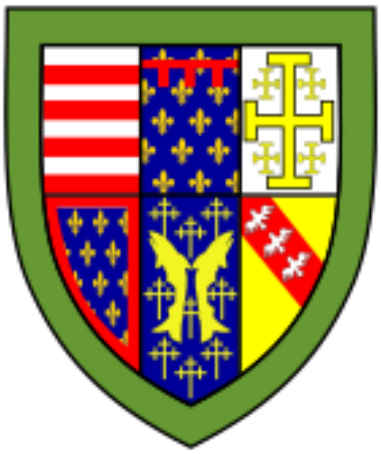
Queens' College Cambridge

Discrete Mathematics
Summary



Alistair O'Brien

Department of Computer Science

February 18, 2021

Contents

1 Sets

1.1 Naive Set Theory

A *set* is a collection of distinct objects. This means that $\{1, 2, 3\}$ is set, but $\{1, 1, 2\}$ is not as the element 1 appears more than once. The second collection is called a *multiset*.

Sets are often constructed using a *set comprehension*, in which we define a set by means of a property.

Definition 1.1.1. (**Separation Principle**) For any set S and any property P, there is a set containing all elements of S that satisfy P.

Definition 1.1.2. (**Membership**) The **set membership symbol** $\in$ is used to say that an object is a member of a set. It has a partner symbol $\notin$ which is used to say an object is not in a set.

Given a set A and a predicate $P(x)$ for the variable x ranging over the set A, we can use the following set-comprehension notation

$$\{x \in A : P(x)\}.$$

for defining a set consisting of all elements a of the set A such that $P(a)$ holds.

Definition 1.1.3. (**Extensionality Axiom (Equality)**) We say two sets are **equal** if they have exactly the same members, that is

$$\forall A, B. A = B \iff (\forall x. x \in A \iff x \in B).$$

Definition 1.1.4. (**The Empty Set**) The **empty set** is the set containing no members. It is denoted as $\{\}$ or by using the symbol $\emptyset$. The definable property of $\emptyset$ is $\forall x. x \notin \emptyset$.

Definition 1.1.5. (**Cardinality**) The **cardinality** of a set is its size. For a finite set, the cardinality of a set is the number of members it contains. The size of a set S is written $|S|$.

1.1.1 Set Operations

Definition 1.1.6. (**Intersection**) The **intersection** of two sets A and B is the collection of all objects that are in both sets. It is written $A \cap B$. We can write this using a set comprehension, such that

$$A \cap B = \{x : x \in A \wedge x \in B\}.$$

Definition 1.1.7. (**Disjoint sets**) If A and B are sets and $A \cap B = \emptyset$, then we say that A and B are **disjoint**.

Definition 1.1.8. (**Union**) The **union** of two sets A and B is the collection of all objects that are in either set. It is written $A \cup B$, such that

$$A \cup B = \{x : x \in A \vee x \in B\}.$$

Definition 1.1.9. (**Compliment**) The **compliment** of a set S is the collection of objects in the universal set $\mathcal{U}$ that are not in S. The compliment is written S^c, such that

$$S^c = \{x \in \mathcal{U} : x \notin S\}.$$

Definition 1.1.10. (**Difference**) The **difference** of two sets A and B is the collection of objects in A that are not in B. The difference is written $A \setminus B$, such that

$$A \setminus B = A \cap B^c = \{x : x \in A \wedge x \notin B\}.$$

Definition 1.1.11. (**Cartesian product**) The **Cartesian product** between two sets A and B is the set of all possible ordered pairs with the first element from A and second element from B. The product is written $A \times B$, such that

$$A \times B = \{(x, y) : x \in A \wedge y \in B\}.$$

1.1.2 Subsets

Definition 1.1.12. (**Subset**) For two sets A and B we say that A **is a subset of** B if each element of A is also an element of B.

$$A \subseteq B \iff \forall x.x \in A \implies x \in B.$$

If $A \subseteq B \wedge A \neq B$ then we write $A \subset B$ and we say A is a *proper subset* of B. The empty set $\emptyset$ is a subset of every set.

Theorem 1.1.1. For all sets A, B, C, we have

1. **Reflexivity**: $A \subseteq A$
2. **Transitivity**: $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$
3. **Antisymmetry**: $A \subseteq B \wedge B \subseteq A \implies A = B$

Definition 1.1.13. (**Powerset Axiom**) For any set S, there exists a set consisting of all it's subsets.

Definition 1.1.14. The set whose existence is postulated by the powerset axiom, denoted $\mathcal{P}(S)$, is defined as

$$\mathcal{P}(S) = \{X : X \subseteq S\}.$$

Theorem 1.1.2. For all finite sets S,

$$|\mathcal{P}(S)| = 2^{|S|}.$$

1.1.3 Pairs

Definition 1.1.15. Pairing Axiom For all a, b there is a set with a and b as it's only elements.

Definition 1.1.16. (**Pair**) The pair of a, b is the set whose existence is postulated by the pairing axiom, denoted $\{a, b\}$.

Note that

$$\forall x. x \in \{a, b\} \iff x = a \vee x = b.$$

Definition 1.1.17. (**Singleton**) For all a, the pair $\{a, a\}$, denoted $\{a\}$, is said to be a *singleton*.

Definition 1.1.18. (**Ordered Pairs**) For all a, b, the ordered pair (a, b) is the set $\{\{a\}, \{a, b\}\}$

Theorem 1.1.3. (**Fundamental property of ordered pairs**) For all a, b, x, y,

$$(a, b) = (x, y) \iff a = x \wedge b = y.$$

Proof. Let a, b, x, y be arbitrary.
$(\implies)$. Let us assume that $(a, b) = (x, y)$, that is to say

$$\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}.$$

We have two cases:

1. **Case** $a = b$. Let us assume that $a = b$, so we have

   $$(a, b) = \{\{a\}, \{a\}\} = \{\{a\}\}.$$

   By our initial assumptions, we have

   $$\{\{x\}, \{x, y\}\} = \{\{a\}\}.$$

   Hence $\{x\} = \{x, y\} = \{a\}$. Hence $x = a$ and $x = y$. By transitivity of $=$, we have $x = a$ and $b = y$.

2. **Case** $a \neq b$. Let us assume that $a \neq b$. We wish to show that

   $$a = x \wedge b = y.$$

   We have three cases:

   (a) **Case** $\{a\} = \{x, y\}$. Let us assume that $\{a\} = \{x, y\}$. Then $a = x = y$. Hence $(x, y) = \{\{a\}\}$. However, this implies that $(a, b) = \{\{a\}\}$, so $a = b$. A contradiction!

   (b) **Case** $\{a, b\} = \{x\}$. Then $x = a = b$. A contradiction!

   (c) **Case** $\{a\} = \{x\}$. Let us assume that $\{a\} = \{x\}$, so we have $a = x$. We wish to show that $b = y$. Suppose that $a = y$. Then $\{x, y\} = \{a\} \neq \{a, b\}$. Hence $b = y$. So we are done.

$(\impliedby)$. Let us assume that $a = x \wedge b = y$. So we have

$$\{a\} = \{x\} \wedge \{a, b\} = \{x, y\}.$$

So by the extensionality axiom, we have

$$\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}.$$

So we are done. □

1.1.4 Big Unions and Intersections

Definition 1.1.19. Let $\mathcal{U}$ be some universal set. For a collection of sets $\mathcal{F} \subseteq \mathcal{P}(\mathcal{U})$, the big union is defined as

$$\bigcup \mathcal{F} = \{x \in \mathcal{U} : \exists X \in \mathcal{F}.x \in X\} \subseteq \mathcal{U}.$$

Definition 1.1.20. Let $\mathcal{U}$ be some universal set. For a collection $\mathcal{F} \subseteq \mathcal{P}(\mathcal{U})$, the big intersection is defined as

$$\bigcap \mathcal{F} = \{x \in \mathcal{U} : \forall X \in \mathcal{F}.x \in X\}.$$

1.1.5 Disjoint Unions

Definition 1.1.21. (**Tagging**) Let S be some set. The set of elements S tagged by labels ℓ is defined as

$$S_\ell = \{\ell\} \times S = \{(\ell, x) : x \in S\}.$$

Note that

$$\forall y \in S_\ell . \exists! x \in S . y = (\ell, x)$$
$$S^1_{\ell_1} = S^2_{\ell_2} \iff \ell_1 = \ell_2 \wedge S^1 = S^2$$

Definition 1.1.22. (**Disjoint Union**) The disjoint union $A \uplus B$ of the sets A, B is

$$A \uplus B = A_1 \cup B_2.$$

Hence

$$\forall x . x \in A \uplus B \iff (\exists! a \in A . x = (1, a)) \vee (\exists! b \in B . x = (2, b)).$$

Theorem 1.1.4. For all finite sets A, B

$$|A \uplus B| = |A| + |B|.$$

1.2 Relations

Definition 1.2.1. (**Relation**) A *relation* $\mathcal{R}$ on $A \times B$ is a tuple $(A, B, \sim)$, denoted

$$\sim : A \nrightarrow B,$$

where $\sim \subseteq A \times B$. For $(a, b) \in \sim$, we denote $a \sim b$ for simplicity.

The set of relations on $A \times B$ is denoted as $\mathcal{P}[A \nrightarrow B]$, that is

$$\mathcal{P}[A \nrightarrow B] = \mathcal{P}(A \times B).$$

Theorem 1.2.1. For finite A, B, we have

$$|\mathcal{P}[A \nrightarrow B]| = 2^{|A| \cdot |B|}.$$

Relations of special types. For a binary relation $\mathcal{R}$ on S, we say $\sim$ is

- (R) *Reflexive* if $a \sim a$ for all $a \in S$
- (S) *Symmetric* if $a \sim b \implies b \sim a$ for all $a, b \in S$
- (T) *Transitive* if $a \sim b \wedge b \sim c \implies a \sim c$ for all $a, b, c \in S$

Axiom 1.2.1. (**Relationship Extensionality**) For all relations $R : A \nrightarrow B$ and $S : A \nrightarrow B$, we have

$$R = S \iff \forall a \in A. \forall b \in B. a \; R \; b \iff a \; S \; b.$$

Definition 1.2.2. (**Relational Composition**) The composition of two relations $R : A \nrightarrow B$ and $S : B \nrightarrow C$ is the relation

$$(S \circ R) = \{(a, c) : \exists b \in B. a \; R \; b \wedge b \; R \; c\} : A \nrightarrow C.$$

Theorem 1.2.2. Relational composition is associative with an identity id_S.

- (A) *Associativity*: For all $R : A \nrightarrow B, S : B \nrightarrow C$ and $T : C \nrightarrow D$,

$$(T \circ S) \circ R = T \circ (S \circ R).$$

- (I) *Identity*: For all $R : A \nrightarrow B$,

$$id_B \circ R = R = R \circ id_A.$$

1.2.1 Partitions and Equivalent Relations

Definition 1.2.3. (**Equivalent Relations**) A relation $\sim : S \nrightarrow S$ is said to be an equivalent relation if (R), (S) and (T) hold.

The set of all equivalent relations on S is denoted $\text{EqRel}(S)$.

Definition 1.2.4. (**Equivalence Class of** x) Let S be some arbitrary set and $\sim$ be an equivalence relation on S. For $x \in S$, the equivalence class of x is defined as

$$[x]_\sim = \{y \in S : y \sim x\}.$$

Definition 1.2.5. (**Partitions**) A partition $\mathcal{F}$ of a set S is a set of non-empty disjoint subsets of S. That is

$$S = \bigcup \mathcal{F},$$

and

$$\forall X, Y \in \mathcal{F}. X \neq Y \implies X \cap Y = \emptyset.$$

The set of all partitions of S is denoted $\text{Part}(S)$.

Theorem 1.2.3. For every set S,

$$\text{EqRel}(S) \cong \text{Part}(S).$$

1.2.2 Orders

Definition 1.2.6. (**Preorder**) A preorder on S is the tuple $(S, \sqsubseteq)$ with the relation $\sqsubseteq$: $S \nrightarrow S$ satisfying (R) and (T).

Definition 1.2.7. (**Partial order**) A partial order on S is the tuple $(S, \sqsubseteq)$ with the relation $\sqsubseteq$: $S \nrightarrow S$ satisfying (R), (AS) and (T).

Definition 1.2.8. (**Total order**) A total order on S is the partial order $(S, \sqsubseteq)$ with the relation $\sqsubseteq$: $S \nrightarrow S$ that further satisfies

$$\forall x, y \in S. x \sqsubseteq y \vee y \sqsubseteq x.$$

1.2.3 Relational Images

Definition 1.2.9. Let $R : A \nrightarrow B$ be a relation. The direct image of $X \subseteq A$ under R is the set $\overrightarrow{R}(X) \subseteq B$ defined as

$$\overrightarrow{R}(X) = \{b \in B : \exists x \in X. (x, b) \in R\} : \mathcal{P}(A) \to \mathcal{P}(B).$$

The inverse image of $Y \subseteq B$ under R is the set $\overleftarrow{R}(Y) \subseteq A$, defined as

$$\overleftarrow{R}(Y) = \{a \in A : \exists b \in Y. (a, b) \in R\} : \mathcal{P}(B) \to \mathcal{P}(A).$$

1.3 Functions

1.3.1 Partial Functions

Definition 1.3.1. (**Partial Function**) A relation $R : A \nrightarrow B$ is said to be a partial function if and only if

$$\forall a \in A. \forall b_1, b_2 \in B. (a, b_1) \in R \wedge (a, b_2) \in R \implies b_1 = b_2.$$

We write $f : A \rightharpoonup B$ to denote that f is a partial function from A to B. The set of all partial functions from A to B is denoted as

$$\mathcal{P}[A \rightharpoonup B] \subseteq \mathcal{P}[A \nrightarrow B].$$

Theorem 1.3.1. For all finite sets A, B,

$$|\mathcal{P}[A \rightharpoonup B]| = (|B| + 1)^{|A|}.$$

The value of f at a, denoted $f(a)$ is defined as

$$f(a) = \begin{cases} b & \text{if } f(a) \downarrow \\ \text{undefined} & \text{otherwise} \end{cases}.$$

where

$$f(a) \downarrow = \exists! x \in f. x = (a, b),$$

which indicates where f is defined at a.

