s.t. $g(x) = n$. Therefore $[|A|] \subset range(f)$. As h is a surjection, f maps to each $y \in |A| + 1, ..., |A| + |B|$ So F is surjective. QED

Theorem 5.4 (Stars and Bars)**.** Let $n, k \in \mathbb{N}$. There exists percisely $\binom{n+k-1}{n}$ multisets of size n, whose elements are drawn from [k].

Proof. Let M be the set of n-element multisets drawn from [k]. We construct a bijection $\varphi : (*^n, i^k - 1) \to M$, as follows $\varphi(*^a 1|...|*^a k) = 1, ..., 1, 2, ..., 2, ..., k, ..., k$. We show that φ is a bijection. Surjection: Let $S = 1, ..., 1, ..., k, ...k^a k \in M$. Then $*^a 1| * a2|...| *^a k| \to$ S under φ So φ is surjective. Injection: Let $\omega, \tau \in R(*^n, |^k - 1)$ such that $\varphi(\omega) = \varphi(\tau) = 1^a, 2^{a_1}, ..., k^{a_k}$. It follows that $\omega = \tau = *^{a_1}| *^{a_2} |*^{a_3}$. So φ is injective, and thus a bijection. QED

Theorem 5.5 (Bionomial Theorem)**.** For $x, y \in \mathbb{C}$,

$$(x + y)^n = \sum_{n=1}^{\infty} \binom{n}{i} x^i y^{n-1}$$

Proof. We observe that on

$$\sum_{n=1}^{\infty} \binom{n}{i} x^i y^{n-1}$$

There are $\binom{n}{i}$ terms of the form $x^i y^{n-1} \forall i \in [n] \cup 0$. Now expanding $(x+y)^n$, each term is of the form $x^i y^{n-1}$ for $i \in [n] \cup 0$. Each factor $(x+y)$ contributes either x or y, but not both to $x^i yn - 1$. As multiplication continues the order in which the x's and y's are selected does not matter. There are $\binom{n}{i}$ ways of selecting the x terms, which fixes the selection of the y terms. The selections of terms of the form $x^i y^{n-1}$, $x^j y^{n-j}$ are disjoint for distinct i,j. So by the rule of sum, we add:

$$\sum_{n=1}^{\infty} \binom{n}{i} x^i y^{n-1} = (x+y)^n$$

. QED

Theorem 5.6. $\mathbb{Z}$ is countable.

Proof. We construct an injection $\varphi\mathbb{Z} \to \mathbb{N}$. Def $\varphi(n) = 2^n : n \geq 0, 3^n : n < 0$. We show that φ is injective. Let $n_1, n_2 \in \mathbb{Z}$ s.t. $\varphi(n_1) = \varphi(n_2)$. As 2,3 are prime they share no common factors or $n_1, n_2 < 0$. Case: Suppose $n_1, n_2 \geq 0$. So $2^{n_1} = 2^{n_2}$. Thus , $n_1 = n_2$. Case: Suppose $n_1, n_2 < 0$. Then $3^{-n_1} = 3^{-n_2}$. Thus, $-n_1 = -n_2$, and we have $n_1 = n^2$. So φ is injective, and we conclude that $\mathbb{Z}$ is countable. QED

6 Finite State Machines

Definition 6.1 (Finite State Machine)**.** A finite state machine is a 5-state(), where:

1. Q is our set of states
2. Σ is our input alphabet
3. δ is the transition function
4. q_0, the initial start state
5. $F \in Q$ the set of final accept states

Definition 6.2 (Deterministic Finite State Automoton)**.** We say that a finite state machine is a DFA(Determanistic finite state automoton) if the transition functions of the form:

$$\delta : Q \times \Sigma \to Q$$

Definition 6.3 (Non-deterministic Finite State Automoton)**.** A finite state machine is a NFA(Non-deterministic Finite State Automoton) if the transition function is of the form:

$$\delta : Q \times \Sigma \to 2^Q$$

Definition 6.4 (ϵ-NFA)**.** A finite state machine is an ϵ-NFA if the transition is of the form:

$$\delta : Q \times (\Sigma \cup \{\epsilon\}) \to 2^Q$$

Definition 6.5 (Complete Computation)**.** Let M be a FSM, and let $w \in \Sigma^*$. A complete computation of M on w is a sequence: $s_0, s_1, ..., s_k$ (where $k = |w|$), with $s_1 \in \delta(s_{i-1}, w_i)$, $\forall i \in [k]$, We can say that the computation is accepting if $s_k \in F$ (i.e. if M holds on a final state when run on w).

Definition 6.6. Let M be a FSM. The language of M is the set:

- $L(M) = \{w \in \Sigma^* | \text{there exists a complete accepting computation for } w\}$
- $M(w) = 1$, if M accepts w
- $M(w) = 0$, if M rejects w

Definition 6.7. Let N be an ϵ-NFA, and let q$\in Q$. The E-closure of q, denoted ECLOSE(q), is defined recursively:

1. $q \in$ ECLOSE(q)
2. If $v \in$ ECLOSE(q) and $r \in \delta(v, \epsilon)$, then $r \in$ ECLOSE(q)

Theorem 6.1 (Kleene Theorem)**.** A language L is regular if and only if there exists a DFA M that accepts L(i.e. $L(M) = L$)

Proof. $\Rightarrow$) We prove by induction on $n = |L|$ that if L is regular, then L is accepted by some DFA. Base Case:

1. Suppose $n = 0$. Then $L = \emptyset$. The DFA q_0 accepts L.
2. Suppose $n = 1$. the DFA q_0 accepts $\{\epsilon\}$
3. If $L = \{a\}$, for $a \in \epsilon$ then $q_0 \to \epsilon_1$, accepts L