Axiom 1.3.1. (**Partial Extensionality**) For all partial functions $f : A \rightharpoonup B$ and $g : A \rightharpoonup B$, we have

$$f = g \iff \forall a \in A. (f(a) \downarrow \iff g(a) \downarrow) \wedge f(a) = g(a).$$

Theorem 1.3.2. Composition of partial functions yields a partial function and the identity relation is a partial function.

1.3.2 Total Functions

Definition 1.3.2. (**Total Function**) A total function is a relation $R : A \nrightarrow B$ that satisfies

$$\forall a \in A. \exists! b \in B. (a, b) \in R.$$

Equivalently, a total function is a partial function $f : A \rightharpoonup B$ such that $\forall a \in A.f(a)\downarrow$. We write $f : A \to B$ to denote a total function f from A to B. The set of all total functions from A to B is written as

$$\mathcal{P}[A \to B] \subseteq \mathcal{P}[A \rightharpoonup B] \subseteq \mathcal{P}[A \nrightarrow B].$$

Theorem 1.3.3. For all finite sets A, B,

$$|\mathcal{P}[A \to B]| = |B|^{|A|}.$$

Theorem 1.3.4. Composition of total functions yields a total function and the identity relation is a total function.

Injections

Definition 1.3.3. A function $f : A \to B$ is said to be injective, or an injection, if and only if

$$\forall a_1, a_2 \in A.f(a_1) = f(a_2) \implies a_1 = a_2.$$

Properties

- For all injections $f : A \to B$ and $g : B \to C$, $g \circ f : A \to C$ is injective.
- For all functions $f : A \to B$ and $g : B \to C$,

  $$g \circ f \text{ is injective} \implies f \text{ is injective},$$

  but g is not necessarily injective.
- For all injections $f : A \to B$, there exists a left unique inverse $g : B \to A$ such that $g \circ f = id_A$.
- The set of injections from A to B is denoted $\text{Inj}(A, B)$.

Surjections

Definition 1.3.4. A function $f : A \to B$ is said to be surjective, or an surjection, if and only if

$$\forall b \in B.\exists a \in A.f(a) = b.$$

Properties

- For all surjections $f : A \to B$ and $g : B \to C$, $g \circ f : A \to C$ is surjective.
- For all functions $f : A \to B$ and $g : B \to C$,

$$g \circ f \text{ is surjective } \implies g \text{ is surjective,}$$

  but f is not necessarily surjective.
- For all surjections $f : A \to B$, there exists a unique right inverse $g : B \to A$ such that $f \circ g = id_B$.
- The set of surjections from A to B is denoted $\mathrm{Sur}(A, B)$.

Bijections

Definition 1.3.5. A function $f : A \to B$ is said to be bijective, or a bijection, if f is injective and surjective.

Equivalently, a function $f : A \to B$ is a bijection if there exists a unique function $f^{-1} : B \to A$ such that

1. f^{-1} is a left inverse for f, that is

$$f^{-1} \circ f = id_A.$$

2. f^{-1} is a right inverse for f, that is

$$f \circ f = id_B.$$

Properties

- For all bijections $f : A \to B$ and $g : B \to C$, $g \circ f : A \to C$ is bijective.
- The set of bijections from A to B is denoted $\mathrm{Bij}(A, B)$,

$$\mathrm{Bij}(A, B) = \mathrm{Inj}(A, B) \cap \mathrm{Sur}(A, B).$$

  where

$$|\mathrm{Bij}(A, B)| = \begin{cases} 0 & \text{if } |A| \neq |A| \\ n! & \text{if} |A| = |B| = n \end{cases}.$$

Definition 1.3.6. (**Isomorphism**) Two sets A and B are said to be isomorphic (and have the same cardinality) if there exists a bijection $\phi : A \to B$. That is to say

$$A \cong B \iff |A| = |B| \iff \exists \phi : A \to B . \phi \in \text{Bij}(A, B).$$

1.3.3 Functional Images

Definition 1.3.7. Let $f : A \to B$ be a function. The direct image of $X \subseteq A$ under f is the set $\overrightarrow{f}(X) \subseteq B$ defined as

$$\overrightarrow{f}(X) = \{f(a) \in B : a \in X\} : \mathcal{P}(A) \to \mathcal{P}(B).$$

The inverse image of $Y \subseteq B$ under f is the set $\overleftarrow{f}(Y) \subseteq A$, defined as

$$\overleftarrow{f}(Y) = \{a \in A : f(a) \in Y\} : \mathcal{P}(B) \to \mathcal{P}(A).$$

1.4 Enumerability, Countability and Other Theorems

Definition 1.4.1. (**Enumerable**) A set S is said to be enumerable if there exists a surjection $\mathbb{N} \to S$.

Definition 1.4.2. (**Countable**) A set S is said to be countable if it is either empty or enumerable.

Theorem 1.4.1. Every non-empty subset X of a enumerable set S is enumerable.

Theorem 1.4.2.

- The product and disjoint union of countable sets is countable
- Every finite set is countable
- Every subset of a countable set is countable

Definition 1.4.3. A set A is of less than or equal cardinality to a set B if there exists an injection $f : A \to B$. We write

$$A \lesssim B \iff |A| \leq |B|.$$

Since each injection has a left inverse (which is surjective), then if there exists a surjection $f : B \to A \implies |A| \leq |B|$.

Theorem 1.4.3. (**Cantor-Schroeder-Bernstein theorem**) For all sets A, B

$$A \lesssim B \wedge B \lesssim A \implies A \cong B.$$

2 Structures

2.1 Binary Operations

Definition 2.1.1. (**Binary operation**) A **binary operation** $*$ on a set S is a function

$$* : S \times S \to S.$$

Instead of writing $*(a, b)$, we write $a * b$ for convenience.

2.1.1 Cayley Tables

For binary operations on small finite sets, the binary operation may be recorded using a table, called the *cayley table*.

For example, let $S = \{\alpha, \beta, \gamma\}$. We may define a binary operation $*$ as follows:

$*$	α	β	γ
α	α	γ	β
β	α	β	β
γ	β	α	γ

where we take the row first then the column. So, for example $\alpha * \beta = \gamma$, $\beta * \alpha = \alpha$, etc. In general, if $S = \{a_1, a_2, \ldots, a_n\}$, then the entry in the row label by a_i and the column labeled by a_j is $a_i * a_j$.

2.1.2 Commutative and associative binary operations

Definition 2.1.2. (**Commutative**) A binary operation $*$ on a set S is **commutative** if

$$a * b = b * a.$$

for all $a, b \in S$.

Definition 2.1.3. (**Associative**) A binary operation $*$ on a set S is **associative** if

$$a * (b * c) = (a * b) * c.$$

for all $a, b, c \in S$.

If $*$ is associative, then we can write $a * b * c$, meaning $(a * b) * c$ and $a * (b * c)$. More generally, we may define longer expressions $a_1 * \cdots * a_n$. Hence for $n \in \mathbb{N}$ and $a \in S$, we may define

$$a^n = \underbrace{a * \cdots * a}_{n\text{-times}}..$$

2.1.3 Identity elements

Consider $\mathbb{Z}$. Note that $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$. Also note that $1 \times a = a \times 1 = a$ for all $a \in \mathbb{Z}$. These two binary operations are said to have an identity element.

Definition 2.1.4. (**Identity element**) Let $*$ be a binary operation on a set S. We say that $e \in S$ is an identity element for S with respect to $*$ if

$$\forall a \in S, \exists e \in S : e * a = a * e = a..$$

Theorem 2.1.1. (**Uniqueness of the identity**) Let $*$ be a binary operation on a set S. Let $e, f \in S$ be identity elements for S with respect to $*$. Then $e = f$

Proof. Given e is an identity element and $f \in S$, then $e * f = f$. Since f is an identity element and $e \in S$, we have $e * f = e$. Hence $e = e * f = f$ □

2.1.4 Inverse elements

Consider addition on $\mathbb{R}$ which has an identity element $0 \in \mathbb{R}$. Note that $a + (-a) = (-a) + a = 0$. This binary operation is said to have inverse elements for each $a \in \mathbb{R}$ which is denoted as $-a \in \mathbb{R}$, in this case they are known as additive inverses.

Definition 2.1.5. (**Inverse elements**) Let $*$ be a binary operations on a set S. We say an inverse of $a \in S$ is an element b, such that $a * b = b * a = e$, where e is the identity element for S with respect to $*$.

2.2 Structures

2.2.1 Monoids

Definition 2.2.1. (**A Monoid**) A **monoid** is a non-empty set M with a binary operation $* : M \times M \to M$ satisfying

(i) **Associativity:** For all $a, b, c \in M$, we have

$$a * (b * c) = (a * b) * c.$$

(ii) **Identity:** There exists an element $e \in G$ with the property that

$$e * a = a * e = a$$

for all $a \in M$.

A monoid $(M, *)$ is said to be **commutative** if $*$ is commutative (unsurprisingly...)

2.2.2 Groups

Definition 2.2.2. (**A Group**) A **group** is a non-empty set G with a binary operation $* : G \times G \mapsto G$ satisfying.

(i) **Associativity:** For all $a, b, c \in G$, we have

$$a * (b * c) = (a * b) * c.$$

(ii) **Identity:** There exists an element $e \in G$ with the property that

$$e * a = a * e = a$$

for all $a \in G$.

(iii) **Invserses:** For every $a \in G$, there is an element $b \in G$ with the property

$$a * b = b * a = e.$$

To be concise, we'll often write $(G, *)$ to denote the set G forming a group under $*$.

Theorem 2.2.1. In (iii), the element b is the **inverse** of a. It is unique, hence we may refer to the (unique) inverse of a, and write a^{-1}.

Proof. Let G form a group under the binary operation $*$, so we have the group $(G, *)$. Let $b_1, b_2 \in G$ be inverses of $a \in G$, with respect to the binary operation $*$ on the set G, hence

$$a * b_1 = b_1 * a = e$$
$$a * b_2 = b_2 * a = e$$

then,

$$b_1 * (a * b_2) = b_1 * e = b_1$$
$$b_2 * (a * b_1) = b_2 * e = b_2$$

since $*$ is associative, we can say

$$b_1 * (a * b_2) = (b_1 * a) * b_2$$
$$b_1 = b_2$$

Thus completing the proof. □

2.2.3 Rings

Definition 2.2.3. A structure $(R, +, \cdot)$ is a **ring** if R is a non-empty set and $+$ and $\cdot$ are binary operations

$$+ : R \times R \to R,$$
$$\cdot : R \times R \to R,$$

such that they satisfy the following axioms:

(i) **Addition**: $(R, +)$ is a commutative group, that is

(A1) **Associativity**: For all $a, b, c \in R$ we have $a + (b + c) = (a + b) + c$.

(A2) **Zero Element**: There exists $0 \in R$ such that for all $a \in R$ we have $a + 0 = 0 + a = a$

(A3) **Inverses**: For all $a \in R$ there exists $-a \in R$ such that $a + (-a) = (-a) + a = 0$.

(A4) **Commutativity**: For all $a, b \in R$ we have $a + b = b + a$.

(ii) **Multiplication**:

(M1) **Associativity**: For all $a, b, c \in R$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) **Distributivity**:

(D1) For all $a, b, c \in R$ we have

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Definition 2.2.4. Assume $(R, +, \cdot)$ is a ring. We say R is a commutative ring if its multiplication $\cdot$ is commutative, that is to say

(M2) **Commutativity**: For all $a, b \in \mathbb{R}$ we have $a \cdot b = b \cdot a$.

(M3) **Identity Element**: There exists $1 \in \mathbb{R}$ such that for all $a \in \mathbb{R}$ we have $a \cdot 1 = 1 \cdot a = a$.

2.2.4 Fields

Definition 2.2.5. A structure $(R, +, \cdot)$, where $+$ and $\cdot$ are binary operations on R is a field if (A1)-(A4), (M1)-(M3) and (D1) hold, $0 \neq 1$ and

(M4) **Inverses**: For all $a \in R$ where $a \neq 0$ there exists $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

This can be expressed in a more modular way as follows, $(R, +, \cdot)$ is a field if

(F1) $(R, +)$ is a commutative group

(F2) $(R \setminus \{0\}, \cdot)$ is a commutative group

(F3) The distributive laws hold

3 Numbers

3.1 Natural Numbers

Recall that we have adopted the convention that

$$\mathbb{N}_0 = \{0, 1, 2, \ldots\}.$$

where $\mathbb{N}_0$ is the set of natural numbers (including 0) and

$$\mathbb{N}_1 = \{1, 2, 3, \ldots\}.$$

where $\mathbb{N}_1$ is the set of natural numbers (excluding 0). Note that $\mathbb{N}_1 = \mathbb{Z}^+$.

3.2 Division

Definition 3.2.1. Given two integers $a, b \in \mathbb{Z}$, we say a *divides* b , written as $a \mid b$ if $a \neq 0$ and there exists some integer k such that $b = k \cdot a$.

3.3 The Division Theorem

Theorem 3.3.1. (**Division Theorem**) For all pairs of integers $m, n \in \mathbb{Z}$ where $n \neq 0$ there exists a unique pair of integers q, r such that $0 \leq r < |n|$ and $m = q \cdot n + r$. More formally

$$\forall m, n \in \mathbb{Z}, n \neq 0. \exists! q, r \in \mathbb{Z}. m = q \cdot n + r, 0 \leq r < |n|.$$

In the above, we say that m is the dividend, n is the divisor, q is the quotient and r is the remainder.

Proof. Let m, n be some arbitrary pair of integers where $n \neq 0$.

Existence.
We have two cases, $n > 0$ and $n < 0$.

1. **Case** $n < 0$. Let $n' = -n$ and $q' = -q$, so the equation $m = q \cdot n + r$ can be rewritten as $m = q' \cdot n' + r$ and the inequality $0 \leq r < |n|$ may be rewritten as $0 \leq r < |n'|$. This reduces the existence for the case $n < 0$ to that of the case $n > 0$.

2. **Case** $n > 0$. We have two cases, $m < 0$ and $m \geq 0$.

   (a) **Case** $m < 0$. Let $m' = -m$, $q' = -q - 1$ and $r' = n - r$. Thus the proof of existence is reduced to the case $m \geq 0$ and $n > 0$.

   (b) **Case** $m \geq 0$. Let $q_0 = 0$ and $r_1 = m$, then these are natural numbers such that $m = q_1 \cdot n + r_1$. If $r_1 < n$, then the division is complete.

   So suppose that $r_1 \geq n$. Then define $q_2 = q_1 + 1$ and $r_2 = r_1 - n$, one has $m = q_2 \cdot n + r_2$ with $0 \leq r_2 < r_1$.

   Given there exists r_1 unique natural numbers less than r_1, then this process needs to repeat at most r_1 times to reach the final quotient and the remainder.

   That is to say, there exists a natural number $k \leq r_1$ such that $m = q_k \cdot n + r_k$ and $0 \leq r_k < |n|$.

   This proves the existence.

Uniqueness
To prove uniqueness, we wish to show the following

$$\begin{aligned}\forall m, n \in \mathbb{Z}, n \neq 0. \forall q, r, q', r' \in \mathbb{Z} \\ .m = q \cdot n + r, 0 \leq r < |n|, m = q' \cdot n + r', 0 \leq r' < |n| \\ \implies q = q' \wedge r = r'\end{aligned}$$

Let $m, n \in \mathbb{Z}$ be arbitrary integers where $n \neq 0$. Let q, r, q', r' be arbitrary integers. Let us assume that

$$\begin{aligned} 0 \leq r' < |n| \\ 0 \leq r < |n| \\ m = q' \cdot n + r' \\ m = q \cdot n + r \end{aligned}$$

Subtracting the two equations yield

$$n \cdot (q' - q) + (r' - r) = 0.$$

So we have $q' - q \mid r - r'$. So n is a divisor of $r - r'$. By our initial assumptions, we have

$$0 \leq |r - r'| < 0.$$

So we have $r - r' = 0$ and $n \cdot (q' - q) = 0$. Since $n \neq 0$, we get that $r = r'$ and $q = q'$. Which proves uniqueness. □

Lemma 3.3.1. Let $q, n, r \in \mathbb{Z}$ be arbitrary integers where $n \neq 0$.

$$q \cdot n + r = 0 \wedge 0 \leq r < |n| \implies q = 0 \wedge r = 0.$$

Proof. Let $q, n, r \in \mathbb{Z}$ be arbitrary integers where $n \neq 0$. Let us assume that $q \cdot n + r = 0$ and $0 \leq r < |n|$ As $q \cdot n = -r$ and since $r \geq 0$, then we have $q \cdot n \leq 0$ and $q \cdot n > -n$.

We have two cases, $n > 0$ and $n < 0$.

1. **Case** $n < 0$. Let $n' = -n$ and $q' = -q$, so the equation $q \cdot n + r = 0$ can be rewritten as $q' \cdot n' + r = 0$ and the inequality $0 \leq r < |n|$ may be rewritten as $0 \leq r < |n'|$. This reduces the existence for the case $n < 0$ to that of the case $n > 0$.

2. **Case** $n > 0$. Assume that $n > 0$, then from $q \cdot n \leq 0$, we have $q \leq 0$ and from $q \cdot n > -n$, we have $q > -1$. Hence $q = 0$, so it follows that $r = 0$.

□

3.4 The Division Algorithm

A division algorithm is an algorithm that given two integers m, n computes their **quotient** and **remainder**.

We will consider the following implementation of the division algorithm in OCaml

```
let divalg m n =
    let rec inner q r =
        if r < n then (q, r)
        else inner (q + 1) (r - n)
    in inner 0 m
```

Theorem 3.4.1. (**Termination and Correctness of** `divalg`) For all natural number $m, n \in \mathbb{N}$ where $n \neq 0$, the evaluation of `divalg m n` terminates producing a pair of natural numbers q_k, r_k such that $0 \leq r_k < n$ and $m = q_0 \cdot n + r_0$.

Proof. Let m, n be some arbitrary natural numbers where $n \neq 0$.
Termination
The evaluation of `divalg m n` diverges if and only if the evaluation of `inner 0 m` diverges; this is true if and only if $m - i \cdot n \geq n$ for all natural numbers i. This is absurd, thus the evaluation of `divalg m n` terminates. With time complexity $\Omega(m)$.
Correctness
We wish to show that `divalg m n` produces a pair of natural numbers q_k, q_r such that $m = q_k \cdot n + r_k$ and $0 \leq r_k < n$.

We proceed by showing the following invariant on the arguments of `inner`.

$$P(i) = i^{th} \text{ recursive call of } \texttt{inner q r} \text{ satisfies } m = q_i \cdot n + r_i \wedge r_i \geq 0.$$

We proceed by induction on $i \in \mathbb{N}$.

Proof.
Base Case. The $i = 0^{th}$ call to `inner` is `inner 0 m`, so we have $q_0 = 0$ and $r_0 = m$, hence

$$m = 0 \cdot n + m,$$

and $r_0 \geq n$. So $P(0)$ holds.
Inductive Step. We wish to show that $\forall i \in \mathbb{N}. P(i) \implies P(i+1)$. Let $i \in \mathbb{N}$ be an arbitrary natural number. Let us assume that $P(i)$ holds, so we have $m = q_i \cdot n + r_i$.

We may assume that `inner` doesn't terminate, so we may assert that $r_i \geq n$, hence for the $i+1^{th}$ call of `inner` we have the arguments $q_{i+1} = q_i + 1$ and $r_{i+1} = r_i - n$ respectively. We note that,

$$q_{i+1} \cdot n + r_{i+1} = (q_i + 1) \cdot n + (r_i - n) = q_i \cdot n + r_i,$$

hence by our initial assumptions $m = q_{i+1} \cdot n + r_{i+1}$. Similarly, since $r_i \geq n$, we have $r_{i+1} = r_i - n \geq 0$.

By the Principle of Mathematical Induction, we conclude that $P(i)$ holds for all $i \in \mathbb{N}$ □

At the k^{th} recursive call, `inner` terminates with $m = q_k \cdot r + r_k$ and $r_k \geq 0$. Since `inner` terminates, we may assert that $r_k < n$. This completes the proof. □

Some notation

1. **Remainder**: $\text{rem}(m, n)$ is defined as the remainder r_k produced by the evaluation of `divalg m n`.
2. **Quotient**: $\text{quo}(m, n)$ is defined as the quotient q_k produced by the evaluation of `divalg m n`.

3.5 Modular Arithmetic

Definition 3.5.1. For a pair of integers a, b and some positive integer m, we say that a is congruent modulo m if $m \mid a - b$. We write $a \equiv b \pmod{m}$.

Definition 3.5.2. (**Congruence relation modulo** m) Let $m \in \mathbb{Z}$ is an integer. We define $\mathcal{R}_m$ as the congruence relation modulo m on the set of all $a, b \in \mathbb{Z}$:

$$\mathcal{R}_m = \left\{(a, b) \in \mathbb{Z}^2 : \exists k \in \mathbb{Z} : a = k \cdot m + b\right\}.$$

For any $m \in \mathbb{Z}$, we denote the equivalence class of an integer $a \in \mathbb{Z}$ by $[a]_m$ such that

$$[a]_m = \{x \in \mathbb{Z} : a \equiv x \pmod{m}\}.$$

Definition 3.5.3. (**Integers Modulo** m) Let $m \in \mathbb{Z}$ be an integer. The integers modulo m are the set of positive integers

$$\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}.$$

which is in fact equivalent to the set of the least positive integer from the equivalence classes $[0]_m, [1]_m, \ldots, [m - 1]_m$.

Definition 3.5.4. (**Modulo Addition**) Let $m \in \mathbb{Z}$ be an integer. Let $\mathbb{Z}_m$ be the set of integers modulo m. The operation of **addition modulo** m is defined on $\mathbb{Z}_m$ as

$$[a]_m +_m [b]_m = [a + b]_m.$$

Definition 3.5.5. (**Modulo Multiplication**) Let $m \in \mathbb{Z}$ be an integer. Let $\mathbb{Z}_m$ be the set of integers modulo m. The operation of **addition multiplication** m is defined on $\mathbb{Z}_m$ as

$$[a]_m \times_m [b]_m = [a \times b]_m.$$

Theorem 3.5.1. ($\mathbb{Z}_n$ **is a ring**) The structure $(\mathbb{Z}_n, +_m, \cdot_m)$ forms a commutative ring.

Proof. We are required to show that $(\mathbb{Z}_n, +_m, \cdot_m)$ satisfies the axioms (A1)-(A4), (M1) and (D1). Recall that $\mathbb{Z}_n = \{0, 1, \ldots, m-1\}$ and

$$[a]_m +_m [b]_m = [a+b]_m \text{ and } [a]_m \cdot_m [b]_m = [a \cdot b]_m.$$

(i) **Addition**:

(A1) **Associativity**: Let a, b, c be some arbitrary integers modulo m. So we have

$$\begin{aligned}
[a]_m +_m ([b]_m +_m [c]_m) &= [a]_m +_m [b+c]_m \\
&= [a + (b+c)]_m \\
&= [(a+b) + c]_m \\
&= [a+b]_m +_m [c]_m \\
&= ([a]_m +_m [b]_m) +_m [c]_m
\end{aligned}$$

So we are done.

(A2) **Zero Element**: The additive identity (or zero element) is 0 since for all $a \in \mathbb{Z}_m$, we have

$$\begin{aligned}
[0]_m +_m [a]_m &= [0+a]_m \\
&= [a]_m
\end{aligned}$$

By (A4), it follows that $[a]_m = [a]_m +_m [0]_m$. So we are done.

(A3) **Inverses**: Let a be some arbitrary integer modulo m. We define the inverse for a as $-a$ since

$$\begin{aligned}
[a]_m +_m [-a]_m &= [a + (-a)]_m \\
&= [0]_m
\end{aligned}$$

By (A4), we have $[-a]_m +_m [a]_m = [0]_m$. So we are done.

(A4) **Commutativity**: Let a, b be some arbitrary integers modulo m.

$$\begin{aligned}[a]_m +_m [b]_m &= [a+b]_m \\ &= [b+a]_m \\ &= [b]_m +_m [a]_m\end{aligned}$$

So we are done.

(ii) **Multiplication**:

(M1) **Associativity**: Let a, b, c be integers modulo m. So we have

$$\begin{aligned}[a]_m \cdot_m ([b]_m \cdot_m [c]_m) &= [a]_m \cdot_m [b \cdot c]_m \\ &= [a \cdot (b \cdot c)]_m \\ &= [(a \cdot b) \cdot c]_m \\ &= [a \cdot b]_m \cdot_m [c]_m \\ &= ([a]_m \cdot_m [b]_m) \cdot_m [c]_m\end{aligned}$$

So we are done.

(M2) **Commutativity**: Let a, b be some arbitrary integers modulo m. So we have

$$\begin{aligned}[a]_m \cdot_m [b]_m &= [a \cdot b]_m \\ &= [b \cdot a]_m \\ &= [b]_m \cdot_m [a]_m\end{aligned}$$

So we are done.

(M3) **Identity Element**: The multiplicative identity (or natural element) is 1 since for all $a \in \mathbb{Z}_m$, we have

$$\begin{aligned}[1]_m \cdot_m [a]_m &= [1 \cdot a]_m \\ &= [a]_m\end{aligned}$$

By (M2), it follows that $[a]_m = [1]_m \cdot_m [a]_m$. So we are done.

(iii) **Distributivity**:

(D1) Let a, b, c be some arbitrary integers modulo m. So we have

$$\begin{aligned}[a]_m \cdot_m ([b]_m +_m [c]_m) &= [a]_m \cdot_m [b+c]_m \\ &= [a \cdot (b+c)]_m \\ &= [(a \cdot b) + (a \cdot c)]_m \\ &= [a \cdot b]_m +_m [a \cdot c]_m \\ &= [a]_m \cdot_m [b]_m +_m [a]_m \cdot_m [c]_m\end{aligned}$$

From (M2), it follows that we are done.

Hence the structure $(\mathbb{Z}_m, +_m, \cdot_m)$ forms a commutative ring. □

Lemma 3.5.1. ($\mathbb{Z}_p$ **is a field**) Let p be prime. The structure $(\mathbb{Z}_p, +_p, \cdot_p)$ forms a field.

3.5.1 Other Theorems

Theorem 3.5.2. Let $m \in \mathbb{Z}^+$ be a positive integer. For all $k, l \in \mathbb{N}$,

$$k \equiv l \pmod{m} \iff \text{rem}(k, m) = \text{rem}(l, m).$$

Proof. Let $m \in \mathbb{Z}^+$ be an arbitrary positive integer. Let $k, l \in \mathbb{N}$ be arbitrary natural numbers.
($\implies$). Let us assume that $k \equiv l \pmod{m}$, that is to say

$$\exists \lambda \in \mathbb{Z}. k - l = \lambda \cdot m.$$

By definition, we have

$$\begin{aligned}k &= \text{quo}(k, m) \cdot m + \text{rem}(k, m) \\ l &= \text{quo}(l, m) \cdot m + \text{rem}(l, m)\end{aligned}$$

Hence

$$k - l = [\text{quo}(k, m) - \text{quo}(l, m)] \cdot m + [\text{rem}(k, m) - \text{rem}(l, m)] = \lambda_0 \cdot m.$$

Hence $m \mid \text{rem}(k, m) - \text{rem}(l, m)$, Since $0 \leq |\text{rem}(k, m) - \text{rem}(l, m)| < m$, it follows that $\text{rem}(k, m) = \text{rem}(l, m)$. So we are done. ($\impliedby$). Let us assume that $\text{rem}(k, m) = \text{rem}(l, m)$, so we have

$$k - l = [\text{quo}(k, m) - \text{quo}(l, m)] \cdot m.$$

Hence $m \mid k - l$, so by definition, $k \equiv l \pmod{m}$. □

Corollary 3.5.2.1. For all $n \in \mathbb{Z}$,

$$n \equiv \text{rem}(n, m) \pmod{m}.$$

Proof. Let $n \in \mathbb{Z}$ be an arbitrary integer. We have

$$n - \text{rem}(n, m) = \text{quo}(n, m) \cdot m.$$

Hence $m \mid n - \text{rem}(n, m)$, so by definition, $n \equiv \text{rem}(n, m) \pmod{m}$. □

3.6 Greatest Common Divisor

Definition 3.6.1. (**Divisors**) Let n be some natural number. The set of divisors of n is defined by

$$D(n) = \{d \in \mathbb{N} : d \mid n\}.$$

Proposition 3.6.1. For all natural numbers k, n, $D(k \cdot n) = D(k) \cup D(n)$

We note that the set of divisors is hard to compute. However, the computation of the greatest divisor of n is straightforward, since it is n.