Inductive Hypothesis: Fix $k \geq 1$, and suppose that every regular language of size $|L| \leq k$ is accepted by some DFA. Inductive Step: Let L_1, L_2 be regular languages of size at most k. By the Inductive Hypothesis, we have DFAs M_1, M_2 s.t. $L(M_1) = L_1$ and $L(M_2) = L_2$. QED

Lemma 6.1. There exists a DFA M to accept $L_1 \cup L_2$

Proof. Let M be a DFA with:

1. $Q_M = Q_1 \times Q_2$
2. $\Sigma_K = \Sigma_1 \cup \Sigma_2$
3. $q_0(M) = (q_0(1), q_0(2))$
4. $(F_1 \times Q_2) \cup (Q_1 \times F_2)$

5. $\delta_M = \delta_1 \times \delta_2$ (i.e. $S_M((q_i, q_j), a) = S_1(q_i, a), S_2(q_j, a))$

We show that $L_1 \cup L_2 = L_M$. Let $\omega \in L_1 \cup L_2$. Thus, $\omega \in L_1$ for some $i \in [2]$. Let $\hat{\delta}_i = (s_0, s_1, ..., s_k)$ be an accepting computation of M_i on ω. Let $\hat{\delta}_j = (r_0, r_1, ..., r_k)$ be a computation of M_j on ω. We have that $((s_0, r_0), (s_1, r_1), ..., (s_k, r_k))$ is an accepting computation of M on ω. Thus $\omega \in L(M)$. So $L_1 \cup L_2 \subset L(M)$. We now show $L(M) \subset L_1 \cup L_2$. Let $\omega \in L(M)$. Let $\hat{\delta}_M = ((a_0, b_0), (a_1, b_1), ..., (a_k, b_k))$ be the accepting computation of M on ω As $\omega \in L(M)$, $(a_k, b_k) \in (F_1 \times Q_2)$ or $(a_k, b_k) \in (Q_1 \times F_2)$. Without the laws of generality, suppose $(a_k, b_k) \in (F_1 \times Q_2)$. So $(a_0, a_1, ..., a_k)$ is accepting computation of $M_1 on \omega$. So $\omega_1 \in L_1$. By similar argument, if instead $(a_k, b_k) \in Q_1 \times F_2$,then $\omega \in L_2$. So $\omega \in L_1 \cup L_2$. QED

Lemma 6.2. $L_1 \cdot L_2$ is accepted by an ϵ-NFA M

Lemma 6.3. L_1^* is regular

7 Group Theory

Definition 7.1 (Group)**.** A group is a two-tuple $(G, *)$ where G is a set and $*$ is a binary operation. Also G must be closed under $GxG \to G$

1. Accociativity: $\forall a, b, c \in G, a(bc) = (ab)c = a * (b * c) = (a * b) * c$
2. Identity: $\exists e \in G$ s.t. $ea = ae = a \ \forall a \in G$
3. Inverses: $\forall e \in G$, $\exists a^{-1}$ s.t. $aa_{-1} = a^{-1}a = e$

Definition 7.2 (Order of an Element)**.** The order of an element for any $a \in G$, $|a| = min\{n \in \mathbb{Z}^+ : a^n = e\}$

Definition 7.3 (Order of a Group)**.** $|G|$ for $(G, *)$, a group, the cardinality of the set G.

Definition 7.4 (Subset)**.** Let G be a group. The set M is a subgroup of G of G if $M \subset G$ and H is a subgroup in it's own right under the same operation denoted $H \leq G$.

Theorem 7.1. Let (G,*) be a group. Then:

1. The identity, e, is unique
2. Inverses are unique
3. $(a^-1)^{-1} = a \ \forall a \in G$

Proof. 1. By def of G being a group, the identity exists. BWOC, let $e, f \in G$, both the identity. Thus, $ef = f$ and $fe = e$ by def of identity. Hence, we also know $ef = fe$ so $f = ef = fe = e$. Thus the identity is unique.

2. By definition of G, $\forall a \in G$, $\exists a^{-1}$ BWOC, let $a_1^{-1}, a_1^{-2} \in G$ are both inverses for a. Then, $aa_1^{-1} = e$ and aa_2^{-1}. So, $a_1^{-1} = a_1^{-1}e = a_1^{-1}(aa_2^{-1}) = (a_1^{-1}a)a_2^{-1}ea_2^{-}1 = a_2^{-1}$.

3. Let a$\in$ G. By definition of G, $\exists a^{-}1$ s.t. $aa^{-1} = e$ and $\exists(a^{-1})^{-1}$ s.t. $a^{-1}(a^{-1})^{-1} = e$.

QED

8 Myhill-Nerode and DFA minimization

9 Turing Machines

10 Planar Graphs

11 P vs. NP

Definition 11.1 (P)**.**

$$P = \bigcup_{n\in\mathbb{N}} DTIME(n^k)$$

$= \{L|\exists$ Turing Machine M and $\exists$ polynomial P_M such that $\forall\omega \in \Sigma^*, M(\omega) = 1 <==> w \in L,$ and M takes time $p(|\omega|)\}$

Definition 11.2 (NP)**.**

$$NP = \{L|\exists \text{ verifier } M \text{ for } L \text{ such that } M \text{ runs in polynomial time.}\}$$

Proposition 11.1. $P \subset NP$

Proof. Let $L \in P$, and let M be a poly-time decider for L. We construct a poly-time verifier for L as follows. For $\omega \in \Sigma^*$, M‘ on input $< \omega, 0 >$ simulates M on ω(ignoring the certificate O). M‘ accepts $< \omega, 0 >$ off M accepts ω. Since M decides L in poly-time, M‘ verifiers members of L in poly-time. So $L \in NP$. QED

12 φ ϕ