Definition 3.6.2. (**Common Divisor**) Let S be a finite set of natural numbers, $S \subset \mathbb{N}$. Let $d \in \mathbb{N}_1$ such that c divides all the elements of S. That is

$$\forall x \in S.c \mid x.$$

Then c is a **common divisor** of all the elements in S.

Definition 3.6.3. (**Common Divisors**) Let m, n be two natural numbers. The set of common divisors of m and n is defined by

$$CD(m, n) = \{c \in \mathbb{N} : c \in D(m) \wedge c \in D(n)\}.$$

Note that since $CD(n, n) = D(n)$, then it follows that the set of common divisors is just as difficult to compute as divisors. However, we note that the *greatest common divisor* will be easier to compute and gives us an upper bound for $CD(m, n)$.

Proposition 3.6.2. For all natural numbers k, m and n:

- $CD(k \cdot n, n) = D(n)$
- $CD(m, n) = CD(n, m)$

Lemma 3.6.1. (**The Key Lemma**) The key lemma states that For all $m, m', n \in \mathbb{N}$ where $n \neq 0$.

$$m \equiv m' \pmod{n} \implies CD(m, n) = CD(m', n).$$

Proof. Let $m, m', n \in \mathbb{N}$ be some arbitrary natural numbers where $n \neq 0$. Assume that $m \equiv m' \pmod{m}$. That is to say there exists some integer $k \in \mathbb{Z}$ such that

$$m = m' + k \cdot n. \tag{†}$$

We're required to show that

$$CD(m, n) = \{d \in \mathbb{N} : d \mid m \wedge d \mid n\} = \{d \in \mathbb{N} : d \mid m' \wedge d \mid n\} = CD(m', n).$$

So we will prove that for all natural numbers $d \in \mathbb{N}$

$$d \mid m \wedge d \mid n \iff d \mid m' \wedge d \mid n. \tag{‡}$$

Let $d \in \mathbb{N}$ be some arbitrary natural number.
($\implies$). Assume $d \mid m \wedge d \mid n$, that is to say there exists some integers $\lambda, \mu \in \mathbb{Z}$ such that

$$m = \lambda \cdot d \tag{i}$$
$$n = \mu \cdot d \tag{ii}$$

From (†), we have

$$\begin{aligned} m' + k \cdot n &= \lambda \cdot d \\ m' + k \cdot (\mu \cdot d) &= \lambda \cdot d \\ m' &= d \cdot (\lambda - k \cdot \mu) \end{aligned}$$

So by definition of division, $d \mid m'$. By our initial assumption $d \mid n$, we have $d \mid m' \wedge d \mid n$.
($\impliedby$). Analogous to the previous implication. □

Lemma 3.6.2. For all $m, n \in \mathbb{N}$,

$$CD(m, n) = \begin{cases} D(n), & \text{if } n \mid m \\ CD(n, \operatorname{rem}(m, n)), & \text{otherwise} \end{cases}.$$

Definition 3.6.4. (**Greatest Common Divisor**) For a given pair of natural numbers $m, n \in \mathbb{N}$, the **greatest common divisor** of m and n is some natural number $d \in \mathbb{N}$ such that

- $d \mid m \wedge d \mid n$
- $\forall c \in \mathbb{N}.c \mid m \wedge c \mid n \implies c \mid d$
- By the transitivity of $\mid$, we note that $d = \gcd(m, n)$ is equivalent to

$$\forall c \in \mathbb{N}.c \mid m \wedge \mid n \iff c \mid d.$$

Proposition 3.6.3. The greatest common divisor of m and n is defined as the upper bound of $CD(m, n)$

3.6.1 Euclid's Algorithm

Since the natural number n is the greatest divisor in $D(n)$, then lemma 3.6.2 and proposition 3.6.3 we have

$$\gcd(m, n) = \begin{cases} n, & \text{if } n \mid m \\ \gcd(n, \text{rem}(m, n)), & \text{otherwise} \end{cases}.$$

The above forms the basis for the implementation of the **Euclidean algorithm** for computing the greatest common divisor of two positive integers m, n. So we have following recursive implementation in OCaml

```
let rec gcd m n =
    let r = rem m n in
        if r = 0 then n
        else gcd n r
```

Theorem 3.6.1. Euclid's Algorithm `gcd` terminates for all pairs of positive integers m, n such that `gcd m n` is the greatest common divisor.

Proof. Let m, n be some arbitrary positive integers.
Termination.
We have two cases $m < n$ and $m \geq n$.

1. **Case** $m < n$. Assume that $m < n$. So it follows that $n \mid m$ is false, hence
$$\gcd(m, n) = \gcd(n, \text{rem}(m, n)).$$
We note that $\text{rem}(m, n) = m$, hence $\gcd(m, n) = \gcd(n, m)$. This reduces the termination for the case $m < n$ to that of the case $m \geq n$.

2. **Case** $m \geq n$. Assume that $m \geq n$. We now have two cases, either $n \mid m$ or $n \nmid m$. In the case of $n \mid m$, `gcd` terminates, returning n.

   In the case of $n \nmid m$, then we may have
$$\begin{aligned}
m &= q_1 \cdot n + r_1 && 0 \leq r_1 < n \\
n &= q_2 \cdot r_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{i-2} &= q_i \cdot r_{i-1} + r_i && 0 \leq r_i < r_{i-1} \\
&\vdots \\
r_{k-3} &= q_{k-1} \cdot r_{k-2} + r_{k-1} && 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &= q_k \cdot r_{k-1} + 0
\end{aligned}$$
   This process must terminate as $0 \leq r_i < r_{i-1} < \cdots < r_2 < r_1 < n$, a strictly decreasing sequence.

Correctness
The correctness of the algorithm can be verified by
$$\gcd(m, n) = \begin{cases} n, & \text{if } n \mid m \\ \gcd(n, \text{rem}(m, n)), & \text{otherwise} \end{cases}.$$
Since for each call of `gcd m n`, we calculate $r = \text{rem}(m, n)$. If $r = 0$ then we terminate, which is equivalent to $n \mid m$. Otherwise we recursively call `gcd`. □

Complexity

Suppose that the Euclidean algorithm takes n steps to compute the greatest common divisor of the pair of natural numbers $a > b > 0$. We claim that

smallest values of a, b for which this is true are the Fibonacci numbers F_{n+2} and F_{n+1} respectively. We proceed by induction on n with the statement

$$P(n) = \forall a, b \in \mathbb{N}. |\gcd(a, b)| = n \implies a \geq F_{n+2} \wedge b \geq F_{n+1},$$

where $|\gcd(\cdot)|$ denotes the number of steps to compute the gcd.

Proof.
Base Case. If $n = 1$, then $b \mid a$. The smallest positive integers for which this is true is $a = 2$ and $b = 1$, which are F_3 and F_2 respectively. So the statement holds for $n = 1$.
Inductive Step. We wish to show that $P(n) \implies P(n+1)$. Let us assume that $P(n)$ holds, that is

$$\forall a, b \in \mathbb{N}. |\gcd(a, b)| = n \implies a \geq F_{n+2} \wedge b \geq F_{n+1}.$$

Let $a, b \in \mathbb{N}$ be arbitrary. Let us assume that $|gcd(a, b)| = n + 1$, that is to say

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b)),$$

requires $n + 1$ steps. So it follows that $\gcd(b, \text{rem}(a, b))$ requires n steps. By our inductive hypothesis, we have

$$b \geq F_{n+2} \wedge \text{rem}(a, b) \geq F_{n+1}.$$

By the division theorem, we note that

$$a = \text{quo}(a, b) \cdot b + \text{rem}(a, b).$$

We wish to show that $a \geq F_{n+3}$. Since $a > b > 0$, it follows that $\text{quo}(a, b) > 0$. Hence

$$a = \text{quo}(a, b) \cdot b + \text{rem}(a, b) \geq b + \text{rem}(a, b) \geq F_{n+2} + F_{n+1} = F_{n+3}.$$

So we have $P(n + 1)$.

By the Principle of Mathematical Induction, we conclude that $P(n)$ holds for all $n \in \mathbb{N}$. □

3.6.2 Extended Euclidean Algorithm

Theorem 3.6.2. (**Bezout Identity**) For all $m, n \in \mathbb{Z}^+$, there exists integers $x, y \in \mathbb{Z}$ such that

$$x \cdot m + y \cdot n = \gcd(m, n).$$

Proof. Let $m, n \in \mathbb{Z}^+$ be arbitrary positive integers. Let us consider the Euclidean algorithm in action:

$$\begin{aligned} m &= q_1 n + r_1 \\ n &= q_2 r_1 + r_2 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

We wish to show that for all $i \in [1, k]$

$$\exists x_i, y_i \in \mathbb{Z}. x_i m + y_i n = r_i.$$

We proceed by strong induction on i.

Proof.
Base Case. When $i = 1$, we introduce the witnesses $x_1 = 1$ and $y_1 = -q_1$. So we have $x_1 m + y_1 n = r_1$. So we have $P(1)$.

When $i = 2$, we introduce the witnesses $x_2 = -q_2$ and $y_2 = 1 + q_1 \cdot q_2$. We note that

$$\begin{aligned} r_2 &= n - q_2 r_1 \\ &= n - q_2 (m - q_1 n) \\ &= (-q_2) m + (1 + q_1 q_2) n \end{aligned}$$

So we have $P(2)$.
Inductive Step. We wish to show that

$$\forall i \in [2, k-1]. (\forall \ell \in [1, i]. P(\ell)) \implies P(i+1).$$

Let $i \in [2, k-1]$ be arbitrary. Let us assume that $\forall \ell \in [1, i]. P(\ell)$ holds. We note that

$$r_{i-1} = q_{i+1} r_i + r_{i+1}.$$

So we have

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i+1} r_i \\ &= (x_{i-1} m + y_{i-1} n) - q_{i+1} (x_i m + y_i n) \\ &= (x_{i-1} - q_{i+1} x_i) m + (y_{i-1} - q_{i+1} y_i) n \end{aligned}$$

So let us introduce the witnesses

$$\begin{aligned} x_{i+1} &= x_{i-1} - q_{i+1} x_i \\ y_{i+1} &= y_{i-1} - q_{i+1} y_i \end{aligned}$$

From the above, it follows that we have $P(i+1)$.

By the Principle of Strong Induction, we conclude that $P(i)$ holds for all $i \in [1, k]$. □

□

The **Extended Euclidean Algorithm** calculates the integers $x, y \in \mathbb{Z}$ whose existence is postulated by the Bezout Identity and the gcd of m and n. We have the following recursive implementation in OCaml

```
let egcd m n =
    let rec inner ((x1, y1), r1) ((x1, y2), r2) =
        (*r_{i + 1} = r_{i - 1} - q_{i + 1} r_i*)
        let (q, r) = divalg r1 r2
        in
            if r = 0 then ((x1, y2), r2)
            else inner ((x1, y2), r2) ((x1 - q * x2, y1 - q * y2), r)
    in inner ((1, 0), m) ((0, 1), n)
```

So we now have

```
let gcd = snd <.> egcd
let x = fst <.> (fst <.> egcd)
let y = snd <.> (fst <.> egcd)
```

We define

$$\begin{aligned} lc_1(m, n) &= x \\ lc_2(m, n) &= y \end{aligned}$$

Hence

$$lc_1(m, n) \cdot m + lc_2(m, n) \cdot n = \gcd(m, n).$$

3.6.3 Other Theorems

Lemma 3.6.3. For all positive integers $l, m, n \in \mathbb{Z}^+$,

(i) **Commutativity**. $\gcd(m, n) = \gcd(n, m)$

(ii) **Associativity**. $\gcd(l, \gcd(m, n)) = \gcd(\gcd(l, m), n)$

(iii) **Distributivity**. $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n)$

Proof. Let $l, m, n \in \mathbb{Z}^+$ be arbitrary positive integers.

(i) is trivial.

(ii) Let $d = \gcd(l, \gcd(m, n))$, by definition, we note that $\forall c.c \mid l \wedge c \mid \gcd(m, n) \iff c \mid d$ We wish to show that $d = \gcd(\gcd(l, m), n)$, that is to say $\forall c.c \mid \gcd(l, m) \wedge c \mid n \iff c \mid d$. We note that

$$\forall c \in \mathbb{Z}^+.c \mid m \wedge c \mid n \iff c \mid \gcd(m, n).$$

Hence we have for,

$$\begin{aligned} \forall c.c \mid l \wedge c \mid \gcd(m, n) &\iff c \mid l \wedge (c \mid m \wedge c \mid n) \\ &\iff \forall c.\, (c \mid l \wedge c \mid m) \wedge c \mid n \\ &\iff \forall c.c \mid \gcd(l, m) \wedge c \mid n \end{aligned}$$

So we are done.

(iii) Let $d = \gcd(m, n)$, we note that

$$(d \mid m \wedge c \mid n) \implies [(l \cdot d) \mid (l \cdot m) \wedge (l \cdot d) \mid (l \cdot n)]$$

Hence $(l \cdot d) \mid \gcd(l \cdot m, l \cdot n)$, that is to say there exists an integer $x \in \mathbb{Z}$ such that $\gcd(l \cdot m, l \cdot n) = x \cdot l \cdot d$. Introducing a witness $x_0 \in \mathbb{Z}$ such that the above holds true gives us $\gcd(l \cdot m, l \cdot n) = x_0 \cdot l \cdot d$. So

$$((x_0 \cdot l \cdot d) \mid (l \cdot m) \wedge (x_0 \cdot l \cdot d) \mid (l \cdot n)) \implies ((x_0 \cdot d) \mid m \wedge (x_0 \cdot d) \mid n)\,.$$

Hence $(x_0 \cdot d) \mid d$, yielding $x_0 = 1$. So we have $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n)$.

□

Theorem 3.6.3. (**Euclid's Theorem**) For all $k, m, n \in \mathbb{Z}^+$,

$$k \mid (m \cdot n) \wedge \gcd(k, m) = 1 \implies k \mid n.$$

Let $k, m, n \in \mathbb{Z}^+$ be arbitrary positive integers. Let us assume that $k \mid (m \cdot n)$, that is to say

$$\exists x \in \mathbb{Z}. m \cdot n = x \cdot k.$$

Introducing a witness $x_0 \in \mathbb{Z}$ such that the above holds gives us $m \cdot n = x_0 \cdot k$. Let us also assume that $\gcd(k, m) = 1$. By the distributivity of gcd, we have

$$\begin{aligned} n &= \gcd(n \cdot k, n \cdot m) \\ &= \gcd(n \cdot k, x_0 \cdot k) \\ &= k \cdot \gcd(n, x_0) \end{aligned}$$

Hence $k \mid n$.

Corollary 3.6.3.1. For all $m, n \in \mathbb{Z}^+$ and prime $p \in \mathbb{P}$,

$$p \mid (m \cdot n) \implies p \mid m \vee p \mid n.$$

Let $m, n \in \mathbb{Z}^+$ be arbitrary positive integers and prime $p \in \mathbb{P}$ be arbitrary. Let us assume that $p \mid (m \cdot n)$. We have two cases:

- **Case** $p \mid m$. Let us assume that $p \mid m$. So we are done.
- **Case** $p \nmid m$. Let us assume that $p \nmid m$, since p is prime, we have $\gcd(p, m) = 1$. By Euclid's Theorem, we have $p \mid n$. So we are done.

3.7 Primes

Definition 3.7.1. (**Prime Number**) A prime number $p \in \mathbb{Z}^+$ is a positive integer, $p \geq 2$, such that

$$\forall x \in \mathbb{Z}^+. x \mid p \implies x = 1 \vee x = p.$$

- We denote the set of primes by $\mathbb{P}$.

Theorem 3.7.1. (**Fundamental Theorem of Arithmetic**) For all positive integers n, $n \geq 2$, there exists a unique finite sequence of primes and exponents $\langle (p_1, n_1), \ldots, (p_k, n_k) \rangle \subset \mathbb{P} \times \mathbb{Z}^+$ where $p_1 < \cdots < p_k$ such that

$$n = \prod_{i=1}^{k} p_i^{n_i}.$$

Proof.
Existence.
We proceed by strong induction on n with the statement

$$P(n) = \exists \langle (p_1, n_1), \ldots, (p_k, n_k) \rangle \subset \mathbb{P} \times \mathbb{Z}^+ . p_1 < \cdots < p_k . n = \prod_{i=1}^{k} p_i^{n_i},$$

from a basis of $n = 2$.

Proof.
Base Case. For $n = 2$, we introduce the witness $\langle (p_1, n_1) \rangle = \langle (2, 1) \rangle$. So we have

$$2 = \prod_{i=1}^{1} p_i^{n_i} = 2^1.$$

So $P(2)$ holds.
Inductive Step. We wish to show that

$$\forall n \geq 2 \in \mathbb{Z}^+ . \left((\forall k \in [2, n] . P(k)) \implies P(n+1) \right).$$

Let $n \geq 2 \in \mathbb{Z}^+$ be an arbitrary integer. Let us assume that $\forall k \in [2, n] . P(k)$ holds, that is to say for all $k \in [2, n]$, there exists the finite sequence $\langle (p_1, n_1), \ldots, (p_\ell, n_\ell) \rangle \subset \mathbb{P} \times \mathbb{Z}^+$ where $p_1 < \cdots < p_\ell$ such that

$$k = \prod_{i=1}^{\ell} p_i^{n_i}.$$

Let us consider $n + 1$, we have two cases:

- **Case** $n+1$ is prime. Let us assume that $n+1$ is prime. Let us introduce the witness $\langle (p_1, 1) \rangle = \langle (n+1, 1) \rangle$. So we have

  $$n + 1 = \prod_{i=1}^{1} p_i^{n_i} = (n+1)^1.$$

  So we have $P(n+1)$.

- **Case** $n+1$ is composite. Let us assume that $n+1$ is composite. That is to say
$$\exists a, b \in [2, n+1).n+1 = a \cdot b.$$
Let us introduce the witness $a_0, b_0 \in [2, n+1)$ such that the above holds. By our inductive hypothesis it follows that there exists the finite sequences such that
$$\begin{aligned} a_0 &= \prod_{i=1}^{\ell} p_i^{n_i} \\ b_0 &= \prod_{i=1}^{\ell'} (p_i')^{n_i'} \\ p_1 &< \cdots < p_\ell \\ p_1' &< \cdots < p_{\ell'}' \end{aligned}$$
We have
$$n+1 = \prod_{i=1}^{\ell} p_i^{n_i} \cdot \prod_{i=1}^{\ell'} (p_i')^{n_i'} = (p_1'')^{n_1''}(p_2'')^{n_2''} \cdots (p_k'')^{n_k''},$$
with the sequence $\langle (p_1'', n_1''), \ldots, (p_k'', n_k'') \rangle$ with $p_1'' < \cdots < p_k''$. So we have $P(n+1)$.

By the Principle of String Induction, we conclude that $P(n)$ holds for all $n \geq 2 \in \mathbb{Z}^+$. □

Uniqueness.
We proceed by induction on k with the statement
$$\begin{aligned} P(k) = \forall \ell \in \mathbb{Z}^+ . \forall \langle (p_1, a_1), \ldots, (p_k, a_k) \rangle , \langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle \subset \mathbb{P} \times \mathbb{Z}^+ \\ . p_1 < \cdots < p_k \wedge q_1 < \cdots < q_\ell \\ . \prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{\ell} q_i^{b_i} \implies \langle (p_1, a_1), \ldots, (p_k, a_k) \rangle = \langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle \end{aligned}$$
from a basis of $k = 1$.

Proof.
Base Case. For $k = 1$. Let $\ell \in \mathbb{Z}^+$ be an arbitrary positive integer. Let

$\langle (p_1, a_1) \rangle$ and $\langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle$ be our finite sequences of primes where $q_1 < \cdots < q_\ell$. Let us assume that

$$\prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{\ell} q_i^{b_i}.$$

So we have

$$\prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{\ell} q_i^{b_i}$$
$$\iff p_1^{a_1} = q_1^{b_1} \cdots q_\ell^{b_\ell}$$

Since p_1 and q_i are prime and $q_1 < \cdots < q_\ell$, it follows that $k = \ell = 1$. Hence $\langle (p_1, a_1) \rangle = \langle (q_1, b_1) \rangle$.

Inductive Step. We wish to show that

$$\forall k \in \mathbb{Z}^+ . P(k) \implies P(k+1).$$

Let $k \in \mathbb{Z}^+$ be an arbitrary positive integer. Let us assume that $P(k)$ holds, that is to say

$$\forall \ell \in \mathbb{Z}^+ . \forall \langle (p_1, a_1), \ldots, (p_k, a_k) \rangle, \langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle \subset \mathbb{P} \times \mathbb{Z}^+$$
$$. p_1 < \cdots < p_k \wedge q_1 < \cdots < q_\ell$$
$$. \prod_{i=1}^{k} p_i^{a_i} = \prod_{i=1}^{\ell} q_i^{b_i} \implies \langle (p_1, a_1), \ldots, (p_k, a_k) \rangle = \langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle$$

We wish to show that $P(k+1)$ holds. Let $\ell \in \mathbb{Z}^+$ be arbitrary. Let $\langle (p_1, a_1), \ldots, (p_1, a_{k+1}) \rangle$ and $\langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle$ be two arbitrary sequences of primes and exponents such that $p_1 < \cdots < p_{k+1}$ and $q_1 < \cdots < q_\ell$. Let us assume that

$$\prod_{i=1}^{k+1} p_i^{a_i} = \prod_{i=1}^{\ell} q_i^{b_i}.$$

We note that $p_1^{a_1} \mid \prod_{i=1}^{k+1} p_i^{a_i}$, hence $p_1^{a_1} \mid \prod_{i=1}^{\ell} q_i^{b_i}$, hence there exists q_i such that $p_1^{a_1} \mid q_i^{b_i}$. Analogously, we have $\exists p_i . q_1^{b_1} \mid p_i^{a_i}$. Since p_i and q_i are prime, it follows that $p_1 = q_i \geq q_1$, $q_1 = p_i \geq p_1$, $a_1 = b_i$ and $b_1 = a_i$. We also note that $p_1 = q_i \geq q_1$ and $q_1 = p_i \geq p_1$. Hence $p_1 = q_1$ and $a_1 = b_1$. Hence

$$\prod_{i=2}^{k+1} p_i^{a_i} = \prod_{i=2}^{\ell} q_i^{b_i}.$$

We note that $\ell \geq 1$ since the product of 2 or more primes $p_1^{a_1}, \ldots, p_{k+1}^{a_{k+1}}$ is not prime. So $\ell - 1 \in \mathbb{Z}^+$. Since we have the sequences of primes $\underbrace{\langle (p_2, a_2), \ldots, (p_{k+1}, a_{k+1}) \rangle}_{\text{length } k}$ and $\langle (q_2, b_2), \ldots, (q_\ell, b_\ell) \rangle$ where $p_2 < \cdots < p_{k+1}$ and $q_2 < \cdots < q_\ell$ with

$$\prod_{i=2}^{k+1} p_i^{a_i} = \prod_{i=2}^{\ell} q_i^{b_i}.$$

So by our inductive hypothesis, we conclude that

$$\langle (p_2, a_2), \ldots, (p_{k+1}, q_{k+1}) \rangle = \langle (q_2, b_2), \ldots, (q_\ell, b_\ell) \rangle .$$

Hence

$$\langle (p_1, a_1), \ldots, (p_1, a_{k+1}) \rangle = \langle (q_1, b_1), \ldots, (q_\ell, b_\ell) \rangle .$$

So we have $P(k+1)$.

By the Principle of Induction, we conclude that $P(k)$ holds for all $k \in \mathbb{Z}^+$. □

So we are done. □

Theorem 3.7.2. (**Euclid's Infinitude of Primes**) The set of primes $\mathbb{P}$ is infinite.

Proof. We proceed by contradiction. Let us assume the set of primes $\mathbb{P}$ is finite, that is

$$\mathbb{P} = \{p_1, \ldots, p_k\},$$

where $k \in \mathbb{N}$. Let us consider

$$p = 1 + \prod_{p_i \in \mathbb{P}} p_i.$$

Since $p \notin \mathbb{P}$, then it follows that by the Fundamental Theorem of Arithmetic, it may be expressed as a unique product of primes. Hence there exists $p_i \in \mathbb{P}$ such that $p_i \mid p$. We note that $p_i \mid (p_1 \cdots p_k)$, so it follows that $p_i \mid p - (p_1 \cdots p_k) = 1$. A contradiction! Hence $\mathbb{P}$ is infinite. □

3.7.1 Other Theorems

Lemma 3.7.1. For all prime $p \in \mathbb{P}$ and $m \in [0, p]$,

$$\binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p}.$$

Proof. Let $p \in \mathbb{P}$ be an arbitrary prime and $m \in [0, p]$ be an arbitrary integer. We have the following cases:

- **Case** $m = 0$. Let us assume that $m = 0$, hence

  $$\binom{p}{0} = 1 \equiv 1 \pmod{p}.$$

  So we are done.

- **Case** $0 < m < p$. Let us assume that $0 < m < p$. We note that

  $$\binom{p}{m} = \frac{p!}{(p-m)!m!} = \frac{p(p-1)!}{(p-m)!m!},$$

  is an integer, so it follows that $(p-m)!m! \mid p(p-1)!$. For simplicity, let $k = (p-m)!m!$. We note that $\gcd(k, p) = 1$ since p is prime. By Euclid's theorem, it follows that $k \mid (p-1)!$. Hence

  $$\frac{(p-1)!}{(p-m)!m!},$$

  is an integer. So we have

  $$p \mid \binom{p}{m}.$$

  By definition of modulo p, we have

  $$\binom{p}{m} \equiv 0 \pmod{p}.$$

- **Case** $m = p$. Let us assume that $m = p$, hence

  $$\binom{p}{0} = 1 \equiv 1 \pmod{p}.$$

  So we are done.

□

Theorem 3.7.3. (**The Freshman's Dream**) For all natural $m, n \in \mathbb{N}$ and prime $p \in \mathbb{P}$,

$$(m+n)^p \equiv m^p + n^p \pmod{p}.$$

Proof. Let $m, n \in \mathbb{N}$ be arbitrary natural numbers. Let prime $p \in \mathbb{P}$ be arbitrary. We wish to show that $(m+n)^p \equiv m^p + n^p \pmod{p}$, by the definition of modulo p, that is

$$p \mid (m+n)^p - (m^p + n^p).$$

Recall that the Binomial Theorem states that

$$\forall x, y \in \mathbb{Z}, n \in \mathbb{Z}^+.(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} (x)^{n-r}(y)^r.$$

Instantiating for $x = m, y = n$ and $n = p$ yields

$$\begin{aligned}(m+n)^p &= \sum_{r=0}^{p} \binom{p}{r} (m)^{p-r}(n)^r \\ &= m^p + \sum_{r=1}^{p-1} \binom{p}{r} (m)^{p-r}(n)^r + n^p\end{aligned}$$

Note that $p \mid \binom{p}{r}$ for $1 \leq r \leq p-1$, so it follows that

$$p \mid \sum_{r=1}^{p-1} \binom{p}{r} (m)^{p-r}(n)^r,$$

hence $p \mid (m+n)^p - (m^p + n^p)$. So we are done. □

Theorem 3.7.4. (**Fermat's Little Theorem**) For all $i \in \mathbb{N}$ and prime $p \in \mathbb{P}$,

$$i^p \equiv i \pmod{p}.$$

Proof. Let prime $p \in \mathbb{P}$ be arbitrary. We proceed by induction on i with the statement

$$P(i) = i^p \equiv i \pmod{p}.$$

Base Case. For $i = 0$, we have

$$0^p \equiv 0 \pmod{p}.$$

So we have $P(0)$.
Inductive Step. We wish to show that

$$\forall i \in \mathbb{N}.P(i) \implies P(i+1).$$

Let $i \in \mathbb{N}$ be arbitrary. Let us assume that $P(i)$ holds, that is to say

$$i^p \equiv i \pmod{p}.$$

Let us consider $i + 1$. So we have

$$\begin{aligned}(i+1)^p &= \sum_{r=0}^{p} \binom{p}{r} (i)^{p-r} \\ &= i^p + \sum_{r=1}^{p-1} \binom{p}{r} (i)^{p-r} + 1 \\ &= i^p + 1 \pmod{p} \\ &= i + 1 \pmod{p}\end{aligned}$$

So we have $P(i+1)$.

By the Principle of Mathematical Induction, we conclude that $P(i)$ holds for all $i \in \mathbb{N}$. □

Corollary 3.7.4.1. For all $i \in \mathbb{N}$, $i \nmid p$ and prime $p \in \mathbb{P}$,

$$i^{p-1} \equiv 1 \pmod{p}.$$

Proof. Let $i \in \mathbb{N}.i \nmid p$ and prime $p \in \mathbb{P}$ be arbitrary. Instantiating Fermat's Little Theorem yields

$$i^p \equiv i \pmod{p}.$$

By the cancellability of congruences and since $\gcd(i, p) = 1$, we have

$$i^{p-1} \equiv 1 \pmod{p}.$$

So we are done. □

4 Formal Languages

4.1 Symbols, Strings, Alphabets and (Formal) Languages

Definition 4.1.1. (**Alphabet**) An alphabet is a finite set Σ, whose elements are referred to as symbols.

Definition 4.1.2. (**String**) A string s of length $n \geq 0$ over the alphabet Σ is an ordered n-tuple $(s_1, \ldots, s_n)$ where $s_k \in \Sigma$.

- $$\Sigma^* = \text{set of all finite strings over } \Sigma.$$
- We often abbreviate the string $(s_1, \ldots, s_n)$ as $s_1 s_2 \ldots s_n$.
- The empty string (or null string) () over the alphabet Σ is denoted ε.
- The length of a string $s \in \Sigma^*$ is denoted as $|s|$.

Definition 4.1.3. (**Concatenation**) The concatenation of two strings $u = u_1 \ldots u_m$ and $v = v_1 \ldots v_n$ over Σ is the string $uv = u_1 \ldots u_m v_1 \ldots v_n$ over Σ, that satisfies the following axioms

(C1) **Identity**.

$$\forall u \in \Sigma^*. u\varepsilon = \varepsilon u = u.$$

(C2) **Associativity**.

$$\forall u, v, w \in \Sigma^*. (uv)w = u(vw) = uvw.$$

- We may inductively define Σ^* as

$$\textbf{Axioms}: \quad \frac{}{\varepsilon} \qquad\qquad \frac{}{a}[a \in \Sigma]$$

$$\textbf{Rules}: \quad \frac{a \quad b}{ab}$$

Theorem 4.1.1. The length of the string uv over Σ is

$$|uv| = |u| + |v|.$$

Proof. Induction on $|u|$. □

- The string u^n where $n \in \mathbb{N}$ and $u \in \Sigma^*$ is inductively defined as

$$u^0 = \varepsilon$$
$$\forall n \in \mathbb{N}. u^n = uu^{n-1}$$

Definition 4.1.4. (**Formal Language**) We say the set L is a formal language over Σ if and only if $L \subseteq \Sigma^*$.

- The empty language consisting of no strings is $\emptyset$.

Theorem 4.1.2. The set of languages over the alphabet Σ is non-enumerable.

Proof. Cantor's diagonalisation argument. □

- Concatenation of the language L_1 and L_2 is defined as

$$L_1 L_2 = \{s_1 s_2 : s_1 \in L_1 \wedge s_2 \in L_2\}.$$

  and satisfies Identity and Associativity axioms with the identity element $\emptyset$.

- The $n \in \mathbb{N}$ concatenation of the language L is

$$L^n = \{s_1 \cdots s_n : s_1, \ldots, s_n \in L\},$$

  where $L^0 = \{\varepsilon\}$.

- The concatenation closure or Kleenean star of the language L is

$$L^* = \bigcup_{n \in \mathbb{N}} L^n.$$

4.2 Inductively Defined Sets

- A set S is inductively defined by a set of rules instances $\mathcal{R}$, consisting of instances of
  - **Axioms**. denoted
    $$\mathcal{D} = \frac{}{a}$$
    where $\mathcal{D}$ is said to be a derivation for the conclusion a, denoted $\mathcal{D} :: a \in S$
  - **Rules**. denoted
    $$\mathcal{D} = \frac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ x_1 & x_2 & \cdots & x_n\end{array}}{y}$$
    where $D_k :: x_k \in S$ are the derivations for the hypotheses (or premises) and $\mathcal{D} :: y \in S$.
- The set of rule instances is $\mathcal{R} \subseteq \mathcal{P}(S) \times S$ where $(X, y) \in \mathcal{R}$ and X is the set of premises and y is the conclusion. Axioms are of the form $(\emptyset, y)$.

Definition 4.2.1. ($\mathcal{R}$**-Closed**) A set S is closed ($\mathcal{R}$-closed) under the rule instances $\mathcal{R}$ if and only if

$$\forall (X, y) \in \mathcal{R}. X \subseteq S \implies y \in Q.$$

Theorem 4.2.1. For all rule instances $\mathcal{R}$,

(i) $I_{\mathcal{R}}$ is $\mathcal{R}$-closed and

(ii) for all S,
$$S \text{ is } \mathcal{R}\text{-closed} \implies I_{\mathcal{R}} \subseteq S.$$

Proof. We define $I_{\mathcal{R}}$ as

$$I_{\mathcal{R}} = \bigcap \{S : S \text{ is } \mathcal{R}\text{-closed}\},$$

the least set closed under $\mathcal{R}$. We will to show that (i) holds. Let $(X, y) \in \mathcal{R}$ be arbitrary. Let us assume that $X \subseteq I_{\mathcal{R}}$. Let S be some arbitrary $\mathcal{R}$-closed set. Hence by the transitivity of $\subseteq$, we have $X \subseteq S$. Hence $y \in S$. Since S is arbitrary, by the definable property of $\bigcap$, we have $y \in I_{\mathcal{R}}$.

(ii) follows trivially from the definable property of $I_{\mathcal{R}}$. □

- $I_{\mathcal{R}}$ is said to be the set inductively defined by $\mathcal{R}$.

4.3 Rule Induction

- We wish to show $\forall x \in I_{\mathcal{R}}.P(x)$. We define

$$S = \{x \in I_{\mathcal{R}} : P(x)\}.$$

By anti-symmetry of $\subseteq$, $\forall x \in I_{\mathcal{R}}.P(x) \iff I_{\mathcal{R}} \subseteq S$. So it suffices to show that S is $\mathcal{R}$-closed. That is

$$\begin{aligned} &\forall (X, y) \in \mathcal{R}.(\forall x \in X.x \in I_{\mathcal{R}} \wedge P(x)) \implies (y \in I_{\mathcal{R}} \wedge P(y)) \\ \iff &\forall (X, y) \in \mathcal{R}.(\forall x \in X.x \in I_{\mathcal{R}} \wedge P(x)) \implies P(y) \end{aligned}$$

since $I_{\mathcal{R}}$ is $\mathcal{R}$-closed.

Definition 4.3.1. (**The Principle of Rule Induction**) Let $I_{\mathcal{R}}$ be inductively-defined by $\mathcal{R}$. The $\forall x \in I_{\mathcal{R}}.P(x)$ holds if

$$\forall (X, y) \in \mathcal{R}.(\forall x \in X.x \in I_{\mathcal{R}} \wedge P(x)) \implies P(y).$$

5 Regular Languages

5.1 Regular Expressions and Languages

- The set regular expressions $\mathcal{R}_\Sigma \subseteq (\Sigma \cup \Sigma')^*$ (or $\mathcal{R}$) over an alphabet Σ where $\Sigma' = \{\varnothing, \epsilon, *, |, (,)\}$ is inductively defined by

  Axioms : $\dfrac{}{a}[a \in \Sigma]$ $\qquad \dfrac{}{\epsilon}$ $\qquad \dfrac{}{\varnothing}$

  Rules : $\dfrac{r}{(r)}$ $\qquad \dfrac{r \quad s}{r \mid s}$ $\qquad \dfrac{r \quad s}{rs}$ $\qquad \dfrac{r}{r^*}$

  where $r, s \in (\Sigma \cup \Sigma')^*$

- The algebraic data type definition of a regular expression is

```
type 'a regex = Symbol of 'a
              | Epsilon
              | Empty
              | Star of 'a regex
              | Concat of 'a regex * 'a regex
              | Union of 'a regex * 'a regex
```

  This is the "abstract syntax" (tree) representation of a regular expression as opposed to the "concrete syntax" defined in $\mathcal{R}_\Sigma$

- The regular language defined by the regular expression r over Σ is

$$L(r) = \{u \in \Sigma^* : u \text{ matches } r\}.$$

- Let $\mathcal{L}_\Sigma$ (or $\mathcal{L}$), denotes the set of regular languages over the alphabet Σ that is

$$\mathcal{L}_\Sigma = \{L(r) : r \in \mathcal{R}_\Sigma\}.$$

- $\mathcal{L}_\Sigma$ satisfies
  - The language $\emptyset \in \mathcal{L}$ and $\emptyset = L(\varnothing)$
  - The language $\{\varepsilon\} \in \mathcal{L}_\Sigma$ and $\{\varepsilon\} = L(\epsilon)$
  - For all $a \in \Sigma$, $\{a\} \in \mathcal{L}_\Sigma$ and $\{a\} = L(a)$
  - $L_1, L_2 \in \mathcal{L}_\Sigma$ and $L_1 = L(r_1)$, $L_2 = L(r_2)$, then
    - $L_1 \cup L_2 \in \mathcal{L}_\Sigma$ and $L_1 \cup L_2 = L(r_1 \mid r_2)$
    - $L_1 L_2 \in \mathcal{L}_\Sigma$ and $L_1 L_2 = L(r_1 r_2)$
  - $L \in \mathcal{L}_\Sigma$ and $L = L(r)$, then $L^* \in \mathcal{L}_\Sigma$ and $L^* = L(r^*)$
- Order of precedence: $*$, concatenation, $|$. Hence $a|b^*c = ((a) \mid ((b^*)c))$
- From properties above, for all $L \in \mathcal{L}_\Sigma$. $L^* \in \mathcal{L}_\Sigma$ and $L^n \in \mathcal{L}_\Sigma$
- The strings $u \in L(r)$ are said to match r, that is:
  - u matches $a \iff u = a$
  - u matches ϵ if u is ε.
  - no strings match $\varnothing$.
  - u matches $r \mid s \iff u$ matches $r \vee u$ matches s
  - u matches $rs \iff \exists u, v \in \Sigma^*.u = vw \wedge v$ matches $r \wedge w$ matches s.
  - u matches r^* iff $\exists v \in \Sigma^*.u = v^n$ where $n \in \mathbb{N}$.
- The matching equivalence relation $\sim$: $\Sigma^* \nrightarrow \mathcal{R}_\Sigma$ is inductively defined as

Axioms : $\dfrac{}{(a,a)}[a \in \Sigma]$ $\qquad \dfrac{}{(\varepsilon, \epsilon)}$ $\qquad \dfrac{}{(\varepsilon, r^*)}$

Rules : $\dfrac{(u,r)}{(u, r \mid s)}$ $\qquad \dfrac{(u,s)}{(u, r \mid s)}$ $\qquad \dfrac{(v,r) \qquad (w,s)}{(uw, rs)}$ $\qquad \dfrac{(u,r) \qquad (v,r^*)}{(uv, r^*)}$

5.2 Finite Automata

5.2.1 NFAs, DFAs and NFA$^\varepsilon$

Definition 5.2.1. (**Non-deterministic finite automaton**) A non-deterministic finite automaton (NFA) is A 5-tuple $M = (Q, \Sigma, q_0, \Delta, A)$ where

(i) $Q = \{q_0, \ldots, q_n\}$ a finite set of states.

(ii) Σ is the finite alphabet of accepted input symbols.

(iii) $\Delta : Q \times \Sigma \to \mathcal{P}(Q)$ the transition function.

(iv) $q_0 \in Q$ is the unique start (initial) state.

(v) $A \subseteq Q$ is the set of accepting states.

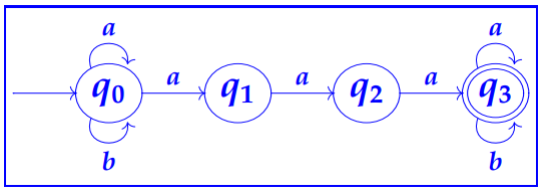


Figure 5.1: NFA over $\Sigma = \{a, b\}$

- $q \xrightarrow{a} q' \iff q' \in \Delta(q, a)$.
- $q_0 \xrightarrow{u}{}^{*} q'$ to denote the transition path
$$q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} \cdots \xrightarrow{u_n} q',$$
where $u = u_1 \ldots u_n$. Note that $q \xrightarrow{\varepsilon}{}^{*} q' \iff q = q'$.
- We may define a transition function $\Delta^* : Q \times \Sigma^* \to \mathcal{P}(Q)$ over Σ^* as
$$\Delta^*(q, \varepsilon) = \{q\}$$
$$\Delta^*(q, ua) = \bigcup_{q' \in \Delta^*(q,u)} \Delta(q', a)$$
equivalently,
$$\Delta^*(q, u) = \left\{q' \in Q : q \xrightarrow{u}{}^{*} q'\right\}.$$
- The language accepted by the finite automaton M is $L(M)$,
$$L(M) = \left\{u \in \Sigma^* : q_0 \xrightarrow{u}{}^{*} q' \in A\right\} = \{u \in \Sigma^* : \Delta^*(q_0, u) \cap A \neq \emptyset\}.$$

Definition 5.2.2. (**Deterministic finite automaton**) A deterministic finite automaton (DFA) is a NFA $M = (Q, \Sigma, \Delta, q_0, A)$, with the property
$$\forall q \in Q, a \in \Sigma. \exists! q'. q \xrightarrow{a} q'.$$

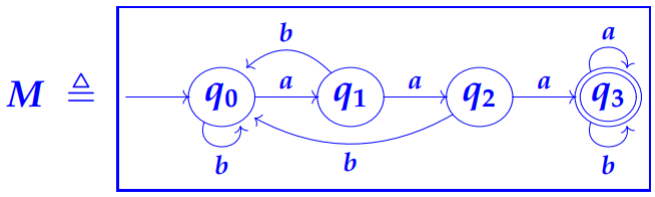


Figure 5.2: DFA over $\Sigma = \{a, b\}$

- To check whether an NFA is a DFA:
  - Ensure all transition sets $\Delta(q, a)$ consist of singletons.
- Since $\Delta Q \times \Sigma \to \mathcal{P}(Q)$ returns singletons, we redefine $\Delta : Q \times \Sigma \to Q$. For simplicity, we write this as δ (to avoid confusion). EXAMPLE
- We define the transition function $\delta^* : Q \times \Sigma^* \to Q$ over Σ^* recursively as

$$\begin{aligned} \delta^*(q, \varepsilon) &= q \\ \delta^*(q, ua) &= \delta(\delta^*(q, u), a) \end{aligned}$$

  equivalently,

$$\delta^*(q, u) = q' \iff q \overset{u}{\to}{}^* q'.$$

- The language accepted by a DFA is

$$L(M) = \left\{ u \in \Sigma^* : q_0 \overset{u}{\to}{}^* q' \in A \right\} = \{ u \in \Sigma^* : \delta^*(q_0, u) \in A \}.$$

Definition 5.2.3. (**NFA with ε-transitions**) A NFA with ε-transitions (NFA$^\varepsilon$) is the 6-tuple $M = (Q, \Sigma, \Delta_\varepsilon, q_0, A)$ where $(Q, \Sigma, \Delta_\varepsilon, q_0, A)$ is a NFA with a modified transition relation, such that

$$\Delta_\varepsilon : Q \times (\Sigma \cup \{\varepsilon\}) \to \mathcal{P}(Q).$$

- ε-transitions are denoted $q \overset{\varepsilon}{\to} q' \iff q' \in \Delta_\varepsilon(q, \varepsilon)$.
- $q \overset{\varepsilon}{\Longrightarrow} q'$ if $q = q'$ or there is a sequence of one or more ε-transitions

$$q \overset{\varepsilon}{\to} \cdots \overset{\varepsilon}{\to} q'.$$

The ε-closure is defined as

$$\mathcal{E}(q) = \left\{ q' \in Q : q \overset{\varepsilon}{\Longrightarrow} q' \right\}.$$

That is the set of states reachable by zero or more ε-transitions. Note that $q \in \mathcal{E}(q)$

- $q \overset{a}{\Longrightarrow} q'$ consisting of the state transition sequence

$$q \overset{\varepsilon}{\Longrightarrow} \cdot \overset{a}{\to} \cdot \overset{\varepsilon}{\Longrightarrow} q'.$$

- The language accepted by the NFA$^\varepsilon$ is

$$L(M) = \left\{ u \in \Sigma^* : q \overset{u}{\Longrightarrow} q' \in A \right\}.$$

- The transition function $\Delta^*_\varepsilon : Q \times \Sigma^* \to \mathcal{P}(Q)$ over Σ^* is defined as

$$\begin{aligned} \Delta^*_\varepsilon(q, \varepsilon) &= \mathcal{E}(q) \\ \Delta^*_\varepsilon(q, ua) &= \bigcup_{q' \in \Delta^*_\varepsilon(q,u)} \left\{ q'' \in Q : q' \overset{a}{\Longrightarrow} q'' \right\} \end{aligned}$$

- The set $\left\{ (q, u, q') \in Q \times \Sigma^* \times Q : q \overset{u}{\Longrightarrow} q' \right\}$ is inductively defined as

$$\textbf{Axioms}: \quad \frac{}{(q, \varepsilon, q)}[q \in Q]$$

$$\textbf{Rules}: \quad \frac{(q, u, q')}{(q, u, q'')}[q' \overset{\varepsilon}{\to} q''] \qquad \frac{(q, u, q')}{(q, ua, q')}[q' \overset{a}{\to} q'']$$

5.2.2 Subset Construction

- All DFAs are NFAs, All NFAs are NFA$^\varepsilon$. We now show that all NFA$^\varepsilon$ have an equivalent DFA.

Theorem 5.2.1. For all NFA$^\varepsilon$ $M = (Q, \Sigma, \Delta_\varepsilon, q_0, A)$, there is a DFA $PM = (\mathcal{P}(Q), \Sigma, \delta, q'_0, A')$ such that $L(M) = L(PM)$ where

(i) $\mathcal{P}(Q) = \{S : S \subseteq Q\}$

(ii) The transition function $\delta : \mathcal{P}(Q) \times \Sigma \to \mathcal{P}(Q)$

$$\delta(S, a) = \bigcup_{q \in S} \left\{ q' \in Q : q \overset{a}{\Longrightarrow} q' \right\}.$$

(iii) The initial state is

$$q_0' = \left\{ q \in Q : q_0 \overset{\varepsilon}{\Longrightarrow} q \right\}.$$

(iv) The accepting states are

$$A' = \{ S \in \mathcal{P}(Q) : S \cap A \neq \emptyset \}.$$

Proof. We wish to show that $L(M) = L(PM)$. It is sufficient to show that $\forall u \in \Sigma^*.\Delta_\varepsilon^*(q_0, u) = \delta^*(q_0', u)$. We proceed by rule induction over Σ^*, we define our statement $P(u)$ as

$$P(u) = (\Delta_\varepsilon^*(q_0, u) = \delta^*(q_0', u)).$$

Base Case. For our axiom

$$\frac{}{\varepsilon}.$$

We have

$$\begin{aligned} \Delta_\varepsilon^*(q_0.\varepsilon) &= \mathcal{E}(q_0) \\ &= \left\{ q \in Q : q_0 \overset{\varepsilon}{\Longrightarrow} q \right\} \\ &= q_0' \\ &= \delta^*(q_0', \varepsilon) \end{aligned}$$

So the statement $P(\varepsilon)$ holds.
Inductive Step. We wish to show that $\forall (X, y) \in \mathcal{R}.(\forall x \in X.P(x)) \implies P(y)$ holds. For the rule

$$\frac{u \qquad a}{ua}[a \in \Sigma],$$

We have $X = \{u\}$ and $y = ua$. Let us assume that $P(u)$ holds, that is $\Delta^*_\varepsilon(q_0, u) = \delta^*(q_0, u)$. We wish to show that $P(ua)$ holds. So consider

$$\begin{aligned}\Delta^*_\varepsilon(q_0, ua) &= \bigcup_{q \in \Delta^*_\varepsilon(q_0,u)} \left\{q' \in Q : q \overset{a}{\Longrightarrow} q'\right\} \\ &= \delta(\Delta^*_\varepsilon(q_0, u), a) \\ &= \delta(\delta(q'_0, u), a) \\ &= \delta(q'_0, ua)\end{aligned}$$

So the statement holds for $P(ua)$.

By the Principle of Rule Induction, the statement holds for all $u \in \Sigma^*$. □

5.2.3 Kleene's Theorem

Theorem 5.2.2. A language L over the alphabet Σ is regular if and only if it can be accepted by a DFA $M = (Q, \Sigma, \delta, q_0, A)$.

Proof. ($\Longrightarrow$). By the subset construction theorem, it is sufficient to show that L can be accepted by the NFA$^\varepsilon$ $M_\varepsilon = (Q, \Sigma, \Delta_\varepsilon, q_0, A)$.

We wish to show $\forall L \in \mathcal{L}_\Sigma . \exists$ NFA$^\varepsilon$ $M . L = L(M)$. We proceed by rule induction over $\mathcal{L}_\Sigma$ with the statement

$$P(L) = (\exists \text{ NFA}^\varepsilon \ M . L = L(M)) .$$

Base Case. For our axioms

Axioms : $\dfrac{}{\emptyset}$ $\dfrac{}{\{\varepsilon\}}$ $\dfrac{}{\{a\}}[a \in \Sigma]$

We have the NFA$^\varepsilon$s

Figure 5.3: NFA$^\varepsilon$ M such that $L(M) = \emptyset$

Figure 5.4: NFA$^\varepsilon$ M such that $L(M) = \{\varepsilon\}$

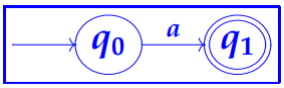


Figure 5.5: NFA$^\varepsilon$ M such that $L(M) = \{a\}$

So the statements $P(\emptyset)$, $P(\{\varepsilon\})$ and $P(\{a\})$, $a \in \Sigma$ hold.

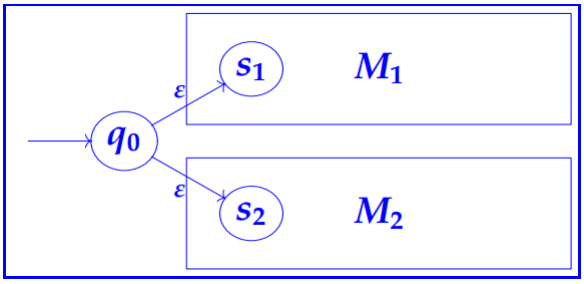
Inductive Step. We wish to show that $\forall (X, y) \in \mathcal{R}.\, (\forall x \in X.P(x)) \implies P(y)$ holds. For the rule

$$\frac{L_1 \qquad L_2}{L_1 \cup L_2}.$$

We have $X = \{L_1, L_2\}$ and $y = L_1 \cup L_2$. Let us assume that $P(L_1)$ and $P(L_2)$ holds, that is to say there exists $M_1 = (Q_1, \Sigma, \Delta^1_\varepsilon, q^1_0, A_1)$ and $M_2 = (Q_2, \Sigma, \Delta^2_\varepsilon, q^2_0, A_2)$ such that $L_1 = L(M_1)$ and $L_2 = L(M_2)$. For simplicity, we assume that $Q_1 \cap Q_2 = \emptyset$.

Let us consider $M = (\{q_0\} \cup Q_1 \cup Q_2, \Sigma, \Delta_\varepsilon, q_0, A_1 \cup A_2)$ where

$$\Delta_\varepsilon = \left\{((q_0, \varepsilon), \left\{q^1_0, q^2_0\right\})\right\} \cup \Delta^1_\varepsilon \cup \Delta^2_\varepsilon.$$



We wish to show that $L(M) = L_1 \cup L_2$, by the extensionality axiom that is

$$\begin{aligned} &\forall u \in \Sigma^*.\, (u \in L(M) \iff L_1 \cup L_2) \\ &\iff \forall u \in \Sigma^*.\, (u \in L(M) \iff u \in L_1 \vee u \in L_2) \end{aligned}$$

Let $u \in \Sigma^*$ be arbitrary.
($\Longrightarrow$). Let us assume that $u \in L(M)$, that is to say there is a transition sequence $q_0 \overset{u}{\Longrightarrow} q'$ where $q' \in A_1 \vee q' \in A_2$. We have the following two cases:

- **Case** $q' \in A_1$. Let us assume that $q' \in A_1$. Since Q_1 and Q_2 are disjoint and $q' \in A_1 \subseteq Q_1$, we deduce that the transition sequence $q_0 \overset{u}{\Longrightarrow} q'$ has the form
$$q_0 \overset{\varepsilon}{\to} q_0^1 \overset{u_1}{\Longrightarrow} q_i \cdots \overset{u_n}{\Longrightarrow} q',$$
where $q_i \in Q_1$. Hence we have the transition sequence $q_0^1 \overset{u}{\Longrightarrow} q' \in A_1$, by the definable property of $L(M_1)$, we have $u \in L(M_1) = L_1$.

- **Case** $q' \in A_2$. Similar argument.

Hence we have $u \in L_1 \cup L_2$.
($\Longleftarrow$). Let us assume that $u \in L_1 \vee u \in L_2$. We have the following two cases:

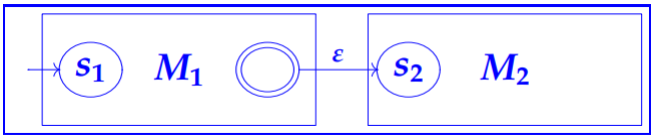
- **Case** $u \in L_1$. Let us assume that $u \in L_1 = L(M_1)$, that is to say we have the transition sequence $q_0^1 \overset{u}{\Longrightarrow} q'$ where $q' \in A_1$. Hence by our definition of Δ_ε for M, we have
$$q_0 \overset{\varepsilon}{\to} q_0^1 \overset{u}{\Longrightarrow} q' \in A_1 \cup A_2.$$
This transition sequence is equivalent to $q_0 \overset{u}{\Longrightarrow} q' \in A_1 \cup A_2$. By the definable property of $L(M)$, we have $u \in L(M)$.

- **Case** $u \in L_2$. Similar argument.

So we have $u \in L(M)$. Hence we are done.

For the rule
$$\frac{L_1 \qquad L_2}{L_1 L_2}.$$
We have $X = \{L_1, L_2\}$ and $y = L_1 L_2$. Let us assume that $P(L_1)$ and $P(L_2)$ holds, that is to say there exists $M_1 = (Q_1, \Sigma, \Delta_\varepsilon^1, q_0^1, A_1)$ and $M_2 = (Q_2, \Sigma, \Delta_\varepsilon^2, q_0^2, A_2)$ such that $L_1 = L(M_1)$ and $L_2 = L(M_2)$. For simplicity, we assume that $Q_1 \cap Q_2 = \emptyset$.

Let us consider $M = (Q_1 \cup Q_2, \Sigma, \Delta_\varepsilon, q_0^1, A_2)$ where
$$\Delta_\varepsilon = \Delta_\varepsilon^1 \cup \left\{((q, \varepsilon), \{q_0^2\}) : q \in A_1\right\} \cup \Delta_\varepsilon^2.$$



We wish to show that $L(M) = L_1L_2$, by the extensionality axiom that is

$$\forall u \in \Sigma^*.(u \in L(M) \iff u \in L_1L_2)$$
$$\iff \forall u \in \Sigma^*.(u \in L(M) \iff \exists v \in L_1, w \in L_2.u = vw)$$

Let $u \in \Sigma^*$ be arbitrary.
($\implies$). Let us assume that $u \in L(M)$, that is to say there exists the transition sequence $q_0^1 \overset{u}{\Longrightarrow} q'$ where $q' \in A_2 \subseteq Q_2$. Since Q_1 and Q_2 are disjoint, we may deduce that the transition sequence has the form

$$q_0^1 \overset{v}{\Longrightarrow} q_i \overset{\varepsilon}{\to} q_0^2 \overset{w}{\Longrightarrow} q' \in A_2,$$

where $q_i \in A_1$ and $u = vw$. So we have the transition sequence $q_0^1 \overset{v}{\Longrightarrow} q_i \in A_1$. By the definable property of $L(M_1)$, we have $v \in L(M_1) = L_1$. Similarly, we have $w \in L(M_2) = L_2$. So we are done.
($\impliedby$). Let us assume that $\exists v \in L_1, v \in L_2.u = vw$ holds. Let us introduce the witnesses $v' \in L_1 = L(M_1), w' \in L_2 = L(M_2)$ such that $u = v'w'$. So we have the transition sequences $q_0^1 \overset{v'}{\Longrightarrow} q' \in A_1$ and $q_0^2 \overset{w'}{\Longrightarrow} q'' \in A_2$. By our definition of Δ_ε for M we have

$$q_0^1 \overset{v'}{\Longrightarrow} q' \overset{\varepsilon}{\to} q_0^2 \overset{w'}{\Longrightarrow} q'' \in A_2.$$

This transition sequence is equivalent to $q_0^1 \overset{u}{\Longrightarrow} q'' \in A_2$. By the definable property of $L(M)$, we have $u \in L(M)$.

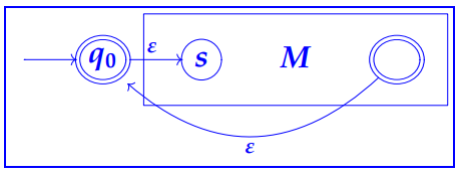
For the rule

$$\frac{L}{L^*}.$$

We have $X = \{L\}$ and $y = L^*$. Let us assume that $P(L)$ holds, that is to say there exists $M = (Q, \Sigma, \Delta_\varepsilon, q_0, A)$ such that $L = L(M)$.

Let us consider $M' = (Q \cup \{q_0'\}, \Sigma, \Delta_\varepsilon', q_0', \{q_0'\})$ where

$$\Delta_\varepsilon' = \Delta_\varepsilon \cup \{((q_0', \varepsilon), \{q_0\})\} \cup \{((q, \varepsilon), \{q_0'\}) : q \in A\}$$



We wish to show that $L(M') = L^*$, by the extensionality axiom that is

$$\forall u \in \Sigma^*.\, (u \in L(M') \iff u \in L^*)$$
$$\iff \forall u \in \Sigma^*.\, (u \in L(M') \iff \exists n \in \mathbb{N}. \exists w_1, \ldots, w_n \in L. u = w_1 \ldots w_n)$$

Let $u \in \Sigma^*$ be arbitrary.
($\implies$). Let us assume that $u \in L(M')$, that is to say there exists the transition sequence $q_0' \overset{u}{\Longrightarrow} q_0'$. We may deduce that the transition sequence has the form

$$q_0' \overset{\varepsilon}{\to} q_0 \overset{w_1}{\Longrightarrow} q_1 \overset{\varepsilon}{\to} q_0' \cdots \overset{\varepsilon}{\to} q_0' \overset{\varepsilon}{\to} q_0 \overset{w_n}{\Longrightarrow} q_n \overset{\varepsilon}{\to} q_0',$$

where $q_i \in A$ and $u = w_1 \ldots w_n$. Decomposing the transition sequence yields the sequences $q_0 \overset{w_1}{\Longrightarrow} q_1 \in A, \ldots, q_0 \overset{w_n}{\Longrightarrow} q_n \in A$. Hence by the definable property of $L(M)$ we have $w_1, \ldots, w_n \in L(M) = L$. So we are done.
($\impliedby$). Let us assume that $\exists n \in \mathbb{N}. \exists w_1, \ldots, w_n \in L. u = w_1 \ldots w_n$. So it follows that we have the transition sequences $q_0 \overset{w_1}{\Longrightarrow} q_1 \in A, \ldots, q_0 \overset{w_n}{\Longrightarrow} q_n \in A$. By our definition of Δ_ε' for M' we have

$$q_0' \overset{\varepsilon}{\to} q_0 \overset{w_1}{\Longrightarrow} q_1 \overset{\varepsilon}{\to} q_0' \cdots \overset{\varepsilon}{\to} q_0' \overset{\varepsilon}{\to} q_0 \overset{w_n}{\Longrightarrow} q_n \overset{\varepsilon}{\to} q_0'.$$

This transition sequence is equivalent to $q_0' \overset{u}{\Longrightarrow} q_0'$. By the definable property of $L(M')$, we have $u \in L(M')$.

By the Principle of Rule Induction, the statement holds for all $L \in \mathcal{L}_\Sigma$. □

Proof. ($\impliedby$). We instantiate lemma 5.2.1 with $S = Q$ and $q = q_0$ and $q' \in A$. So given the NFA $M = (Q, \Sigma, \Delta, q_0, A)$ we have $L(M) = L(r^Q_{q_0,q'}) = L$. By the subset construction theorem, we have the DFA $PM = (\mathcal{P}(Q), \Sigma, \delta, q_0', A')$ such that $L(PM) = L(M) = L(r^Q_{q_0,q'}) = L$. So we are done. □

Lemma 5.2.1. Given a NFA $M = (Q, \Sigma, \Delta, q_0, A)$, for all subsets $S \subseteq Q$ and for each pair of states $(q, q') \in Q \times Q$, there is a regular expression $r^S_{q,q'}$ such that

$$L(r^S_{q,q'}) = \left\{ u \in \Sigma^* : q \overset{u}{\to}{}^* q' \right\},$$

where all intermediate states in the transition sequence $q \xrightarrow{u}{}^{*} q'$ are members of S.

Proof. (**Induction on** $|S|$)
Base Case. We have $|S| = 0$, hence $S = \emptyset$. Let $(q, q') \in Q \times Q$ be arbitrary. We wish to show the existence of $r^{\emptyset}_{q,q'}$ such that

$$L(r^{\emptyset}_{q,q'}) = \left\{ u : q \xrightarrow{u}{}^{*} q' \text{ has no intermediate states} \right\}.$$

So L simply consists of symbols (strings of length 1) a (if $q \xrightarrow{a} q'$) and ε if $q = q'$. Hence $L(r^{\emptyset}_{q,q'}) \subseteq (\Sigma^1 \cup \{\varepsilon\})$. So we define $r^{\emptyset}_{q,q'}$ as

$$r^{\emptyset}_{q,q'} = \begin{cases} a_1 \mid \cdots \mid a_k & \text{if } q \neq q' \\ a_1 \mid \cdots \mid a_k \mid \epsilon & \text{if } q = q' \end{cases}.$$

So we have $P(0)$.
Inductive Step. We wish to show that $\forall |S| \in \mathbb{N}. P(|S|) \implies P(|S| + 1)$. Let $S \subseteq Q$ be some arbitrary subset. Let us assume that $P(|S|)$ holds, that is to say $\forall (q, q') \in Q \times Q. \exists r^{S}_{q,q'} \in \mathcal{R}_{\Sigma}$ such that

$$L(r^{S}_{q,q'}) = \left\{ u : q \xrightarrow{u}{}^{*} q' \text{ has intermediate states in } S \right\}.$$

Let $q_0 \in Q \setminus S$. Let us consider $S' = S \cup \{q_0\}$. Instantiating our inductive hypothesis, we have the regular expressions

$$\begin{aligned} r_1 &= r^{S}_{q,q'} \\ r_2 &= r^{S}_{q,q_0} \\ r_3 &= r^{S}_{q_0,q_0} \\ r_4 &= r^{S}_{q_0,q'} \end{aligned}$$

We define r as

$$r = r_1 \mid r_2 (r_3)^* r_4.$$

Evidently $L(r) \subseteq L(r^{S'}_{q,q'})$. We wish to show that $L(r) \supseteq L(r^{S'}_{q,q'})$, that is

$$\forall u \in \Sigma^*. u \in L(r^{S'}_{q,q'}) \implies u \in L(r).$$

Let $u \in \Sigma^*$ be arbitrary. Let us assume that $L(r^{S'}_{q,q'})$, that is to say there exists the state transition sequence $q \xrightarrow{u}{}^{*} q'$ has intermediate states in $S \cup \{q_0\}$. We have the following cases:

- **Case** $q \xrightarrow{u}{}^{*} q'$ doesn't contain q_0. Let us assume that $q \xrightarrow{u}{}^{*} q'$ doesn't contain q_0. Hence $u \in L(r_1)$.

- **Case** $q \xrightarrow{u}{}^{*} q'$ contains q_0. Let us assume that $q \xrightarrow{u}{}^{*} q'$ contains q_0. Let k be the number of times q_0 appears in the transition sequence $q \xrightarrow{u}{}^{*} q'$. We may deduce the transition sequence has the form

$$\underbrace{q \xrightarrow{v}{}^{*} q_0}_{\text{part } (i)} \underbrace{\xrightarrow{w_1}{}^{*} q_0 \xrightarrow{w_2}{}^{*} \cdots \xrightarrow{w_n}{}^{*} q_0}_{\text{part } (ii)} \underbrace{\xrightarrow{x}{}^{*} q'}_{\text{part}(iii)}.$$

  So we have $u = v(w_1 w_2 \dots w_n)x$ where $v \in L(r_2)$, $w_i \in L(r_3)$, so $w_1 w_2 \dots w_n \in L((r_3)^*)$ and $x \in L(r_4)$. Hence $u \in L(r_2(r_3)^* r_4)$.

So we have $u \in L(r_1 \mid r_2(r_3)^* r_4) = L(r)$. By the antisymmetry of $\subseteq$, we have $L(r_{q,q'}^{S'}) = L(r)$, hence $r = r_{q,q'}^{S'}$. So we have $P(|S|+1)$.

By the Principle of Mathematical Induction, we conclude the statement $P(|S|)$ holds for all $|S| \in \mathbb{N}$. □

5.2.4 The Pumping Lemma

Theorem 5.2.3. (**Pumping Lemma**) For all regular languages $L \in \mathcal{L}_\Sigma$, there exists $\ell \geq 1$ such that for all $w \in L$ where $|w| \geq \ell$ (the pumping length) can be written as $w = xyz$ satisfying the following conditions:

(i) $|y| \geq 1$.

(ii) $|xy| \leq \ell$.

(iii) $\forall n \geq 0. xy^n z \in L$.

Proof. Let $L \in \mathcal{L}_\Sigma$ be arbitrary. By Kleene's theorem there exists a DFA $M = (Q, \Sigma, \delta, q_0, A)$ such that $L = L(M)$. Let us introduce the witness $\ell = |Q|$. Let $w \in L$ be some arbitrary string such that $w = a_1 \dots a_n$ where $n \geq \ell$. By definition of $L(M)$, it follows that there exists some transition sequence $q_0 \xrightarrow{w}{}^{*} q' \in A$, that is

$$\underbrace{q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \cdots \xrightarrow{a_\ell} q_\ell}_{\ell+1 \text{ states}} \cdots \xrightarrow{a_n} q_n = q' \in A.$$

Since $\ell = |Q|$ it follows that $q_0 \dots q_\ell$ can't all be distinct by the pigeonhole principle. So there exists $0 \leq i < j \leq \ell$ such that $q_i = q_j$. So we may write the transition sequence as

$$q_0 \xrightarrow{x}{}^* \underbrace{q_i \xrightarrow{y}{}^* q_j}_{loop} \xrightarrow{z}{}^* q_n \in A,$$

where $x = a_1 \dots a_i$, $y = a_{i+1} \dots a_j$ and $z = a_{j+1} \dots a_n$. So we have $|y| \geq 1$ and $|xy| \leq \ell$. We now wish to show that $\forall n \geq 0, xy^n z \in L$. Let $n \geq 0$ be arbitrary. Consider $xy^n z$. The transition sequence $q_0 \xrightarrow{x}{}^* q_i$ leaves us in state q_i, from the above, we then repeat the *loop* n times, giving us the transition sequence $q_0 \xrightarrow{xy^n} q_j$. We also have the transition sequence $q_j \xrightarrow{z}{}^* q_n \in A$. Composing them yields the sequence $q_0 \xrightarrow{xy^n z}{}^* q_n \in A$. Hence $xy^n z \in L(M) = L$. So we are done.

□

- We may use to pumping lemma to show that a language is not regular using the following argument:

  $\forall \ell \geq 1. \exists w \in L. |w| \geq \ell \wedge w = xyz \wedge |y| \geq 1 \wedge |xy| \leq \ell \wedge \exists n \geq 0. xy^n z \notin L.$

5.2.5 Other Theorems

Theorem 5.2.4. For all regular languages L over Σ, $\overline{L} = \Sigma^* \setminus L$ is regular.

Proof. Let $L \in \mathcal{L}_\Sigma$ be an arbitrary regular language over Σ. By Kleene's theorem, there exists a DFA $M = (Q, \Sigma, \delta, q_0, A)$ such that $L = L(M)$. We wish to show that

$$\overline{L} = \{u \in \Sigma^* : u \notin L\},$$

is regular. It suffices to show that there exists a DFA $\overline{M}$ such that $\overline{L} = L(\overline{M})$. Let us introduce the witness $\overline{M} = (Q, \Sigma, \delta, q_0, Q \setminus A)$. We wish to show that $\overline{L} = L(\overline{M})$, by the extensionality axiom, that is

$$\forall u \in \Sigma^*. u \in \overline{L} \iff u \in L(\overline{M}).$$

So we have

$$\begin{aligned}
&\forall u \in \Sigma^*. u \in \overline{L} \iff u \in L(\overline{M}) \\
&\iff \forall u \in \Sigma^*. u \notin L \iff q_0 \xrightarrow{u}{}^* q \in Q \setminus A \\
&\iff \forall u \in \Sigma^*. u \notin L \iff q_0 \xrightarrow{u}{}^* q \notin A \\
&\iff \forall u \in \Sigma^*. u \notin L \iff u \notin L
\end{aligned}$$

So we are done. □

- The equivalent regular expression for $\overline{L} = \overline{L(r)}$ is denoted $\overline{r}$.

Theorem 5.2.5. For all regular languages L_1 and L_2 over Σ, their intersection $L_1 \cap L_2$ is regular.

- The equivalent regular expression for $L(r_1) \cap L(r_2)$ is denoted $r_1 \& r_2$.

Definition 5.2.4. (**Equivalence of Regular Expressions**) The regular expressions r_1 and r_2 are said to be equivalence if $L(r_1) = L(r_2)$.